Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries

Study for the
European Commission
Directorate-General Information Society (2002)

RAND Europe

Project Managers:
Dr Andrew Rathmell/Dr Lorenzo Valeri
RAND Europe
Grafton House, 64 Maids Causeway
Cambridge, CB5 8DD
United Kingdom
Tel: +44 (0)1223 353329
E-mail: lvaleri@rand.org

Project Coordinator
Neil Robinson
RAND Europe
Grafton House, 64 Maids Causeway
Cambridge, CB5 8DD
United Kingdom
Tel: +44 (0)1223 353329
E-mail: neilr@rand.org

Project Officer:
Andrea Servida
DG Information Society
European Commission
No 9 Ave des Beaulieu
B 1160 Brussels
Belgium
Tel: +32 2 2958186
E-mail: Andrea.Servida@cec.eu.int

Information Society Technologies

The opinions expressed in this Study are those of the authors and do not necessary reflect the views of the European Commission.
© ECSC-EC-EAEC, Brussels -Luxembourg 2003

Executive Summary

This Handbook is composed of two sections followed by three annexes and a glossary.

Section one opens by bringing forward an analytical framework for describing and categorising those computer misuse and security incidents that CSIRTs can map across various legal frameworks. This analysis builds upon work undertaken in the context of the European Commission, Internet Engineering Task Force, G8 and several other inter-governmental and business initiatives. Afterwards, a comprehensive overview of international legal principles in the area of cybercrime is provided. Particular attention is devoted to the examination of the content of the Council of Europe´s Cybercrime Convention and the proposed European Framework Decision on Attacks Against Information Systems. This analysis is followed by an overview of the main issues associated with incident response and forensic principles for cybercrime. Particular attention is directed to the admissibility of electronic evidence, privacy concerns, investigation and presentation. The last part of section one provides an overview of current cybercrime-related surveys. The analysis focuses primarily on assessing strengths and weaknesses of these surveys and actions to be taken to develop a better understanding of the size of cybercrime.

Section two of the handbook contains an analysis for each EU member states of their legislation in the area of computer crime. A summary table is also provided together with the necessary point of law enforcement point of contacts and reporting mechanisms.

For more information about the Handbook, please contact the project coordinator:

Neil Robinson
RAND Europe
Grafton House, 64 Maids Causeway
Cambridge, CB5 8DD
United Kingdom
Tel: +44 (0)1223 353329
E-mail: neilr@rand.org

The opinions expressed in this Study are those of the authors and do not necessary reflect the views of the European Commission.
© ECSC-EC-EAEC, Brussels-Luxembourg 2003

Preface

Enhancing the capabilities of Europe's Computer Security Incident Response Teams (CSIRT)[1] is an important objective of eEurope Action Plan 2002, the eEurope Action Plan 2005, the European Council Communication on Network and Information Security and the IST Programme (WP2002). Europe's CSIRTs face a serious challenge in dealing with incidents, many of which are cross-border in origin. They are operating in an environment where EU Member States have divergent legal codes dealing with computer crime and misuse and in which law enforcement authorities have varied approaches to dealing with the same.

This Handbook is a tool which has been designed to help CSIRTs to meet this challenge. It is an easy to use guide that matches technical descriptions of incidents to the legal framework of the country in question and details procedures for working with law enforcement to respond to incidents. This Handbook will be of interest to organisations involved in the incident handling phase. These include Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT) and Warning, Advice and Reporting Points (WARPs). It will also be of use to law enforcement agencies that are engaged in incident response and investigation and to other organizations involved in warning and information sharing. Finally, although it covers only legal and law enforcement issues in the 15 EU Member States, the Handbook will be of use to incident response teams in other countries who may need to deal with EU legislation or law enforcement. It is hoped that the Handbook could provide a model for such work in other regions and perhaps at the global level.

This Handbook was commissioned and funded by the European Commission, Directorate-General Information Society to RAND Europe, who led the project (Maarten Botterman, Shawna Gibson, Andrew Rathmell, Neil Robinson, Rebecca Shoob, and Lorenzo Valeri). The user requirements and incident categorisation scheme was developed by Professor Danilo Bruschi from the Università degli Studi di Milano and President of CLUSIT, the Italian Association for Information Security. The legal survey was undertaken by Professor Ernesto Savona, Mara Mignone and Leonardo del Negro from the Transcrime Research Centre at the University of Trento. Pieter van Dijken led the work on forensic procedures. Nicola Dileone, Serious Crime Department, High Tech Crime, EUROPOL, led the work in integrating the law enforcement perspective into the report. Andrea Monti provided assistance concerning the legal situation Italy. Particular thanks to Andrew Cormarck from UKERNA and the staff at TERENA in the Netherlands for their constant support.

Disclaimer
All legislation was verified as accurate on 30 September 2003, unless otherwise stated. European Commission, RAND Europe and all the authors of this report are not liable of the implications of any actions or activity based upon the information contained in this report and its subsequent versions and developments. Moreover, this work represents the view of its authors only and not those of the European Commission or associated institutions.

[1] The term CSIRT is used to encompass the term Computer Emergency Response Team (CERT®) and associated concepts such as Warning, Advice and Reporting Points (WARP).

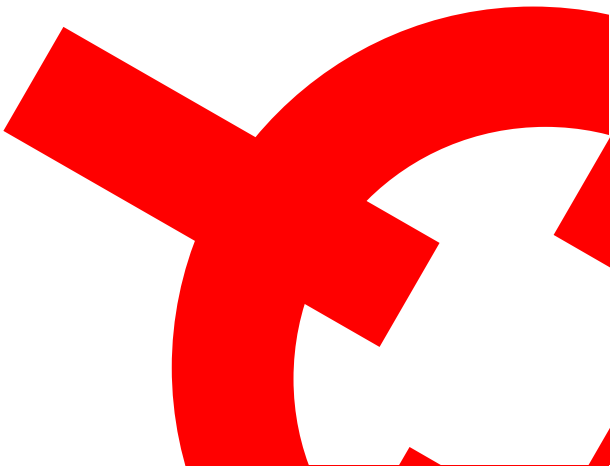
Contents

Section 1

Introduction and Overview

Chapter 1

How to Use this Handbook



Chapter 1: How to Use this Handbook

1.1 Introduction

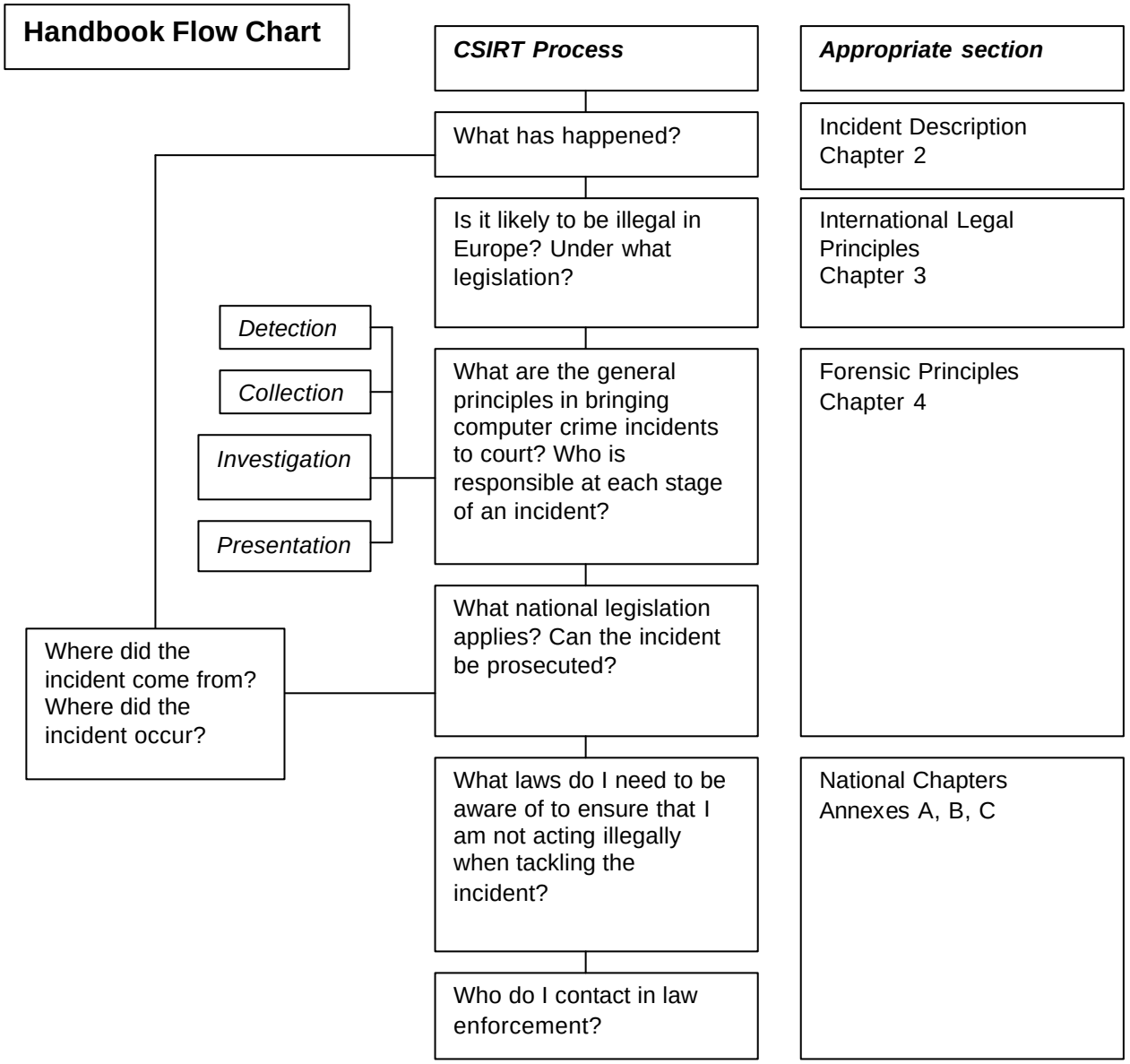
This section provides a guide to how Computer Security Incident Response Teams (CSIRTs) can make effective use of this Handbook.

Most CSIRTs operate in the following manner: a member of their constituency or a external party reports a potential security incident which relates to a problem affecting computer systems under the unit's responsibility. The CSIRT evaluates the information and, in the case of a real incident being reported, it begins investigations – or more precisely, the incident response phase. The incident is classified, and the 'customer' is provided with the information necessary to restore the systems involved.

As they go through this process, CSIRTs will want to know what, if any, criminal laws apply to the breach of confidentiality, integrity or availability; who to contact in law enforcement; and the steps that they should take in order to assist with evidence collection and preservation.

This Handbook has been designed to give CSIRTs quick answers to the following questions.

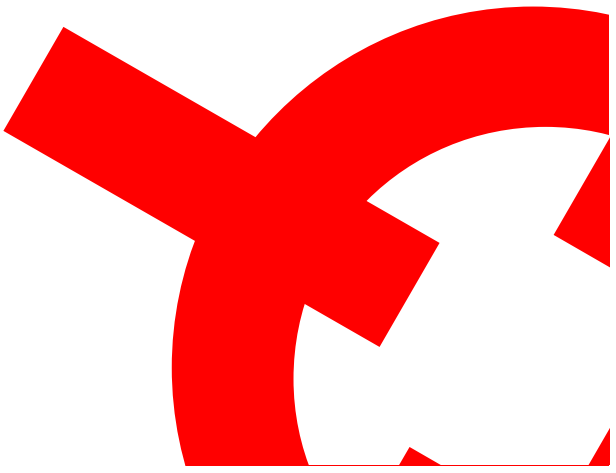
- Is the incident prosecutable?
- Which crime(s) are related to the incident?
- Under which legal framework does it fall?
- What evidence has to be collected in order to prosecute the attacker?
- How should evidence be collected?
- How should evidence be preserved?
- How should reports to law enforcement be made?
- Are there are other reporting mechanisms?


Handbook Flow Chart
CSIRT Process
Appropriate section
What has happened?
Incident Description
Chapter 2
Is it likely to be illegal in Europe? Under what legislation?
International Legal Principles
Chapter 3
Detection
Collection
Investigation
Presentation
What are the general principles in bringing computer crime incidents to court? Who is responsible at each stage of an incident?
Forensic Principles
Chapter 4
Where did the incident come from? Where did the incident occur?
What national legislation applies? Can the incident be prosecuted?
What laws do I need to be aware of to ensure that I am not acting illegally when tackling the incident?
National Chapters
Annexes A, B, C
Who do I contact in law enforcement?

Notes

Chapter 2

Incident Descriptions



Chapter 2: Incident Descriptions

2.1 Introduction

The purpose of this chapter is to provide a framework for describing and categorising computer misuse and security incidents that CSIRTs can map across to various legal frameworks.

There is considerable work underway in Europe and in the international CSIRT community to standardise descriptions of computer security incidents. This standardisation work builds upon vulnerability description work, such as the Common Vulnerabilities and Exposures Database.[2] Standardisation work involves, *inter alia*:

- IST project eCSIRT network;[3]
- Common Intrusion Detection Framework and IETF work on intrusion detection;[4]
- Incident Object Description and Exchange Format Working Group[5] and now the Extended Incident Handling (INCH) Working Group at the IETF;[6] and
- G–8 and other inter-governmental and business (e.g. ISAC) incident classification initiatives.[7]

This Handbook adopts the following classification of information security incidents. The attack vectors described are samples and do not represent an exhaustive list.

2.1.1 Computer Fingerprinting

Definition: actions performed in order to gather information about a target.
Techniques: probing, scanning, DNS interrogation, Ping.
Attack vector (means or characteristics used): UDP/TCP active ports, O/S, hosts' addresses, SNMP servers' characteristics, CGIs' names, ICMP war dialling.

2.1.2 Malicious Code

Definition: Target host compromised via independent program execution.
*Techniques***:** Conscious or unconscious independent program execution.
Attack vector (i.e. means or characteristics used): Computer virus, worms, backdoor software,Trojans and spyware.

---

[2] Common Vulnerabilities and Exposures Database: http://cve.mitre.org.
[3] The European CSIRT Network: http://www.ecsirt.net.
[4] Common Intrusion Detection Framework: http://www.isi.edu/gost/cidf/.
[5] Incident Object Description and Exchange Format Working Group: http://www.terena.nl/tech/task-forces/tf-csirt/iodef/.
[6] http://www.ietf.org/html.charters/inch-charter.html.
[7] Peter G. Allor and James R. Lindley (2000) *A Short Narrow Look at the History and Purpose of Information Sharing and Analysis Centers* (January), available at: http://www.it-isac.org/isacinfowhtppr.php.

2.1.3 Denial of Service

Definition: Repeated target access that overloads capacity or otherwise disrupts a service.
Techniques: Execute programs which perform endless requests of computer resources such as: memory, CPU time, TCP–UDP connections, disk space.
Attack vector: SYN-flood, Ping of Death, Land, WinNuke, TFN, TFN2K, Trin00, Slice3, MStream, Smurg, Fraggle.

2.1.4 Account Compromise

Definition: Unauthorised access to a system, or system resource at sys-admin (root) or user level.
Techniques: Exploit, either locally or remotely, software vulnerabilities in order to obtain unauthorised access to user accounts. The same result can also be obtained using credentials which have been illegally obtained (stolen, intercepted, coerced).
Attack vector: Buffer overflow, format bug, CGI attack or use of stolen credentials (username and password).

2.1.5 Intrusion Attempt

Definition: Attempted unauthorised access to a computer system.
Techniques: Either trying to gain access to a system by guessing users' credentials, or trying to perform any of the attack vectors described herein, unsuccessfully.
Attack vector: Multiple login attempts, unsuccessful buffer overflow attempts, use of default user ID/password, attempts to exploit older vulnerabilities, attempted use of default accounts, attempted connections to SMNP ports.

2.1.6 Unauthorised Access to Information

Definition: Attempts to obtain unauthorised access to data.
Techniques: Trying to gain access, either locally or remotely, to data circumventing access control mechanisms.
Attack vector: SQL-injection, CGI parameter manipulation.

2.1.7 Unauthorised Access to Transmissions

Definition: Interfering without right and by technical means, with non-public transmissions of computer data to, from, or within a computer system.
Techniques: Intercepting network packets, injecting packets into traffic flow and removing packets from traffic flow.
Attack vector: Session hijacking, 'man-in-the-middle' attack, replay attack, 'sniffing' and keylogging, ARP poisioning.

2.1.8 Unauthorised Modification of Information

Definition: Unauthorised modification of information that is held electronically on a computer system.
Techniques: Local or remote modification, or creation of any kind of data, which resides in a computer without the required authorisation.
Attack vector: web defacements, viruses, alteration of log files, installation of unauthorised software, SQL-injection, removal of archives, hard disk formatting.

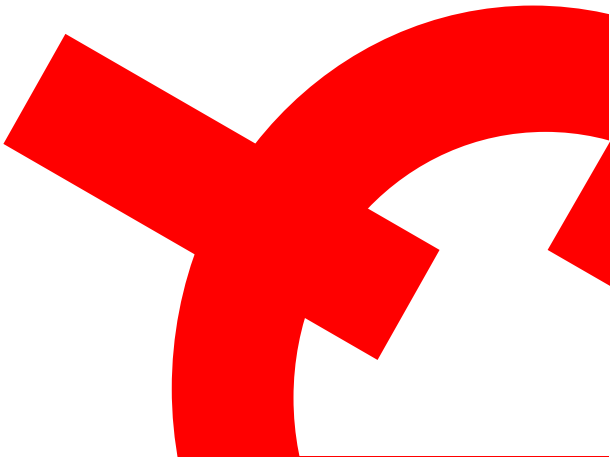
2.1.9 Unauthorised Access to Communication Systems

Definition: Unauthorised use of a communication system.
Techniques: Modify configuration settings of communication systems in order to gain personal advantage of their use.
Attack vector: DNS spoofing, unauthorised use of mail transfer agents, mail relays, proxies, private telephone exchanges and voicemail systems, war driving, war dialling and modification of routing tables.

Notes

Chapter 3

International Legal Principles



Chapter 3: International Legal Principles

3.1 Introduction

This chapter aims to provide an overview of the main international legal principles in the area of cyber-crime. Particular attention is directed to an analysis of pillar documents, such as the Council of Europe (CoE) Convention on Cybercrime and the proposed European Framework Decision on Attacks against Information Systems. A structure–text comparison between these two texts has been undertaken in order to simplify the reading and understanding of the document.

The legal framework existing at an international level in the area of cybercrime remains confused. There is wide agreement on the need to harmonise national legal provisions and to enhance judicial and police cooperation, but there are still many obstacles that hamper the achievement of concrete results. Nonetheless, the need to prevent and control cybercrime in order to enhance the development of an Information Society is a priority on the agendas of almost all national and international institutions. Therefore, there are good prospects for improved harmonisation and cooperation in coming years.

3.2 Working Definitions

Given that there is still no agreement about the terms and the definitions that are used to classify cybercrime, it is important to explain the working definitions used in this Handbook.

First, we discuss the difference between computer crimes and computer-related crimes.[8]

3.2.1 Computer Crimes

Computer crimes encompass all offences against the confidentiality, integrity and availability (CIA) of computer data and systems. Examples include illegal access to computer systems or malicious code-writing.

3.2.2 Computer-related Crimes

Computer-related crimes are: 'traditional crimes that can be, or have been, committed utilising other means of perpetration which are now being, or are capable of being, executed via the Internet, computer-related venue (e-mail, newsgroups, internal networks) or other technological computing advancement.'[9] For example, intellectual property rights infringement (e.g. digital music and software piracy) and payment system frauds (e.g. credit card fraud via the Internet).

[8] Very often, different terms and expressions are used as synonyms of both computer crime and computer-related crime. For example, computer crime is also called cybercrime, while computer-related crimes are defined as computer-facilitated crime, or technocrime. High-tech crime is often used to cover both categories.

[9] Transcrime Research Centre, University of Trento (2002) *Transatlantic Agenda EU/US Co-operation for Preventing Computer Related Crime – Final Report*.

3.2.3 Scope of this Handbook

First, the scope of the Handbook is limited to computer crime. (This takes into account the importance of distinguishing between Pillar 1 or European Community action in Research and Development and Pillar 3 or Justice and Home Affairs responsibilities, and a review of CSIRT-user requirements.) Second, it is important to be clear about the way in which this Handbook uses the term 'crime'. A crime is an intentional act that is committed in breach of criminal law. That is, there is no crime without a criminal provision and a related sanction.

As far as computer crimes are concerned, the legal framework existing at both national and international levels is still too fragmentary to distinguish clearly between criminal, civil and administrative laws. For example, in some cases there are no laws at all. In other cases, where a legal provision exists, the main problem is that not all countries have chosen to regulate computer crime (i.e. CIA offences) by means of criminal law.

Crime will not be considered here from a technical standpoint, but rather as a synonym of offence, infringement or violation.

Third, it is important to understand the variety of ways in which European countries have dealt with computer crime in their legal systems. In continental European countries, the criminal code brings together and codifies substantive national criminal law. Updates to deal with new crimes can either be added to the criminal code or can be the subject of new laws. In relation to computer crime, some European countries have added new articles to their criminal code, while others have introduced specific new laws.

Table 1 Criminality of Incidents in the 15 Member States of the EU

Country	Target fingerprinting	Malicious code	Denial of service	Account compromise	Intrusion attempt	Unauthorised access to information	Unauthorised access to transmissions	Unauthorised modification of information	Unauthorised access to communication system
Austria	n.a.	n.a.	n.a.	Adm.	Adm.	Adm.	n.a.	n.a.	Adm.
Belgium	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.	Crim.
Denmark	Crim	Crim	Crim	Crim	Crim	Crim	Crim	n.a.	Crim
Finland	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
France	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Germany	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Greece	n.a.	n.a.	n.a.	Crim	Crim	Crim	n.a.	n.a.	Crim
Ireland	n.a.	n.a.	n.a.	Crim	Crim	Crim	n.a.	n.a.	Crim
Italy	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Luxembourg	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
The Netherlands	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Portugal	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Spain	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
Sweden	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim
United Kingdom	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim	Crim

Source: RAND Europe / Transcrime Research Centre

Legend:
n.a. = no available legislation
Adm. = Administrative sanction provided
Crim. = Penal sanction provided

3.3 International Legal Overview

In international terms, the Council of Europe's Convention on Cybercrime,[10] is considered to be one of the main unique points of reference. Currently, the text is not legally binding. It is open for signature by CoE Member States and those non-Member States who participated in its elaboration. Additionally, it is open for accession by other non-Member States.[11] The Convention is one of the most comprehensive documents on cybercrime available. It contains concrete efforts towards the outlining of common definitions for crimes related to computer systems.[12]

The Handbook legal survey was conducted taking into account the legal definitions provided by the Convention on Cybercrime.

The European Commission has also proposed a Council Framework Decision on Attacks against Information Systems. After being discussed by the Substantive Criminal Law Working Group, it would appear that the text will be finally approved before the end of the Greek Council Presidency in June 2003.[13] The objective of this initiative is 'to improve cooperation between judicial and other competent authorities, through approximating rules on criminal law in the Member States in the area of attacks against information systems'. As explained in the Framework Decision, attacks against information and computer systems are a concrete and dangerous threat that require an effective response. Specifically, it is necessary to further increase awareness of the problem related to information security and to provide practical assistance. This Framework Decision intends to complement the work performed by international organisations, in particular that of the Council of Europe's on approximating criminal law and the Group of Eight (G8)'s efforts to enhance transnational cooperation in the area of high-tech crime.

The Convention on Cybercrime and the Framework Decision are closely connected and their definitions overlap deliberately. For example, Title 1 of

---

[10] Council of Europe (2001, November), Convention on Cybercrime and explanatory memorandum, Strasbourg, France: European Committee on Crime Problems, available at: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm.

[11] For the Convention to enter into force, five ratifications are necessary. This number must include at least three Member States of the Council of Europe. The status as of 27 May 2003 is as follows:

- total number of signatures not yet followed by ratifications: 33;
- total number of ratifications/accessions: 3 (Albania, Croatia and Estonia).

[12] For the sake of completeness, it is necessary to point out that there is no consensus on the final text of the Convention. Organisations dealing with the defence of civil rights and the free use of the Internet do not share the approach adopted by the CoE. They believe that this Convention will enhance different forms of surveillance by governments and law enforcement agencies, at national and international levels, while reducing the freedom and privacy of Internet users. According to these organisations, there should be other ways of preventing and controlling cybercrime, while respecting the essence of the Internet, the aim of which is primarily to develop and improve a worldwide, easy and fast communication and information system.

[13] Council of the European Union, Council Framework Decision on Attacks Against Information Systems, Brussels, 12 May 2003, Interinstitutional file 2002/0086 (CNS), 8687/03, available at: http://register.consilium.eu.int/pdf/en/03/st08/st08687en03.pdf.

the Convention is concerned specifically with *offences against the confidentiality, integrity and availability of computer data and systems*. These offences are also found in the Framework Decision. Table 2 (below) summarises the articles from the Convention and the Framework Decision. The articles are listed in numerical order.

Table 2: Article summary of the Convention on Cybercrime and the Framework Decision on Attacks Against Information Systems

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME	COUNCIL OF THE EUROPEAN UNION FRAMEWORK DECISION ON ATTACKS AGAINST INFORMATION SYSTEMS
Illegal access (Article 2): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Illegal access to Information Systems (Article 2):** 1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor. 2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.
Illegal interception (Article 3): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	
Data interference (Article 4): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Illegal data interference (Article 4):** Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.
System interference (Article 5): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Illegal system interference (Article 3):** Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

	Instigation, aiding and abetting and attempt (Article 5): 1. Each Member State shall ensure that the instigation of, aiding and abetting and attempt to commit an offence referred to in Articles 2, 3 and 4 is punishable as a criminal offence. 2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence. 3. Each Member State may decide not to enforce paragraph 2 for the offences referred to in Article 2.
Misuse of devices (Article 6): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2–5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and b. the possession of an item referred to in paragraphs (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1(a)(ii).	Not defined within the Framework Decision.

Attempt and aiding or abetting (Article 11): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2–10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9(1)(a) and 9(1)(c) of this Convention. 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	

The following crimes are classified in the Convention on Cybercrime but are not addressed by the Framework Decision. Although they refer to the category of computer-related crime, they are mentioned here because they are clearly crimes that are related to computers. However, it is important to point out that Member State legislation may exist only for crimes that are perpetrated in the offline environment. These legislative measures may not take into account for similar crimes being perpetrated with the assistance of a computer.

The Convention on Cybercrime identifies three other groups of offences:

- (1) computer-related offences;
- (2) content-related offences; and
- (3) offences related to infringements of copyright and associated rights.

3.3.1 Computer-related Offences

These include two main typologies of crime:

- (1) computer-related forgery: the Convention on Cybercrime defines this as the 'input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible'; and
- (2) computer-related fraud: the Convention on Cybercrime defines this as 'the causing of a loss of property to another by: any input, alteration, deletion or suppression of computer data, any interference with the functioning of a computer system'.

3.3.2 Content-related Offences

These cover activities related to the distribution of illegal content, of which the most visible expression is child pornography.[14] They are listed as follows:

(a) producing child pornography for the purpose of its distribution through a computer system;
(b) offering or making available child pornography through a computer system;
(c) distributing or transmitting child pornography through a computer system;
(d) procuring child pornography through a computer system for oneself or for another;
(e) possessing child pornography in a computer system or on a computer-data storage medium.

3.3.3 Offences Related to Infringements of Copyright and Related Rights

Finally, this encompasses violations of copyright and related rights – with the exception of moral rights – 'where such acts are committed wilfully, on a commercial scale and by means of a computer system'. The Convention on Cybercrime refers to all the international treaties and conventions that already exist at an international level.

3.4 Relating Incidents to international Legal Definitions

In order to assist CSIRTs to understand the legal dimensions of the technical incidents that they encounter, we have developed matrices to match those technical incident descriptions to international legal definitions. The following observations are useful to understand the methodology which is used to match the incident taxonomy to international legal definitions.

3.4.1 Legal Framework

The legal framework that exists at an international level is still embryonic. This means that there are significant gaps and differences in the laws of Member States in the area of computer crime. The lack of common and/or harmonised definitions is one of the most relevant problems, and the fact is that there is no agreement on the constituent elements of computer crime as criminal offences.

This situation is likely to change with the entry into force of the Convention on Cybercrime, especially after its implementation at a national level. Because the Convention is the only existing international text, it is used here as the reference document. That is, the incident taxonomy is matched to the legal definitions of CIA offences listed in the Convention on Cybercrime.

[14] According to the Convention on Cybercrime, child pornography includes pornographic material that visually depicts: a minor who is engaged in sexually-explicit conduct; a person appearing to be a minor who is engaged in sexually-explicit conduct; and realistic images representing a minor who is engaged in sexually-explicit conduct. The term 'minor' includes all persons under 18 years of age. Nevertheless, a Party may also require a lower age-limit, which shall be not less than 16 years of age.

3.4.2 Development of Laws

To date, national laws have been developed autonomously. This means that, while some countries have preferred to amend their penal or criminal code, other countries have decided to pass specific laws on cybercrime (not included in the penal/criminal code). There are even some countries that do not have legal provisions regarding cybercrime at all – either in their penal/criminal code, or in the form of special laws.

3.4.3 Legal Approach

The legal approach to cybercrime is significantly different from the technical approach. Consequently, matching the incident taxonomy resulting from the user requirement analysis to international legal definitions on CIA offences is imprecise. On the one hand, legal provisions tend to be far more general, in order to encompass the widest set of offences and to take account of future technological innovations. On the other hand, the technical perspective is extremely offence-oriented, i.e. it is characterised by a detailed or granular approach to the understanding of the techniques used to perpetrate the offence/crime.

It is quite clear that this generalised legal approach does not fit well with the precise and detailed technical analysis of computer security incidents.

3.4.4 Terminology

Another issue is one of terminology. It is obvious that legal concepts and terms are unrelated to those used in the area of information security. Moreover, when the same term is used in both law and science, it is frequently used with a different meaning; resultant confusion is inevitable.

3.5 The Matrices

In developing this section we discovered that, due to the differences between the definitions in the Convention on Cybercrime and those in the national laws, there was a risk that the matrix would turn out to be inapplicable or too complex. Therefore we took two steps, which are reflected in the two matrices.

The first step required the development of a matrix matching the incident classification based on user requirements to the Convention on Cybercrime. Although no exact matches in terminology exist, it was considered important that the aim of each article encompassed the activities outlined within the incident classification. The articles used were only those related to CIA offences (Article 2 – Illegal access; Article 3 – Illegal interception; Article 4 – Data interference; Article 5 – System interference; Article 6 – Misuse of device; and Article 11 – Attempt and aiding of abetting).

The second step consisted of the integration of the matrix with an additional set of legal definitions. The new definitions resulted from the analysis of both the preliminary texts of the Convention on Cybercrime and national laws. This should make the matrix clearer and easier to understand, especially for readers who do not have a legal background.

Matrix 1: Incident classification – Convention on Cybercrime

INCIDENT CLASSIFICATION	CONVENTION ON CYBERCRIME
Target Fingerprinting: actions performed in order to gather information about a target.	**Misuse of device (Art. 6)**[15] a) The production, sale, procurement for use, import, distribution or otherwise making available of: 1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2–5 (namely CIA offences); 2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2– 5; and b) The possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5 (namely, CIA offences).
Malicious Code: target host compromised via unattended code execution.	**Data interference (Art. 4)** The damaging, deletion, deterioration, alteration or suppression of computer data without right. **System interference (Art. 5)** The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Denial of Service: repeated target access that overloads capacity or otherwise disrupts a service	**System interference (Art. 5)** The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Account Compromise: unauthorised access to a system or system resource at Administrator (root) and/or user level	**Illegal access (Art. 2)** The access to the whole or any part of a computer system without right.
Intrusion Attempt: attempted unauthorised access to a computer system	A combination of the following articles: **Illegal access (Art. 2)** **Attempt and aiding or abetting (Art. 11)** **Illegal access (Art. 2)** The access to the whole or any part of a computer system without right. **Attempt and aiding or abetting (Art. 11)** Attempt to commit the illegal access to the whole or any part of a computer system without right.
Unauthorised access to information: attempts to obtain	**Illegal access (Art. 2)** The access to the whole or any part of a computer system without right.

[15] The applicability of this article to target fingerprinting is somewhat forced. However, as far as the Convention on Cybercrime is concerned, it is the only article that fits.

unauthorised access to data	**Illegal interception (Art. 3)** The interception, without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying out such computer data.
Unauthorised access to transmissions: interfering without right and by technical means, with non-public transmissions of computer data, to, from or within a computer system	**Illegal interception (Art. 3):** The interception, without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying out such computer data.
Unauthorised modification of information: unauthorised modification without right of information held electronically on a computer system	**Data interference (Art. 4):** The damaging, deletion, deterioration, alteration or suppression of computer data without right.
Unauthorised access to communication system: unauthorised use of a communication system	**Illegal access (Art. 2)** The access to the whole or any part of a computer system without right.

Matrix 2: Incident classification – Convention on Cybercrime, legal definitions

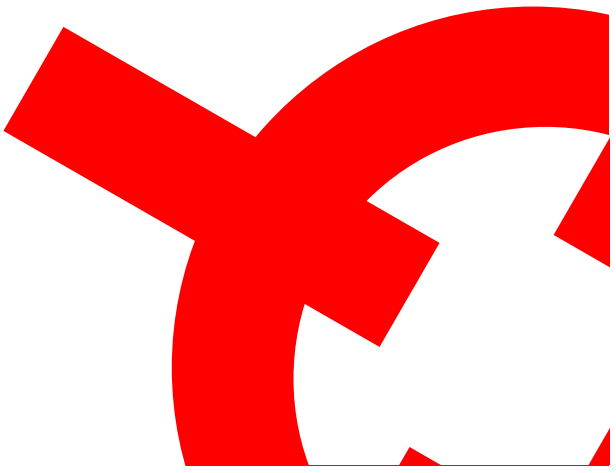
INCIDENT CLASSIFICATION	CONVENTION ON CYBERCRIME	LEGAL DEFINITIONS
Target Fingerprinting: actions performed in order to gather information about a target	**Misuse of device (Art. 6)** a) The production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2–5 (namely CIA offences); ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and b) The possession of an item referred to in paragraphs (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5 (namely, CIA offences).	**Unauthorised interception:**[16] The interception, made without right and by technical means, of communication to, from and within a computer system or network.
Malicious Code: target host compromised via unattended code execution	**Data interference (Art. 4)** The damaging, deletion, deterioration, alteration or suppression of computer data without right. **System interference (Art. 5)** The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Computer sabotage:** The input, alteration erasure, or suppression of computer data or computer programs, or interface with computer systems with the intent to hinder the functioning of a computer or a telecommunications system **Damage to computer data or computer programs:** The erasure, damaging, deterioration or suppression of computer data or computer programs without rights.
Denial of Service: repeated target access that overloads capacity or otherwise disrupts a service	**System interference (Art. 5)** The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Computer sabotage:** The input, alteration erasure, or suppression of computer data or computer programs, or interface with computer systems with the intent to hinder the functioning of a computer or a telecommunications system.
Account Compromise: unauthorised access to a system or system resource at Administrator	**Illegal access (Art. 2)** The access to the whole or any part of a computer system without right.	**Unauthorised access:** The access without rights to a computer system or network by infringing security measures.

[16] For the purpose of the Handbook, the term interception refers almost exclusively to the interception, made without right and by technical means, of communications *within* a computer system.

(root) and/or or user level		
Intrusion Attempt: attempted unauthorised access to a computer system	A combination of the following articles: **Illegal access (Art. 2)** **Attempt and aiding or abetting (Art. 11)** **Illegal access (Art. 2)** The access to the whole or any part of a computer system without right. **Attempt and aiding or abetting (Art. 11)** Attempt to commit the illegal access to the whole or any part of a computer system without right.	**Unauthorised access:** The access without rights to a computer system or network by infringing security measures.
Unauthorised access to information: attempts to obtain unauthorised access to data	**Illegal access (Art. 2)** The access to the whole or any part of a computer system without right. **Illegal interception (Art. 3)** The interception, without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying out such computer data.	**Unauthorised interception:** The interception, made without right and by technical means, of communication to, from and within a computer system or network. **Unauthorised access:** The access without rights to a computer system or network by infringing security measures.
Unauthorised access to transmissions: interfering without right and by technical means, with non-public transmissions of computer data, to, from or within a computer system	**Illegal interception (Art. 3)** The interception, without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying out such computer data.	**Unauthorised interception:** The interception, made without right and by technical means, of communication to, from and within a computer system or network.
Unauthorised modification of information: unauthorised modification without right of information held electronically on a computer system	**Data interference (Art. 4)** The damaging, deletion, deterioration, alteration or suppression of computer data without right.	**Alteration of computer data or computer programs:** The alteration of computer data or computer programs without right.
Unauthorised access to a communication system: unauthorised use of a communication system	**Illegal access (Art. 2)** The access to the whole or any part of a computer system without right.	**Unauthorised access:** The access without rights to a computer system or network by infringing security measures.

Chapter 4

Forensic Principles



Chapter 4: Forensic Principles

4.1 Introduction

The objective of this section is to provide an overview of the issues associated with incident response and forensic principles. Particular attention is directed to issues related to the admissibility of electronic evidence, the impact of privacy concerns, investigation and presentation.

It is not the role of CSIRTs to undertake law enforcement tasks such as building an evidentiary case, although some CSIRTs in large companies do have sophisticated forensic and investigatory capabilities. Nonetheless, CSIRTs need to understand the common forensic procedures that are followed by law enforcement, if only to prevent their initial actions from damaging evidence.

During the incident response phase, a lot of data is collected which includes all system events (audit records) automatically collected by the system as well as any information that can document the activities undertaken for managing the incident, for example, all external conversations, telephone calls, etc. Such data is very useful for performing the incident *post mortem* analysis and, if required, for forensic purposes.

Procedural laws and practices surrounding computer forensics and the preparation of evidence for court vary widely, even within the 15 EU Member States. Therefore, it is important for CSIRTs to make early contact with the relevant law enforcement agency and to be guided by the authorities who have access to detailed and up-to-date knowledge of national requirements. Prospects for harmonisation of procedural law across Europe are distant.

4.2 Incident Response

4.2.1 Security Breach Strategies

It is important for an organisation to have robust, effective strategies in case of an information security breach. Unfortunately, the main objective of these strategies is to re-establish service and get systems and networks up and running as quickly as possible because of lost revenue, and this can mean that securing evidence is overlooked.

There are numerous aspects of a system which can provide evidence, such as intrusion detection systems (IDS), honeypots and honeynets, auditing tools, network traffic logs, access logs and tripwires. All of these need to be treated in the correct manner as to not damage or contaminate evidence.

The main priority for a corporation in the middle of a security breach is to restore systems to working order; *downtime means lost revenue, so preserving evidence is often neglected in favour of system restoration*.

From the security angle it is important to focus not only on computer solutions, as there are many aspects which should make up a robust information

security policy: from physical security to policy, and software and hardware solutions.

However, ensuring effective deployment of a comprehensive security policy across often fragmented, segregated units is challenging. Vulnerabilities are further heightened by the fragmentation of responsibility between various departments such as information and communications technology (ICT), legal and security, which can lead to neglect or oversight.

Some of the most glaring aspects of poor system administration are:

- poor password policy;
- poorly-managed data access controls;
- system and software patches not kept up-to-date;

The networks can prevent various challenges for law enforcement, as data relating to a single investigation can be located on numerous systems and networks.

Reliance on system administrators for assistance in providing information on network architectures, users and their privileges, logs and electronically stored information, is one of the main areas where private industry and law enforcement have to work together when an incident occurs. *This information is essential in order to outline criminal behaviour and to aid in locating the source.*

4.3 The Crime Scene

At the crime scene, the first person to respond usually is the system administrator who has detected the incident him/herself or because s/he has been alerted by someone in the company. Usually, the system administrator has to provide answers to the following questions.

- What shall I do now?
- Shall I proceed promptly in order to restart the system and avoid economic losses?
- How shall I preserve data for further investigation, with a view to locating the source?
- How shall I help the police when I report the incident?

However, at the beginning, a law enforcement representative is concerned mainly with standardising recovery procedures in case of incident. First, a person (usually the system administrator) has to be appointed as responsible and to be the point of contact. As soon as the incident has been detected, the system administrator and appropriate members of technical staff should follow preliminary guidelines.

4.3.1 Preliminary guidelines

These are as follows:

- locate the likely machine that has been attacked;
- take anti-contamination precautions: isolate the area close to the machine (nobody must access in the area around it or touch the machine;
- provide access logs (firewall and servers);
- freeze activities, whether possible – if not, try to fill a gap between those ones before the incident and after it (and keep the logs);
- in case the incident comes from inside the company, keep the logs which locate the machine.
- determine possible data lines that can reach the machine.
- isolate the machine from telephone lines (because data on the computer can be accessed remotely) – provide a possible password for access to the machine;
- compile a list of users who have access to the machine; and
- be prepared for a briefing session with the police.

4.4 Law Enforcement Briefing and Coordination

The joint team (first responders and the police) should consider the following points before commencing any examinations for digital evidence:

- prioritising: the urgency and priority of both the victim's and investigator's need for information, along with time constraints;
- other types of forensic examination which may have to be carried out on the same items above;
- which items can provide the most information in response to the various proposals?
- which items offer the best choice of target data, in terms of evidential value?
- the system administrator should provide the police with the architecture of the computer system;
- where the company is using an unknown operating system, provide assistance with supplying manuals (or a proper technician as point of contact who is aware of the functionality of the system);
- whether the machine should be removed, assuring an appropriate holding location is available for the technical equipment which is seized;

any decision need to be agreed during these activities.

In general, in a transborder or international incident, a CSIRT should inform the law enforcement authority of its own jurisdiction first, which will then coordinate with other law enforcement bodies.

4.5 Summary

Forensic computing is:
the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.

Key Principles

- Minimise handling of the original data set
- Account for any change
- Comply with the rules of evidence
- Do not exceed your own knowledge

Computer data is:
'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.'[17]

4.6 Computers and the Courts: General Challenges

Courts across the world continue to struggle with the submission of computer data as evidence. The fundamental question is the extent to which computer data can be treated as documentary evidence. The problem is that the data which can eventually be classed as evidence are volatile – they can be easily deleted or disappear. Furthermore, the highly complex nature of the data means that the risk of a case failing on poor evidence increases, as the evidence becomes more complex and fragmentary.

Procedurally, the main task and objective is to expedite the preservation of stored data.

[17] Convention on Cybercrime, Chapter 1 – Use of Terms, Article 1 – Definitions, available at http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (visited 18 June 2003).
[18] Recommendation No. R(95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Minister's Deputies), available at http://www.coe.fr/cm/ta/rec/1995/95r13.htm (visited 18 June 2003)
[18] Convention on Cybercrime, Chapter 1 – Use of Terms, Article 1 – Definitions, available at http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (visited 18 June 2003).

4.7 Admissibility of Electronic Evidence in Criminal Cases

4.7.1 General Principles Regarding Admissibility

Admissibility is governed by a set of principles that cover the following areas:

- the evidence must have been lawfully collected (i.e. it must be collected by means under the proper powers);
- the evidence must be collected in accordance with formal requirements (which may be contained within procedural law) to establish its reliability;
- evidence collection must respect safeguards (respect for privacy and the principles of a fair trial).

4.7.2 European Background to the Introduction of Electronic Evidence

Electronic material can be defined as any representation of text, sound, images, multimedia or programs that may serve as proof of facts in court. It is very vulnerable to loss or modification, is not directly readable and may require specific technical means for its collection.

Council of Europe Recommendation No. R(95) 13 was one of the first efforts at making a direct attempt to establish equality for digital evidence with other forms of documentary evidence under EU law.[18] Furthermore, parties to the Convention on Cybercrime should make it explicit in their own laws that information contained in digital or electronic form can be used as evidence before a court, regardless of the nature of the criminal offence.

4.7.3 When is Electronic Evidence Documentary Evidence?

There is a legal debate underway regarding the acceptance of digital evidence as documentary evidence. The legal rules for documentary evidence can be particularly strict, but leave many questions open. It is only with the advent of digital signature legislation, giving electronic material the same legal status as paper material, that several issues have begun to be addressed. In most countries, in the eyes of the law there is a big difference between the acceptance of electronic evidence as documentary evidence – where it is expected to 'stand on its own' and requires no context or interpretation by expert witnesses – and electronic evidence as supporting evidence (where independent explanation of its relevance is necessary). There is a debate whereby the law should be significantly altered in order to explicitly allow electronic evidence to be admitted under documentary evidence rules.

In any event, the crucial point is that the integrity and authenticity of material should be established in court. This requires standard techniques and methods for the collection, preservation and presentation of stored material. The technical means and methods should be subjected to independent testing and certification.

4.7.4 Other Electronic Material

Electronic material that is not readily admissible as documentary evidence may be classified into programs or software (computer code, etc) and images and sound files. Generally, this is not admitted as documentary evidence. It

may require some form of presentation technique or technology and other supporting documentation to explain its relevance. Similarly, the testimony of an expert may be required where detailed information about its collection, analysis and meaning must be provided.

4.8 The Impact of Privacy and Data Protection Legislation in Electronic Evidence Handling

If the collection and processing of electronic evidence is executed without due regard to privacy and data protection laws, then there is a real risk that the evidence will be inadmissible in court. There are a number of legal constraints operating at different levels.[19]

There are three main levels of applicable legislation that govern privacy and data protection constraints. These are:

(1) internationally-applicable legislation;
(2) supranational or regional legislation; and
(3) national legislation.

The full text of international and European supranational laws governing privacy and data protection can be found in Annex C.

With regard to international legislation, there are two main instruments: the 1950 European Convention on Human Rights and Fundamental Freedoms[20] and the 1981 European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[21]

With regard to supranational regional legislation, there is the overarching EU Charter on Human Rights and Fundamental Freedoms. Under the First Pillar, there are two EC Directives: Directive 95/46EC of 24 October 1995 on the Protection of Individuals with Regard to Processing of Personal Data and the Free Movement of Such Data,[22] and Directive 97/66EC of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.[23]

---

[19] Maria Veronica Perez Asinari, *Legal Constraints for the Protection of Privacy and Personal Data in e-evidence Handling', CTOSE Conference, 8–9 May 2003.*

[20] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms 1950, as amended by Protocol 11, available at: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=005&CM=8&DF=23/06/03 (visited 18 June 2003).

[21] Available at: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=23/06/03 (visited 18 June 2003).

[22] Available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (visited 18 June 2003)

[23] Available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett (visited 18 June 2003)

Third pillar activities (police and judicial cooperation in criminal matters) are also relevant for the collection and processing of evidence. These include the 1985 Schengen Agreement (the abolition of checks between borders of Belgium, France, Germany, Luxembourg and the Netherlands) and the establishment of Europol and Eurojust.[24]

With regard to national jurisdictions, each Member State will transpose directives (for example, on data protection) to its own law. Annex B provides a comparative review of national data protection legislation. There may also be laws governing sector-specific areas (for example, electronic signatures or traffic monitoring).[25]

4.8.1 Exemptions

Article 13(1) of 95/46EC states that:

> *Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:*
>
> *(a) national security*
> *(b) defence*
> *(c) public security*
> *(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; etc*.

Similarly, Article 8(2) of the European Convention on Human Rights and Fundamental Freedoms states:

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

4.8.2 Risks

There are three classes of risks for breaking any of these laws in respect of collection of electronic evidence:

(1) civil liability;
(2) criminal liability; and
(3) inadmissibility of evidence in court.

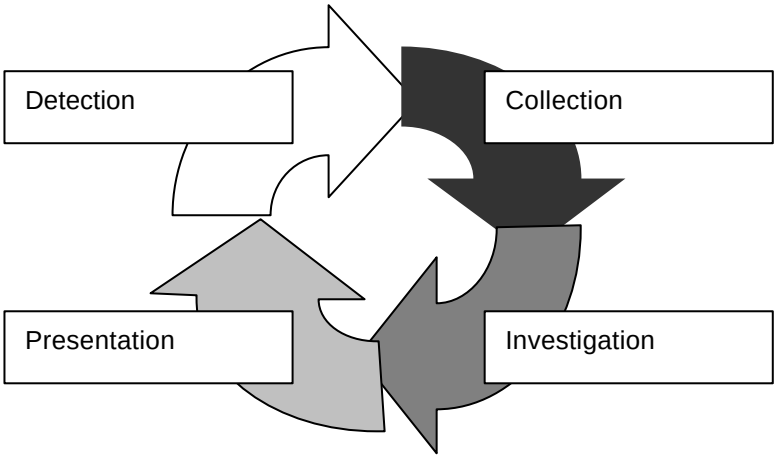
[24] Eurojust is a European agency which was set up in 2002 to enhance judicial cooperation and coordination. Europol was set up in 1992 to handle Europe-wide criminal intelligence.
[25] The UK's Regulation of Investigatory Powers Act 2000 is an example of legislation under which codes of conduct are being developed to regulate traffic monitoring.

4.9 Incidents: from the Computer to the Courtroom

4.9.1 Introduction

Computer users, CSIRTs, law enforcement and forensic experts share responsibility for taking a computer security incident from the stage at which it is detected through to successful prosecution (if required). The commonly accepted steps in this journey are shown in Figure 1.

Figure 1: Stages of a computer security incident through to prosecution



The following sections summarise the forensic activities that must take place at each stage of the journey and discuss the issues with which CSIRTs must deal.

4.9.2 Detection – Responsible Parties: CSIRTs and End-users

4.9.2.1 Alert: Via Technology or Other Means

An incident may come to the attention of the CSIRT or organisation staff in a number of ways. It may be flagged via an IDS (Intrusion Detection System) or other automated system, or a person might notice abnormal behaviour and report it. Heuristics and other advanced technology may come into play, where a system might be able to detect an incident before it occurs (although this is computationally complex), or algorithms that reflect biological systems might be used.

In any technologically-raised alert, it is crucial to consider the following elements:

- the systems might not be able to collect the data that they are designed to collect; and
- where data collection occurs, they may only be able to provide a partial data set, and this data itself may be flawed, erroneous or may have been already tampered with.

Of course, this also holds for the data collection phase. The detection phase may be more or less simple, depending on the level of technological sophistication and systems implemented inside the organisation. For

example, some document management systems and role-based security access will flag inappropriate access to files or resources. In terms of the human element, it may be possible to detect an incident via observation of activity regarding access to files or folders that are not required as part of the suspect's day-to-day activity. However, care must be taken in this instance, as it is very easy to infringe civil liberties and ruin any chances of a successful prosecution of the suspect. It is more justifiable if monitoring of suspicious activity on a system (especially if there are clear banners advertising this fact) is conducted as part of an organisation's information security policy.

4.9.2.2 Suspicion

This is concerned with the human element. In the context of any potential investigation, things to watch include the following.

- Did the person who first raised the alarm do so in a calm manner?
- How did the person judge when the incident turned into something serious?
- Were there standard thresholds applied, or was this an informal process?

This is essentially a risk assessment process and a question of the resources that the organisation is prepared to invest in incident response. Other issues include the following.

- If they are not part of a CSIRT, will the person taking the call note everything and, if so, how will this have an impact on normal business operations?
- Did he or she accidentally delete information at the time when logging the incident or when making authorities aware (e.g. by sending a file which may alter attribute information)?

'Pulling the plug' may preserve system continuity, but will make it more difficult to prosecute. The line between shutting-down (i.e. saving the system but with little or no chance of prosecution) and leaving it running (with the potential for more damage, but with the likelihood of being more successful in catching the attacker) is fine.

This decision might be down to a management decision or judgement call, or alternatively a formal threshold that is embedded in a list of CSIRT objectives. There is also the possibility that a number of apparently unrelated incidents may be connected. In this respect, it may be down to a sophisticated CSIRT to spot patterns or keep track of a number of incidents in the incident response system being used. Alternatively, in smaller organisations with little or no CSIRT capability, it might fall to those with adequate technical knowledge to see that several events are connected to the same incident or series of incidents.

4.9.3 Collection – Responsible Parties: CSIRTs and Law Enforcement

4.9.3.1 Monitoring

Physical and electronic monitoring is a difficult issue and it is usually best to allow law enforcement to conduct any activity, with technical advice being provided by the CSIRT. This is especially the case with regard to conducting monitoring operations on a network, as legislative requirements need to be met in order to ensure that the investigation is not jeopardised further down the line. The process often involves the acquisition of a warrant or court order which allows such activities to take place. Internally, within an organisation, monitoring may be slightly easier depending on the extent and rigour of any security policy. In any monitoring process, advice from both law enforcement and legal experts should be taken as (1) the activity may well alert the suspect that an investigation is being undertaken; and (2) the investigation must be undertaken with due regard to human rights and privacy. This means being aware of the legal landscape in whichever country the monitoring is taking place (and also perhaps the country where the monitors are located), as it is all too easy for an investigation to be let down by unlawful or illegal monitoring which then becomes an issue later in court. A matrix of relevant data protection legislation can be found at Annex C.

There are limitations to privacy if the suspect is using company property (hardware, software) but confusion in the current landscape means that legal advice must be taken. The technology for monitoring suspect activity on networks is of course similar to that for monitoring network activity generally, but care must be taken that all appropriate measures are put in place in logging each and every action, in order to ensure an accurate record of the activity. Timestamps are particularly important in this respect.

4.9.3.2 Seizure

Much has been written on the methodologies for searching and seizing an environment, specifically with regard to proportionality. However, with regard to seizure, there is a vast gap in any investigation between civil and criminal aspects. In the case of a criminal investigation, where law enforcement is involved, it may be necessary and appropriate to freeze the entire environment. Clearly, this has an impact on the rest of business operations. In the case of a civil case within an organisation, it may not be necessary to freeze the environment, merely to ring-fence the activities of the suspect to limit damage.

Other aspects of the seizure process are data production, a process which is more relevant with regards to remote network activity (e.g. in the case of an incident perpetrated via a service provider). This is a delicate mix of compliance with the law and management of a sometimes fraught relationship between the law enforcement organisation and the service provider.

It is quite likely that in the search and seizure process, when information and information systems change hands between the organisation or individual being investigated and the law enforcement authorities, a black hole or gap will occur. This is one of the most difficult parts of any investigation, as the

data and information systems must be frozen in a state as near to that which they were in when the investigation took place. The authority that has taken custody of the data must take great pains to ensure that it stays in this condition, lest it be declared inadmissible in court.

The question remains of how to go about freezing the environment. There is a clear need for a comprehensive approach in the planning of any investigation, in order to address the issue. All those conducting the search and seizure operation must know which rooms they will be entering, the location of the communication and server rooms and other relevant information. Within the bounds of the relevant legislation, suspects should be searched and all employees moved away from their computers and isolated from the working environment. A register of all computer equipment, including system manufacturer, device names, types, serial numbers, year of manufacture and details of external removable media and manuals should be made. Care should be taken to ensure that all the conceivable places that are likely to hide both information processing equipment and removable media are searched thoroughly.

4.9.3.3 Storage

In data collection, it is essential that what is collected can stand on its own, and that it does not require extensive expert interpretation (other than what is required for the purposes of a court) before submission as evidence. For example, alerts may be correctly raised by the system in the detection phase, but the evidence (log files, etc) does not show this without an expert piecing together separate bits of information to show the meaning of this information. Legally, this means that the evidence will stand up if an external expert witness is called.

Best practices in data storage require CSIRTs and law enforcement to preserve the chain of evidence. This may involve the use of an 'evidence locker', recording who has checked the evidence out, using an evidence book, proving an unbroken chain of evidence from the person who first identified the incident to the time it gets locked in the safe.

It may also be necessary to hash the electronic evidence to prove that it has not been tampered with. Further questions would include: whether to keep a backup or not; and whether to work on a separate image.

4.9.4 Investigation – Responsible Parties: Law Enforcement and Forensic Experts

4.9.4.1 Who?

The issue of who was responsible is extremely difficult to state categorically. An IP (Internet Protocol) address or MAC (Media Address Control) address will lead to a single computer, but it is then necessary to identify who was behind that machine at the time. This is markedly different, given the environment – in an academic or commercial network it is difficult to establish which user was at what keyboard. For an Internet Service Provider (ISP) this is less of an issue, as ISPs will record (but may not keep) records of the IP

address that has been assigned to a particular customer for billing purposes. The issue not only concerns motive but also capability – can the source identified have actually perpetrated the attack, and is it possible for the source identifier to be forged? In cases of internal investigation (e.g. a company with an intranet) it is possible for an IP address to be forged and obfuscation may occur at the internet access provider side (for example, with the use of NAT – Network Address Translation). In the case of a MAC address, this can also be changed – and frequently is – by many applications.

4.9.4.2 What?

To find out what has been done may range from an extremely easy assessment to something almost impossible to estimate. However, it is still easier than any of the other investigative issues mentioned in this section. For example, rendering an e-commerce site inaccessible for a period of time results not only in losses to transactions being completed at the time, but also to any transactions that would have occurred during the time that the site was offline, as well as future transactions which did not occur as customers viewed the site as unreliable or untrustworthy. Further, there may be costs involved with employing computer software or hardware experts to get the system back online again, as well as loss of reputation.

Some experts break these into soft, semi-soft and hard costs. It is important to note that, in conducting forensic examinations, several different incidents may have occurred with a number of different types of data, ranging from text files and cryptographic keys, to databases (and the data within them) and program files. The need to estimate direct and indirect costs is paramount and may form the basis for any monetary claims to be made in a civil case.

4.9.4.3 Why?

This is where the role of the civil or criminal investigative specialist comes into its own. Determining the 'why' is out of the scope of this report, but it must be borne in mind that a suspect must have the knowledge, skills and attributes – as well as the motive and opportunity – to commit any offence. The legal term for this is known as *male fide* ('in bad faith'), and it is advisable to let law enforcement experts undertake this aspect of the investigation.

4.9.4.4 When?

When the incident actually happened is one of the most difficult issues to resolve. Notwithstanding any disparities that might occur with time zones, it is important to establish in the investigation phase that the system clock used on affected computers has not been tampered with. In a best case scenario, each system activity or process will have been logged by an external computer that is independent of any of the affected systems (this includes systems that are used as a conduit in the incident). SysLog is a good example of such an external system. An even better solution is that the log is kept on a dedicated appliance and the time and date is authenticated by a trusted third party using a trusted service provider. This means that it may be possible to state that, according to the logs, the time that something apparently happened was indeed the time it actually happened. The worst case scenario would be

where the log is on the affected machine, as it would be comparatively easy for the suspect to alter the system time.

4.9.4.5 How?

See the list of incident classifications. This is ultimately one of the factors that will tie an incident to a crime prosecutable by the criminal law or code.

4.9.5 Presentation – Responsible Parties: Law Enforcement and Forensic Experts

4.9.5.1 Evidentiary Principles

The principles of the law of evidence in European criminal cases are the fact that the burden of proof (obligation to prove) rests on the prosecution, while the weight of evidence is related to the relevance of the provable elements. One definition of evidence is:

> *Any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present or future existence or non-existence of the other.*[26]

The question of relevance is open to interpretation by the judge. Other issues to bear in mind are the volatility and fragility of electronic evidence and its intangible nature. However, electronic evidence is also more plentiful and reliable due to its automated nature. This highlights the important role of the expert witness in explaining electronic evidence to the court.

Admissibility (validity) is established by a judge. Evidence that has been gathered illegally must be ruled out. While it is not that difficult to collect electronic data, doing so legally – ensuring that it is valid and can be fully admissible – is a different case. The circumstances of collection are extremely important.

It is fundamental to ensure that the court is in no doubt about the chain of custody. This can be addressed by complying with principle of the chain of custody, i.e. keeping a record of who had control of the electronic material from the moment of collection until presentation in court: where, when, why and in what form it was preserved or transferred to other persons, and finally, what processing has been done in relation to the material.

4.9.5.2 Evidential Systems

The three systems of evidence in use in Europe are: *positive–legal* or formal; *negative–legal,* and *informal* (or free).[27]

Positive–legal

- law defines the means of proof;

[26] Olivier Leroux 'Overview of Legal Aspects, E-Evidence and Data Protection' CTOSE Conference, Namur, 8–9 May 2003.

[27] Henrik W.K. Kaspersen, 'Admissibility of Electronic Evidence', CTOSE Conference, Namur, 8–9 May 2003.

- evidentiary value defined by law;
- if a certain number of means of evidence are present, then proof has to be assumed; and
- little room for interpretation by jury or judge.

Negative–legal

- law defines the means of evidence;
- minimal rule: proof may be assumed if a minimum number of means of evidence is available; and
- law may prohibit some certain means of evidence.

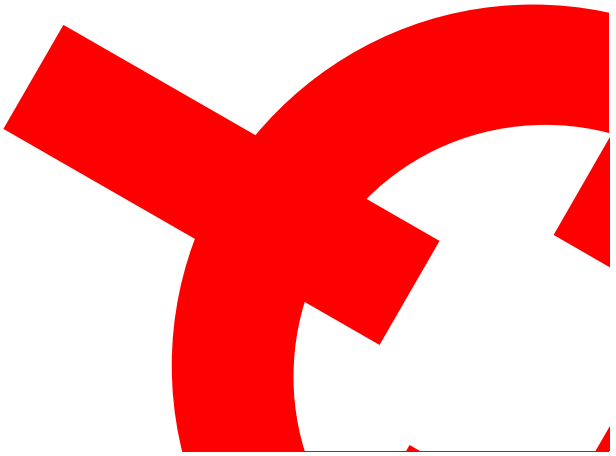
Informal (or free)

- no legal rules about admission of evidence: case law applies;
- no rules beyond evidentiary value; and
- evidence proves beyond reasonable doubt.

Although legal and evidence systems exist in Europe, there are often precise prescriptions of collection methods that will ensure reliability in court. Therefore, in this context it is extremely important that CERTs/CSIRT personnel interact with the local law enforcement authorities in order to develop a more detailed understanding of the intricacies of digital/electronic evidence in prosecuting computer-related criminal activities.

Chapter 5

Incident Survey



Chapter 5: Incident Survey

5.1 Introduction

The aim of this task was to report on the prevalence and impact of computer security incidents in EU Member States from 1 January 2000 to the time of this report completion, based on existing surveys. The intention is to analyse critically existing surveys in order to prepare the way for improved European-level incident data collection and analysis.

In the past few years, there has been an increase in press, government and industry reports about computer crime and information security breaches and incidents. Although these have played a pivotal role in fostering general awareness about information security, little information has been provided concerning the methodological processes that are employed in developing these surveys. Therefore, in this section, the focus is on surveys where it is possible to ascertain those methodological processes.

5.2 Law Enforcement Surveys

The collection of incident data by the law enforcement agencies of EU Member States is ad hoc and uncoordinated, leading to a lack of pan-European statistics on the level of computer crime. Even when systematic data collection processes are implemented, there does not seem to be a correlation between the notion of 'incident' and its legal and operational connotations. This is primarily due to the fact that law enforcement agencies tend to describe facets of computer and computer-related crime in different ways. Therefore, they may collect data on computer crime, content-related criminal activities and telephone and postal frauds. This mix of activities results in the development of different data collection methodologies. This is evident in the following three cases of law enforcement organisations that are involved in collecting incident-related data.

5.2.1 Italy – Polizia Postale e delle Comunicazioni

Italy has three main law enforcement bodies (Guardia di Finanza, Arma dei Carabinieri, Polizia di Stato). Despite the fact that each one is – in theory - entitled to fight any kind of crime, the Guardia di Finanza is more focused on the financial crimes, while Carabinieri (that also work as Military Police and Counterintelligence) and Polizia di Stato operations are often similar.

Each body has a special computer crime branch. The Gruppo Anticrimine Tecnologico belongs to the Guardia di Finanza, the Raggruppamento Carabinieri Investigazioni Scientifiche (Ra.C.I.S) to the Carabinieri while The Polizia Postale e delle Comunicazioni,[28] is the branch of Italy's Polizia di Stato, in charge offighting online child pornography, telephone fraud, illegal trespass and cracking activities. This mix of activities is evident in its monthly operational statistics.[29] These indicate the police unit's intervention to counter illegal activities carried out through telephone systems, radio, television,

[28] http://www.poliziadistato.it/informatica/ (visited on 10 June 2003).
[29] These are available on a monthly basis at:
http://www.poliziastato.it/pds/online/postale/postale122002.htm (visited on 10 June 2003).

postal systems and IT systems. In addition, an overview of the financial penalties and fines is also presented, although there is no differentiation according to specific criminal activities. In July 2002, the Polizia della Comunicazioni issued its annual statistics: these focused only partially on issues associated with cracking or other computer crimes, such as illegal access to computer systems and malicious code writing. In 2001, this section of the Italian national state police undertook 152 investigations related to 'hacking' activities that led to the prosecution of over 8,000 people and 70 references to foreign police forces.[30]

Despite the above mentioned figures related to the investigations, the computer-crime related cases actually prosecuted and judged are still a few. Apart from strictly-defined computer-crime court cases, a relevant amount of Court decisions (often settled in pre-trial stages) is mainly related to minor copyright infringement, sat-TV card cloning and online child pornography pictures exchanging.

5.2.2 France – Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communication

A similar approach is undertaken by the Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communication, which is part of the Direction Général de la Police Judiciare in France. The operational task of this unit involves many of the possible criminal activities that can be undertaken with the use of ICT. Its statistics are produced as part of a general report on economic and commercial crimes in France.[31]

5.2.3 Germany – Bundeskriminalamt

Unlike the two previous cases, the German Bundeskriminalamt (BKA) collects detailed information about computer-related data and subdivides them according to the crimes that are outlined in the federal German Criminal Code. For example, in 2002 there were 1,327 cases of computer sabotage. At the same time the statistics indicated that, in 2002, there were 1,947 cases of software piracy.[32]

5.2.4 UK – National Hi-Tech Crime Unit

In the UK, the National Hi-Tech Crime Unit (NHTCU) is a multi-agency law enforcement group that is tasked to tackle problems raised by the use of computers and the Internet for criminal activity. Pulling together personnel and resources from the National Crime Squad, National Criminal Intelligence

---

[30] Barbara Ferraris di Celle (2002) 'Chi ci protegge dai Crimini Informatici: Intervista con il Direttore del Servizio Polizia Postale e delle Comunicazioni' ('Who Is Protecting Us from Computer Crimes?', interview with the head of the Italian Police for Postal Services and Communications), *ICT Security* (July): 49–51, available at http://www.ictsecurity.it (visited on 27 July 2002).

[31] For more information, see 'Direction General de la Politie Nationale, Crime et Delits Constantes en France en 2002' available at: http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c31_actualites/2003_01_13_delinquance/conference.pdf (visited on 10 June 2003).

[32] These statistics originate from Bundeskriminalamt (BKA), *Polizieliche Kriminalstatistik 2002* available at: http://www.bundeskriminalamt.de/pks/pks2002/index2.html (visited on June 2003).

Service (NCIS), HM Customs & Excise and computer crime units in police forces and other law enforcement agencies, NHTCU subdivides cybercrime into existing and new offences categories. In 2002, NHTCU released a report based on a survey which was carried out over multiple phases, using face-to-face interviews and a structured questionnaire to accumulate data. The survey was conducted by NOP (the leading polling group in the UK) and evaluated 105 firms, 97% of which reported some kind of high-tech attack. The report found that more than 3,000 incidents were reported, with virus attacks accounting for 43.5% of the total. Hacking and denial of service attacks accounted for 20% and employee sabotage of data and networks were also particular problems.[33] These findings were consistent were also particular problems. These findings were consistent with the patterns and themes founding with the Department of Trade and Industry (DTI)'s 2002 report, *Information Security Breaches Survey*.

5.2.5 Summary

In sum, the data from these surveys reveals that cybercrime is a topic that European law enforcement agencies and businesses take seriously. Nonetheless, there are three significant factors impeding the efficient analysis, investigation and prosecution of cybercrime:

(1) the lack of a common approach among European law enforcement agencies in assessing or tackling the problem;
(2) the fact that companies are unaware of the range of services that law enforcement can provide in response to cybercrime; and
(3) cybercrime's coverage of a broad range of social, business and technological spheres at national and international levels.

These findings suggest that international collaboration at EU level, a multi-agency approach to investigating and prosecuting these crimes, and an advertising campaign that targets business and industry, could improve the factors contributing to these problems.

5.3 Other Surveys

Law enforcement authorities focus on protecting society from criminal activities. Therefore, it is not their primary role to undertake analysis and assessment concerning the socio-economic and legal extent of computer crimes. This activity is primarily undertaken by industry organisations or research organisations.

5.3.1 United Kingdom – Department of Trade and Industry

Every two years the DTI, in partnership with specialised consultancy organisations, undertakes a survey of information security breaches affecting UK-based public and private organisations. The last survey was published in April 2002.[34] A quantitative survey using a structured questionnaire across a

[33] NOP World and NHTCU (2002) *High-tech Crime: the Impact on UK Business*.
[34] PriceWaterhouseCoopers and Department of Trade and Industry (2002) *Information Security Breaches Survey 2002: Technical Report* (April), available at: http://www.security-survey.gov.uk (visited 10 June 2003).

range of organisations is the core of this activity. The questionnaire is supplemented by telephone or face-to-face interviews with information security experts. The end result of this exercise is a comprehensive overview of the state of 'information security' in the UK.

This survey begins with an assessment of the way that organisations are embracing IT as part of their operational and strategic activities. It is followed by an assessment of business executives' attitudes towards information security. The core of this survey is the collection of data concerning the number of security breaches that are suffered by British companies. The findings involve data concerning the proportion of UK-based business that have suffered security incidents, as well as their cause and origin. Particular attention is paid to specific areas, such as the types and costs of security breaches, organisations' incident response and crisis management capabilities, implementation of information security management processes and the use of insurance policies to counter monetary losses associated with incidents.

The survey exercise examines the issues associated with the impact of security breaches on organisations' compliance with specific legislation, such as data privacy. It also provides an assessment of the future challenges to be faced by organisations in their management of the risks and threats that are associated with the use of information technologies and processes.

Notwithstanding some of the positive information brought forward by this survey, it does have limitations. The survey does not link a specific security breach to a specific criminal offence. Moreover, its approach towards information security is too broad, since it includes, as security breaches, issues such as access to illegal material by employees. As in the case of some EU Member States' law enforcement organisations, this lack of differentiation between individual security breaches and incidents leads to difficulties in cross-national comparisons of data.

5.3.2 France – Club de la Securité des Systèmes d'Information Français

In France, the Club de la Securité des Systèmes d'Information Français (CLUSIF), a not-for-profit organisation bringing together over 600 companies and organisations with an interest in information security, has been undertaking an assessment of the state of information security in the country for the last three years. Its most recent report was released in April 2003, based on data from the previous year. In addition to the overall findings, one of the most interesting aspects of this survey is the constant evolution of its methodology.[35] The first two surveys did not involve public sector organisations, while responses were subdivided according to geographical criteria. These two approaches were discarded for the most recent edition, when CLUSIF undertook an assessment of the state of information security among public institutions. Data collection is undertaken through surveys sent to selected individuals via fax. Nevertheless, responses are often provided via

[35] CLUSIF (2002) *Etude et statistiques sur la sinistralite informatique en France – Annee 2002*, available at: http://www.clusif.asso.fr (visited on 10 June 2003).

telephone due to respondents' concerns about the confidentiality of information.

Compared with the survey undertaken by the DTI, CLUSIF's survey is more comprehensive. The results are subdivided by industry sector, as well as by the IT/Internet presence of a company, its size and activities. However, as with the DTI survey, the report fails to differentiate between content-related crime, computer-related crime and other forms of criminal activities (i.e. fraud) that are undertaken through information technologies and the Internet. CLUSIF espouses a comprehensive approach to information security.

5.3.3 Italy – Associazione Italiana per la Sicurezza Informatica

Along the same lines as CLUSIF, Associazione Italiana per la Sicurezza Informatica (CLUSIT) has undertaken an annual survey which is aimed at assessing the state of information security in Italy.[36] Based on a telephone survey of 500 Italian companies and public organisations, this investigation seeks to evaluate issues such as level of information security investments, employee awareness and risk perception. A specific section is dedicated to providing data and information about security breaches ranging from viruses and hacking to access to illegal content. As with the two previous cases, there has been a failure to appreciate the need to differentiate between various forms of 'computer crime'.

5.3.4 United States – US Computer Security Institute and Federal Bureau of Investigation Survey

Perhaps the most established annual information security and computer crime survey is that carried out by the US Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI).[37] Although it is a US exercise, its data and findings are often used in Europe to describe the level of risks and information security in public and private organisations. As with the other cases mentioned here, the findings of this activity are based on a survey of US-based organisations of different sizes and commercial turnover. Among its questions, the Computer Security Institute requests organisations to provide data on annual losses that are related to security breaches. As indicated in the overview section of the final report, the authors draw attention to the 56% decrease in annual losses in 2003, clarifying that the amount of loss – US$201,797,340 – represents the 'total losses reported by a specific number of organisations (251) and [that it] is not any kind of more broadly extrapolated total'. Although the end result might prove useful, this approach has methodological shortcomings, including the limited number of respondents and the failure to factor into the analysis the use of mitigating instruments, such as insurances.

5.3.5 Basel Agreement for Capital Provision (Basel II)

Over the last three years, there has been increased attention amongst information security experts about the possible impact of the new Basel Agreement for Capital Provision (commonly known as Basel II), which was developed under the auspices of the Basel Committee on Banking Supervision. As part of its activities, the Committee, which brings together the central banks of the 10 most developed nations, has undertaken a data collection exercise which is aimed at the provision of information on individual operational losses. Following the first two exercises in 1998 and 2000, the Committee has now completed a survey of 89 banks. This survey does not focus exclusively on IT risks such as computer-related activities; these are just some of the many operational risks that banks needs to take into

[36] SIRMI SpA and CLUSIT (2001) *La Sicurezza nelle Imprese Italiane*, November.
[37] CSI and FBI (2003) *Computer Crime and Security Survey 2003*, available at: http://www.gocsi.com (visited 10 June 2003).

consideration when calculating capital allocation to cover the potential fall-out of these risks.[38]

The survey concluded that most of the losses relating to operational risks occur in retail banking operations and involve external fraud, leading to total losses of US$787.1 million. Nevertheless, it is important to emphasise that the category of 'external fraud' includes computer crime. According to the survey, computer crimes such as hacking comprised only 66 incidents, which represents 0.14% of the individual losses during events that were experienced by the 89 surveyed banks in 2001, causing overall losses of approximately US$11 million. However, the survey does not appear to have specific categories in place to identify issues such as incidents caused by internal, disaffected employees or improper business and market practices. However, there is data on business disruptions and system failures. It is interesting to note that these represent 1.1% of total events, causing cumulative losses of approximately US$187 million.

Notwithstanding some of its shortcomings, the results of this survey emphasise the importance of detailed legal and operational definition of incidents and other IT-related risks. Moreover, they also indicate that regulatory and supervisory agencies are best placed to undertake this detailed analysis, so long as they provide full anonymisation. These institutions have the legal and regulatory clout to encourage reluctant commercial organisations into providing detailed information about the incidence of IT risks, including incidents involving computer crimes such as hacking and denial of service.

5.3.6 Statistical Indicators for Benchmarking the Information Society (SIBIS)

The previous surveys were mainly designed to assess the information security status of public or private organisations. Increasingly, individual users are becoming the main target of incidents and computer-related crime through viruses and denial of service attacks. In order to undertake a survey of their experiences, specific investigations need to be made. One example is represented by the EU-funded project Statistical Indicators for Benchmarking the Information Society (SIBIS). As clearly stated by its title, the objective of this project is to develop statistical indicators to measure the development of the European information society. Among several topics, particular attention has been directed to examining users' approaches to, and perceptions of, information security.

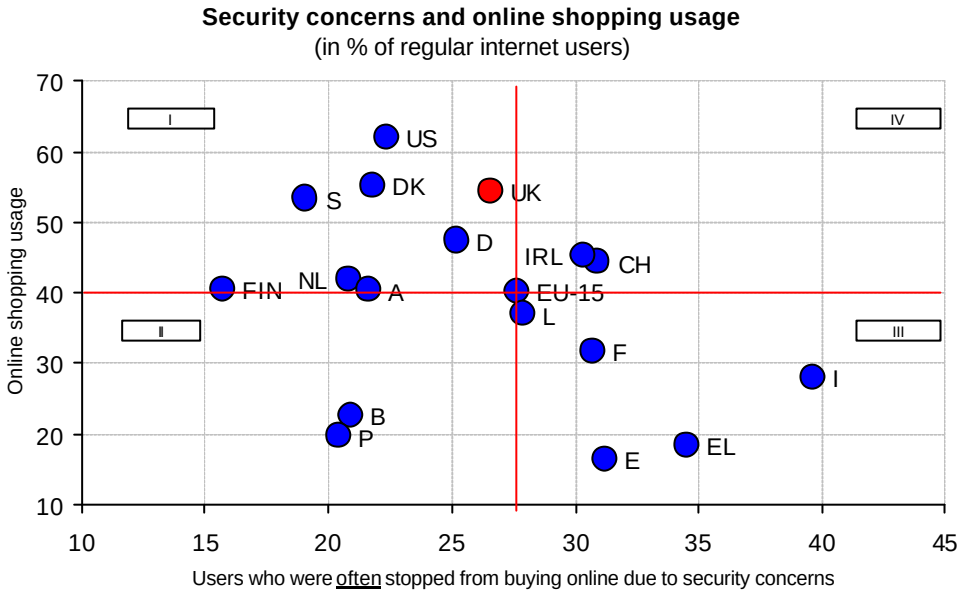
In order to achieve this objective, specific questions about concerns relating to information security and their impact on online activities, as well as willingness to report incidents, formed part of the survey. The project conducted over 11,832 telephone interviews with individuals aged 15 years and over in private households from all EU Member States and associate states. The results of

[38] Basel Committee on Banking Supervision and Bank for International Settlements, Risk Management Group (2003) *The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected*, March, available at: http://www.bis.org/bcbs/publ.htm (visited on 10 June 2003).

the findings related to the field of information security confirm how security threats may undermine the development of e-commerce and e-government, due to individuals' fear and lack of trust. However, it also revealed individuals' willingness to report incidents if provided with the necessary information.

Notwithstanding these achievements, the SIBIS exercise also highlighted the difficulty of undertaking these kind of exercises, due to the challenges for non-technologically 'savvy' individuals in understanding the differences between incidents and other cases of criminal activity, or behaviour that has been enhanced by the pervasiveness of the Internet and IT.

Figure 2: Security concerns and online shopping usage



5.4 Issues Associated with the Quantification of Computer Crime and its Financial and Legal Implications

5.4.1 Introduction

The previous section presented an overview of the most visible surveys that address issues related to computer crime. Particular attention has been devoted to highlighting the different methodological approaches used. The goal of this exercise was not to question their usefulness in assessing the current state of information security in both the public and private sectors, but to suggest the need to develop more advanced and detailed approaches in collecting and analysing computer crime-related statistics and, at the same time, assessing their financial implications.

The most visible shortcoming of these survey exercises is their failure to focus data collection comprehensively, according to legal definitions of offences against the confidentiality, integrity and availability of computer data and systems, which leads to the impossibility of undertaking comparative analysis. Primarily, this is due to the fact that these surveys aim at providing an overarching view of the state of information security 'preparedness' and awareness of overall IT-related risks. Moreover, it is also important to

emphasise that most of these surveys are targeted towards information security experts and/or general business and IT managers, whose knowledge of the legal intricacies of computer crime is limited or, more often, outside their professional competences and responsibilities. Their interest is directed more towards examining information security trends and evolution and implementing the necessary changes or identified best practices within their organisations.

The remaining section of the analysis focuses primarily on examining the three main survey activities that were undertaken by CLUSIF, DTI and US CSI/FBI. Their objective is to provide a quantitative and qualitative measurement of the impact and extension of IT risks, which include computer crime inside public and private sector organisations. The exclusion of the other surveys is justified by the fact that those undertaken by police forces aimed primarily at examining the state of criminal activities; they did not engage in assessing the financial implications of these activities. The surveys by SIBIS and BASEL II approach the issues of computer crime as part of a larger policy or regulatory effort. The goal of SIBIS was to develop statistical indicators for measuring the European information society and in this context, attention has been given to some aspects of computer crime, such as viruses and hacking, as a starting point in order to examine whether these activities are undermining the development of a European information society. Similarly, BASEL II examines activities such as computer crime as one of the many instances and situations that need to be taken into consideration when calculating the capital charge to counter operational risks.

5.4.2 France – CLUSIF

The annual survey undertaken in France by CLUSIF has a specific section which is dedicated to assessing the kind of IT-related damages that affected French organisations. The survey revealed that, in 2002, 26.3% of French organisations suffered 'data interference', as they were affected by computer viruses, while 0.3% experienced 'illegal accesses' or activities commonly described as 'intrusions'.

In both cases, this survey fails to assess the various different aspects of both 'illegal access' or 'data interference'. In particular, it does not specify issues such as intrusion attempts, targeted fingerprinting, unauthorised access to communication systems or unauthorised modification of information. This limitation becomes even more evident in the case of a specific statistic, suggesting that 2% of the surveyed organisations have suffered so-called 'attacks to encryption tools'. In this case, it is possible to consider data and systems interference situations, as well as illegal access and interception.

Notwithstanding these limitations, it is important to emphasise that the CLUSIF survey specifies the number of users affected by specific IT-related risks, in particular malicious codes and viruses. CLUSIF indicates that computer viruses affect 35% of service industry and only 13.5% of telecommunication companies. In terms of the operational impact of computer viruses, only 15% of the surveyed organisations indicated that these malicious codes had a severe impact on their activities. The rest had limited or average

operational implications. Finally, in terms of financial implications of all IT risks, the survey concluded that 86% of the surveyed organisations had been able to counter their financial implications without needing to resort to insurance or external financial measures. However, what is more disturbing is the fact that only 2% had taken legal action. No detailed analysis differentiating IT risk or even computer crime had been undertaken.

5.4.3 UK – DTI

The biannual information security survey undertaken by the DTI suffers from some of the limitations which were uncovered in the CLUSIF survey exercise, although at a different level. As with the CLUSIF survey, the objective of the DTI's activity here is to provide a picture of the overall status of information security in the UK. In particular, the survey has unveiled that fact that virus infections are by far the largest number of security incidents, affecting approximately 41% of commercial organisations. At the same, the survey reveals that 14% of organisations have suffered unauthorised access, which includes hacking attacks on websites. Although it has not been possible to access the interview protocol that was used while undertaking this survey, an examination of the results clearly indicates that the researchers have tried to link their data collection to specific legal definitions of computer crime, especially in the case of unauthorised access. However, it is also interesting to note that this survey does not appear to have taken into consideration cases such as 'illegal interception of data' (as has been done by CLUSIF), or issues such as denial of service as a 'system interference'.

The most interesting aspect of the UK survey is its extensive analysis of the financial implications of computer crime, or so-called 'security breaches'. This exercise concluded that most security breaches result only in minor costs, with two-thirds of the most serious incidents incurring less than UK£10,000 to resolve. However, there have been some businesses that have suffered damages of over UK£500,000 following an individual security breach. The survey concludes that, on average, security breaches in the UK cost approximately UK£30,000. This detailed quantification of the financial implications of security breaches is then paralleled by an analysis of specific post-event actions. The survey indicates that over half of the organisations that were affected by a security breach did not pursue legal action since the event was not that serious, while 20% considered that 'no laws' had been broken. In addition, quite interestingly, the survey indicated that 8% of the organisations did not know whom they needed to pursue.

The DTI survey also provides an assessment of the use of insurance to cover the potential financial losses associated with security breaches. It concluded that approximately 44% of organisations are covered through insurance. The rest are either positively sure that they are not covered, or they do not know.

As aforementioned the UK survey is, in part, more comprehensive than that undertaken by CLUSIF. However, it also suffers from a partial lack of assessment of all forms of computer crime. Its primary focus has been on unauthorised access and data or system interference through viruses or other

malicious codes. Despite this, the analysis of the financial implications of these security breaches is relatively comprehensive.

5.4.4 CSI/FBI Survey

Several weaknesses that were indicated in both the CLUSIF and DTI surveys are overcome partially by the CSI/FBI survey. One of its strengths is the strong focus in identifying the types of so-called 'attacks' or 'misuses' that have been detected by organisations during 2002. Among the categories, the surveying organisations make specific references to situations such as:

- denial of service;
- active wire-tapping;
- unauthorised access;
- unauthorised access by insiders;
- viruses;
- insider abuse of Internet access;
- system penetration; and
- sabotage.

Among these categories, some cases such as denial of service, system penetration and viruses can be related directly to particular legal definitions of computer crime. Nevertheless, the situation is more complicated for situations such as active wire-tapping or telecom eavesdropping, which can be conceived to be unauthorised access to transmission or information. It is also possible to consider these to be illegal access if they happen to involve penetration of a protected, closed network via a 'sniffer' or other tool.

The most interesting aspect of the CSI/FBI survey is the specific financial quantification of individual, so-called 'attacks'. During 2002, denial of service attacks have led to losses of over US$65 million, while viruses account for over US$27 million in losses. Notwithstanding this, it is important to emphasise that these data do not provide the full picture, since only 47% of respondents could actually quantify the financial implications of computer crime.

The survey engages in an interesting differentiation between IT systems and websites, as the two elements are separate. However, in legal terms it is safe to say that denial of service against an information system may lead to the same legal consequences as similar illegal activity against a website, although the situation changes in the case where the computer crime has been directed towards a critical public IT system.

5.5 Conclusion

This analysis of the major survey activities related to computer crime clearly indicates the need for a set of standardised definitions of the various aspects of such criminal activities. The framework presented in this report can provide a useful base, since it provides standardised definitions of specific forms of computer crime. By structuring collection of data along specific legal definitions of these criminal phenomena, it would be possible also to

undertake comparative analysis, due to the similarity of the units of analysis. Finally, harmonisation of definitions would assist in assessing the specific financial impact of individual sets of computer crime.

Section 2

Country Data

Section 2:
Country Data[39]

[39] A number of alternative national reporting mechanisms deal specifically with illegal content (exploitation of children, race hate and e-Commerce fraud) and are frequently funded by the European Commission Safer Internet Action Plan

Austria

Austria has a civil law tradition. All jurisdiction in Austria proceeds from the Federal Republic and all verdicts and findings are proclaimed in the name of the Republic. There is no binding case law – all law is created by legislative bodies.

There are two public law courts in Austria; the Constitutional Court (Verfassungsgerichtshof) and the Administrative Court (Verwaltungsgerichtshof).

Civil and criminal matters are heard in the ordinary courts. Civil matters up to €10,000 are heard in the District Court (Bezirksgericht) with appeal to the Regional Court (Landesgericht). Claims worth more than €10,000 go straight to the Regional Court. Appeal from the District Court can be made to the Regional Court and from there to the Supreme Court (Oberster Gerichtshof). If the Regional Court is the court of first instance, an appeal is heard by the Court of Appeal (Oberlandesgericht) and then by the court of final instance, the Supreme Court.

Criminal prosecutions are brought by the Public Prosecutor's office, which is independent of the court system. Offences for which the statutory punishment does not exceed one year's imprisonment are heard in the District Court with appeals heard by the Regional Court. If the sanction is greater than one year's imprisonment, cases are heard in the Regional Court with appeal, generally, to the Court of Appeal. There is no court of third instance for criminal matters.

The Directorate General for Public Security is part of the Federal Ministry of the Interior and is divided into four groups: Federal Police, Supreme Command of the Gendarmerie, State Security and Criminal Investigations – Interpol. All federal law enforcement bodies are subordinate to the Ministry of the Interior.

According to the Federal Constitutional Act the term law enforcement officers refers to "armed or uniformed formations or other formations of military character organised to carry out police tasks". This includes the federal police, the federal gendarmerie and the Criminal Investigation Department. There are eight federal gendarmeries, ie one for each Land apart from Vienna.

Legislation

Privacy Data Act 2000: art 15, art 26, art 52

The Confidentiality, Integrity and Availability of data in Austria are managed through the Privacy Data Act 2000 (DSG2000). It that deals specifically with personal data but is relevant to some of the CIA Offences listed in the CSIRT Taxonomy.

Art 52 of the DSG2000 deals with the administrative penalties, providing for a

fine, for anyone who intentionally and illegally gains access to a data application [*Datenanwendung*] or maintains an obviously illegal means of access, or transmits data intentionally in violation of the rules on confidentiality (sect. 15 of DSG2000), and in particular anybody who uses data entrusted to him according to sect. 46 and 47 of DSG2000 (“*Scientific Research and Statistics*” and “*Transmission of Addresses to Inform or to Interview Data Subjects*”) for other purposes.

A fine may also be levied on anyone who intentionally erases data in violation of sect. 26 par. 7 of DSG2000 (Right of Information). Art. 52 also provides for punishment for attempts to undertake illicit conduct.

No other CIA Legislation is available.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting				
Malicious Code				
Denial of Service				
Account Compromise	Art 52 DSG2000: it is an administrative offence to illegally gain access to a data application or to maintain an obviously illegal means of access, or transmit data intentionally in violation of the rules on confidentiality	An administrative fine		
Intrusion Attempt	Art 52 DSG2000: it is an administrative offence to illegally gain access to a data application or to maintain an obviously illegal means of access, or transmit data intentionally in violation of the rules on confidentiality	An administrative fine		
Unauthorised Access to Information	Art 52 DSG2000: it is an administrative offence to illegally gain access to a data application or to maintain an obviously illegal means of access, or transmit data intentionally in violation of the rules on confidentiality	An administrative fine		
Unauthorised Access to Transmissions				
Unauthorised Modification of Information				
Unauthorised Access to Communication System	Art 52 DSG2000: it is an administrative offence to illegally gain access to a data application or to maintain an obviously illegal means of access, or transmit data intentionally in	An administrative fine		

	violation of the rules on confidentiality			

Forensics

Reporting & Law Enforcement Organisations

Federal Ministry of Interior, Group D– Interpol, Department II/16-ITB
Liechtenwerderplatz 5,
1090 Vienna,
Austria
T: +43 1 5125622
F: +43 1 53126 4329
W: www.bmi.gv.at

Federal Ministy of the Interior - State Police Service
Minoritenplatz 9
Vienna
Austria
T: 0043-1-53126-0
F: 0043-1-53126-3739
W: www.bmi.gv.at
E: staatspolizei@mail.bmi.gv.at

Datenverarbeitungsregister (Data Processing Registrar)
Hohenstaufengasse 3
1010 Wien
AUSTRIA
T: (+43 01) 53 115 / 4043
F: (+43 01) 53 115 / 4016
E: dvrpost@bka.gv.at
W: www.bka.gv.at/datenschutz/

Office of the Data Protection Commission
An das
Büro der Datenschutzkommission
Ballhausplatz 1
1014 Wien
AUSTRIA
T: +43 1 531 15 / 2525
F: +43 1 531 15 / 2690
E: dskpost@bka.gv.at

Other Reporting Mechanisms

Arge Daten is a private organisation in Austria providing alerting services to Austrian consumers regarding data protection issues.[40]

STOPLINE is a platform for users that stumble over illegal material on the Internet. The matters dealt with are solely child-pornography and neo-Nazi content.[41]

[40] http://www.ad.or.at

[41] www.stopline.at

Belgium

Belgium is a federal state with a civil law system. Its legal tradition has been greatly influenced by the French legal system.

There are five codes which form the basis of Belgian law: Code civil, Code de commerce, Code penal, Code d'instruction criminelle and Code judiciaire.

Criminal procedures are set out in the Code of Criminal Procedure (1867). The Tribunal de Police is the lowest level court dealing with criminal matters (prior to which preliminary investigations will have been dealt with by an Examining Magistrate and a Public Prosecutor). The next level of court is the Tribunal Correctionel. More serious crimes are dealt with by the Cour d'Assises, the only Belgian Court to have a jury.

Civil procedures are set out in the new Code of Civil Procedures (1967). The lowest level court for civil cases is Tribunal des Juges de Paix. The majority of civil cases go straight to the Tribunal de Premiere Instance.

The Cour d'Appel may hear civil and criminal case appeals from the lower courts. The final court of appeal, on points of law only, is the Cour d'Appel.

The police consist of the Local Police and the Federal Police. There are 196 local police forces engaged in community policing. The federal police came into being on 1 January 2001. They are involved in areas such as criminal investigations, fraud investigations, national security, coordinating royal protection and cooperating with foreign police forces as well as with the Local Police.

Legislation

art. 550 (b) sec. 1, 2, 6 – art 523 – art 528 – Law on the 1934 Law on the Transmission Lines - Law on the Reform of Certain Public Institutions

In November 2000 the Belgian Parliament adopted new articles in the Criminal Code to deal with Computer Crime. The new articles have effect from February 13, 2001.

In particular art. 550(b) focuses on illicit behaviour related to Computer Hacking.

Art. 550b sec.1 deals with unauthorised access and unauthorised maintenance of access, to a computer system of a person who is aware that he is not unauthorised. The punishment may be a fine or a period of detention between three months and one year.

The second section of the article deals with the abuse of power in accessing the computer system, meaning the situation of a person who has the right to access the computer system and uses this permission in order to defraud or

with the intention of cause harm. In this case the person may be sentenced to a term of imprisonment from six month to two years or with a fine.

The third section of art. 550(b) adds the provision of an unlawful access to data. The article says that it is a crime to access without permission data which is stored, processed or transmitted by a computer system, or to procure such data in any way whatsoever, or to make any use whatsoever of a computer system, or to cause any damage, even unintentionally, to a computer system or to data which is stored, processed or transmitted by such a system. The punishment for this crime is a fine and imprisonment for a period from 1 to 3 years.

Attempting to perpetrate the above-mentioned crimes is also punishable. Section 6 of art. 550(b) also makes punishable a person who orders or incites one of the offences in the previous sections. The penalty is a term of imprisonment from six months to five years and a fine.

Other articles in the Belgium Penal Code are related to CIA Offences: in particular art. 314 in its first paragraph, which deals with the interception of a private communication and data communication without the agreement of all the parties involved. In its second paragraph it deals with the disclosure of the contents of an intercepted communication. The punishment for this crime is from one to three years of imprisonment.

CIA Offences such as Malicious Code or Denial of Service are managed through other articles of the Belgian Penal Code and in particular through art. 523 that deals with the destruction of machinery and art. 559, sec. 1, that deals with damage to property. Finally art. 528 is related to the destruction of property with threat or violence. These articles clearly refer to physical goods but in this specific situation they can be useful in managing “virtual” goods such as information.

In dealing with CIA Offences, three additional laws have to be mentioned: the 1934 Law on the Transmission Lines, the Law on the Reform of Certain Public Institutions, and the 1990 Law that among other issues takes into consideration Deliberate Access to the National Social Security Database.

Art. 16 of the Law of 1934 declares that it is a punishable offence to interfere with military communications lines in order to hinder their functioning, and establishes a penalty of three years of prison. The Law on the Reform of Certain Public Institutions establish that is a public offence to use means of telecommunications to hinder or damage correspondence. The penalty for this illicit behaviour is up to four years of prison and/or a fine.

The 1990 Law considers it a crime to deliberately access without right the National Social Security Database, and establishes a penalty of a fine or a term of up than one year of prison if the access is committed with fraudulent intent.

The last series of articles that must be take into consideration in Belgian legislation deals directly with *Unauthorised Modification of Information*. This specific CIA offence is covered by three articles of the Belgian Penal Code: art 193, that deals with Forgery in general and establishes a term of up to five years of prison or even more in special circumstances. The second article is art. 461, that deals with Theft in general and provides a term of up to five years of prison and a fine. The third article is art. 496, the general provision for Fraud; as for the previous article the penalty is up to five years of prison and a fine.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Art 314 bis para.1: interception of a private communication or a data communication without the agreement of all the parties involved in the communication.	1 year's imprisonment and or a fine 2 years' imprisonment and/or a fine when the offender is a government officer Art 259 bis para.1
			Art 314 bis para.2: disclosure of the contents of an intercepted communication	2 years' imprisonment and or a fine 3 years' imprisonment and/or a fine when the offender is a government officer Art 259 bis para.2
Malicious Code	Art 16 Law on Transmission Lines of 03.01.1934: it is a punishable offence to interfere with military communication lines in order to hinder their functioning	Up to 3 years of prison and a fine	Art 523: destruction of machinery	3 years' imprisonment and or a fine
			Art 559, 1°: damage or destruction of property	A fine
	Art 114, para 8, 2° Law on the reform of certain public institutions: it is a public offence to use telecommunications means to hinder or damage correspondents	Up to 4 years' imprisonment and /or a fine	Art 528: damage to or destruction of property with threats or violence	3 years' imprisonment or a fine
Denial of Service	Art 16 Law on Transmission Lines of 03.01.1934: it is a punishable offence to interfere with military communication lines in order to hinder their functioning	Up to 3 years' imprisonment and a fine	Art 523: destruction of machinery	3 years' imprisonment and or a fine
			Art 559, 1°: damage or destruction of property	A fine

	Art 114, par 8, 2° Law on the reform of certain public institutions: it is a public offence to use telecommunications means to hinder or damage correspondents	Up to 4 years of prison and /or a fine	Art 528: damage to or destruction of property with threats or violence	3 years' imprisonment or a fine
Account Compromise	Law 15.01.1990: deliberate unauthorised access to the National Social Security Database	A fine	Art 550 bis, para 1: any person who, aware that he is not authorised, accesses and maintains his access to a computer system	A fine
				3 months' to 1 year's imprisonment From 6 months' to 2 years' imprisonm ent if the intention is to defraud
		Up to one year's imprisonment if there is fraudulent intent to damage	Art 550 bis para 2: any person who, with intent to defraud or with intent to cause harm, exceeds his power of access to a computer system	A fine
				6 months' to 2 years' imprisonment
Intrusion Attempt	Law 15.01.1990: deliberate unauthorised access to the National Social Security Database	A fine	Art 550 bis para 1: any person who, aware that he is not authorised, accesses and maintains his access to a computer system	A fine
				3 months' to 1 year's imprisonment. 6 months' to 2 years' imprisonment if the intention is to defraud
		Up to one year's imprisonment if there is fraudulent intent to damage	Art 550 bis para 2: any person who, with intent to defraud or with intent to cause harm, exceeds his power of access to a computer system	A fine
				6 months' to 2 years' imprisonment
Unauthorised Access to Information	Law 15.01.1990: deliberate unauthorised access to the National Social Security Database	A fine	Art 550 bis para 1: any person who, aware that he is not authorised, accesses and maintains his access to a computer system	A fine
				3 months' to 1 year's imprisonment. 6 months' to 2 years' imprisonment if the intention is to defraud
		Up to one year's imprisonment if	Art 550 bis para 2: any person	A fine

		there is fraudulent intent to damage	who, with intent to defraud or with intent to cause harm, exceeds his power of access to a computer system	6 months' to 2 years' imprisonment
Unauthorised Access to Transmissions			Art 314 bis para 1: interception of a private communication or a data communication without the agreement of all the parties involved in the communication.	1 year's imprisonment and or a fine 2 years' imprisonment and/or a fine when the offender is a government officer Art 259 bis para 1
			Art 314 bis para 2: disclosure of the contents of an intercepted communication	2 years' imprisonment and or a fine 3 years' imprisonment and/or a fine when the offender is a government officer Art 259 bis para 2
Unauthorised Modification of Information			Art 193: Forgery	Up to 5 years' imprisonment or greater in special circumstances
			Art 461: Theft	Up to 5 years' imprisonment and a fine
			Art 496: Fraud	Up to 5 years' imprisonment and a fine
Unauthorised Access to Communication System	Law 15.01.1990: deliberate unauthorised access to the National Social Security Database	A fine	Art 550 bis para 1: any person who, aware that he is not authorised, accesses and maintains his access to a computer system	A fine
				3 months' to 1 year's imprisonment. 6 months' to 2 years' imprisonment if the intention is to defraud
		Up to one year's imprisonment if there is fraudulent intent to damage	Art 550 bis para 2: any person who, with intent to defraud or with intent to cause harm, exceeds his power of access to a computer system	A fine
				6 months' to 2 years' imprisonment

Forensics

There is a free or informal system of evidence in Belgium (à charge et à décharge').

Unusually, in court, the prosecutor relies upon reports of investigations into electronic evidence, not the evidence itself. Such reports may be compiled by law enforcement or expert witnesses. The FCCU has completed presentations during the last year trying to raise awareness about the importance of digital evidence in criminal proceedings.

Electronic evidence is regarded as a common form of evidence, but generally is complimentary to other kinds of evidence and is commonly used in a supporting role in a similar fashion to blood samples in narcotics cases.

The general principles of collection and preservation of digital evidence are that a copy of the hard disk is made for security reasons, it is then restored to another hard disk at a forensic workstation, forensic tools are then used to conduct an investigation and if necessary tools are sometimes used on the suspects machine itself. Finally, the police send a report to the prosecutors office.

Investigations and forensics are carried out by the local police units of the Federal Police and the FCCU. In some cases, a prosecutor or judge will use a civil expert to carry out the investigation and the suspect is allowed this privilege in the case of a counter argument. Forensic evidence is admissible as both documentary evidence and supporting evidence (see above). In the case of documentary evidence it is backed up by other material evidence and declaration of the suspects and witnesses.

Forensic procedures are a standardised version of Interpol / other national best practice and procedures.

Reporting & Law Enforcement Organisations

Federal Computer Crime Unit
Notelaarsstraat 211 Rue du Noyer
B - 1000 Brussel / Bruxelles
Belgium, Europe
T: +32 2 743 74 74
F: +32 2 743 74 19
E:contact@fccu.be

Commission de la protection de la vie privée
Boulevard de Waterloo, 115
B-1000
Bruxelles
T:+32(0) 2 / 542.72.00
F:+32(0) 2 / 542.72.01 et +32 (0)2 / 542.72.12

E: commission@privacy.fgov.be
W: www.privacy.fgov.be

The FCCU is part of the Federal Police, General Direction of Judicial Police, Direction of Financial and Economic Crime. The local Computer Crime Units are part of the Federal Police (Arrondissemental Judicial Service). They consist of 18 units spread over Belgium.

A functional link between the FCCU and the local units exist but there is no hierarchical command structure between the two unit levels.

The FCCU should be alerted in cases of 'computer crime': information system and telecom hackings, denial-of-service attacks and major computer crime incidents as well as illegal content related crime. The FCCU also has responsibility to investigate attacks on 'critical' infrastructure, generally in cooperation with the local CCU.

In terms of the reporting threshold, computer crime which is common but has no impact on the safety of citizens or where the financial impact is low is put at a lower priority, but is within the bounds of the police obligation to investigate any crime.

Other Reporting Mechanisms

In March 2000, Child Focus launched the prevention campaign SurfSafe. The aim of this campaign was to encourage children (target group : 10 to 13 year-olds) to be alert to the potential dangers of the Internet. A poster was created for this purpose, setting out 7 safety rules. An e- mail address was also set up to receive reports of abuse of a paedophile nature on the Internet and complaints relating to them.[42]

[42] http://www.childfocus.org/20/html/surf_safe_fr.htm

Denmark

The Nordic legal tradition has features distinct from the West European traditions of Common Law or Civil Law and the fundamentals of Danish law can be traced back the Middle Ages. Nonetheless, its development has been greatly influenced by Roman law, in particular German and French law. Danish civil law, however, is found in specific legislation or established by practice rather than found in Codes. The ultimate source of all Danish law is the Constitution (Grundloven).

There are three levels of regular courts: district (byret), appeal (landsret) and the supreme court (hojesteret). The regular courts hear civil and criminal cases. Cases are usually tried in two instances. However, some minor cases have only one instance and are heard in the district courts only.

The police force comes under the Ministry of Justice who exercises his powers through the National Commissioner, the Commissioner and Chief Constables. There are 54 police districts, each headed by a Chief Constable and assisted by Deputy Chief Constables, Prosecutors and Deputy Prosecutors. The Chief Constable is also the Public Prosecutor for the district and as such comes from a legal background.

The national police force is made up of the police of Denmark (54 police districts), the Faroe Islands and Greenland. The functions of the police are to be found in the Administration of Justice Act. As well as enforcing the law and controlling crime, they are to take preventative measures against crime. They also have wide ranging administrative duties including the issue of passports, weapons licences, driving licences and administering driving tests and vehicle registration.

Legislation

art 263 sec 1, 2 - art 193 - art 291

The Danish Penal Code provides four main articles to deal with the CIA Offences listed in the CSIRT taxonomy.

In particular, art. 263 sec. 1 establishes that it is illegal to deprive someone of a letter, a telegram or other sealed communication, or to open such a communication. The second paragraph of this article affirms that it is a crime to obtain illicit access to the place where other persons keep personal property. Moreover it is also a crime to conduct the unauthorised eavesdropping of a conversation or communication with the aid of equipment. The penalty provided for this illicit conduct is a fine or a term of imprisonment not exceeding six months.

Art. 263 sec.2 takes into consideration the unauthorised access to another person's information or programs designed to be used in connection with electronic data processing. The penalty may be a fine or a term of imprisonment not exceeding six months.

Article 193 of the Denmark Penal Code deals with unlawful disturbance to the operation of a public means of communication, of the public mail service, of public used telegraph or telephone services, of radio and television installation, of data processing systems or of installations for the public supply of water, gas, electricity or heating. The punishment for this illicit behaviour may be a fine or a period of detention.

Finally, the general provision of damage to propriety in article 291 establishes that a person who destroys or removes object belonging to another is punishable with a fine or imprisonment for a term not exceeding one year.

There is a provision of imprisonment for a term not exceeding four years in the case of serious damage or when the offender is recidivist under the same section of the code. The most serious punishment is provided in case the damage has been committed by gross negligence: the penalty is a term of imprisonment not exceeding six years.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Para 263, c.1: any person who unlawfully: 1_ deprives someone of a letter, telegram, or other sealed communication, or opens such a communication, or acquaints himself with its contents, 2_ obtains access to places where other persons keep personal property, 3_ with the aid of equipment, secretly listens to or records statements made privately, by telephone or in other conversations, or negotiations during a meeting he is not attending or to which he has unlawfully obtained access.	A fine Up to 6 months' imprisonment
Malicious Code			Para 193 (1): any person who unlawfully causes major disturbance in the operation of public means of communication, of the public postal service, of publicly used telegraph or telephone services, of radio and television installations, of data processing systems or of installations for the public supply of water, gas, electricity or heating,	A fine or simple detention if such act has been committed negligently

			Art 291 (1), (2), (3): any person who destroys or removes objects belonging to others	(1) A fine or imprisonment for a term not exceeding 1 year (2) Imprisonment for a term not exceeding 4 years in the case of serious damage or when the offender has previously been convicted under this section or in pursuance of Section 180, 181, 183-1, 183-2,184-1, 193 or 194 of this act (3) Imprisonment for a term not exceeding 6 years if the damage has been committed by gross negligence
Denial of Service			Para 193 (1): any person who unlawfully causes major disturbance in the operation of public means of communication, of the public postal service, of publicly used telegraph or	A fine or simple detention if such act has been committed negligently

			telephone services, of radio and television installations, of data processing systems or of installations for the public supply of water, gas, electricity or heating,	(1) A fine or imprisonment for a term not exceeding 1 year (2) Imprisonment for a term not exceeding 4 years in the case of serious damage or when the offender has previously been convicted under this session or in pursuance of Section 180, 181, 183-1, 183-2,184-1, 193 or 194 of this act (3) Imprisonment for a term not exceeding 6 years if the damage has been committed by gross negligence
Account Compromise			Art 263 (2): any person who unlawfully obtains access to another person's information or programs designed to be used in connection with electronic data processing	A fine Imprisonment for a term not exceeding 6 months
Intrusion Attempt			Art 263 (2): any person who unlawfully obtains access to another person's information or programs designed to be used in connection with electronic data processing	A fine Imprisonment for a term not exceeding 6 months

Unauthorised Access to Information			Para 263, c.1: any person who unlawfully: 1_ deprives someone of a letter, telegram, or other sealed communication, or opens such a communication, or acquaints himself with its contents, 2_ obtains access to places where other persons keep personal property, 3_ with the aid of equipment, secretly listens to or records statements made privately, by telephone or in other conversations, or negotiations during a meeting he is not attending or to which he has unlawfully obtained access.	A fine Imprisonment for a term not exceeding 6 months
			Art 263 (2): any person who unlawfully obtains access to another person's information or programs designed to be used in connection with electronic data processing	A fine Imprisonment for a term not exceeding 6 months
Unauthorised Access to Transmissions			Par 263, c.1: any person who unlawfully: 1_ deprives someone of a letter, telegram, or other sealed communication, or opens such a communication, or acquaints himself with its contents, 2_ obtains access	A fine

				Imprisonment for a term not exceeding 6 months
			to places where other persons keep personal property, 3_ with the aid of equipment, secretly listens to or records statements made private, telephone or in other conversations, or negotiations during a meeting he is not attending or to which he has unlawfully obtained access.	Imprisonment for a term not exceeding 6 months
Unauthorised Modification of Information				
Unauthorised Access to Communication System			Art 263 (2): any person who unlawfully obtains access to another person's information or programs designed to be used in connection with electronic data processing	A fine Imprisonment for a term not exceeding 6 months

Forensics

Digital Evidence is quite common in the criminal justice system in Denmark. Lawyers, the judiciary and the courts in general are au fait with dealing with digital evidence, due in part to the large numbers of content related crimes in Denmark in the last few years.

There is a free or informal system of evidence in Denmark.

Reporting & Law Enforcement Organisations

Rigspolitichefens afd. A Nationalt Efterforskningsstøttecenter (Information Technology Support Unit, "A" Department, Danish National Police)
Polititorvet 14,
DK-1780
Copenhagen V,
Denmark
T: +45 3314 8888 ext.5307
F: +45-3332 2771
E: It-kriminalitet@politi.dk
W: http://www.anmeldelse.politi.dk/

Data Protection Agency
Datatilsynet
Borgergade 28, 5,
1300 Copenhagen K
Denmark
+45 3319 3200
+45 3319 3218
dt@datatilsynet.dk
www.datatilsynet.dk

There are two cybercrime units in Denmark. The Copenhagen Computer Forensics Unit is a small unit composed only of 6 police investigators and deals with cybercrimes related to the geographic area of the capital city.

The National Computer Forensics Unit (NCFU) itself is a much larger unit composed of 20 professionally trained investigators. These two units are the only organisations dealing with cybercrime in Denmark. The NCFU specialises in two areas – cybercrime and forensics (which analyse static evidence left on computer storage media). The unit itself deals with both cybercrime and content related criminal investigations. Outside expert assistance is rarely called upon due to the technical expertise of the unit.

All policemen in Denmark have a basic knowledge of computer crime and the importance of digital evidence in scene of crime investigations.

Training to a further professional level is via vocational on the job training at the NCFU, whereby recruits are taken on for a probationary period after a

spell of 6-8 years in the regular police. Moves are currently in place to change this to a formal training scheme, although at the time of going to print nothing has been formalised. Training also takes place with other international units (particularly the Visigrad countries) and Interpol and Europol. It is not known but assumed that outreach activities are also conducted on a case by case basis due to the small number and dedicated nature of the staff.

The NCFU's relationship with other national governmental organisations in Denmark dealing with criminality is limited. There is no national research and development body and the unit has contacted the military 2 or 3 times in the last 5 years for technical assistance. Liaison with other units (such as the national intelligence unit) is on an equally small scale, maintained on an ad-hoc basis as and when major events occur.

Finland

The legal system is based on the Nordic tradition; its roots can be traced back 700 years to when Finland belonged to the Kingdom of Sweden. Swedish remains an official language of Finland and all Finish legislation is published in both languages.

The Finish police organisation operates under the Ministry of the Interior and is headed by the Police Department. The second level is the National Police Units, Provincial Police Commands and the Helsinki District Police. The third level is the local police, which operates under the Provincial Police Commands. The Åland Islands form their own independent police district. National police operations on the Åland Islands are conducted by the National Bureau of Investigation's Åland unit. The police must discharge their duties in accordance with the Police Act.

The police will commence a pre-trial investigation if there is reason to suspect that a crime has been committed. Not all reports of offences lead to pre-trial investigation. The general principles concerning pre-trial investigation are laid down in the Pre-Trial Investigation Act. In a pre-trial investigation the police will establish whether or not an offence has actually been committed, under what circumstances it occurred and the identity of the parties concerned. The pre-trial investigation will also establish the extent of the injury or damage caused by the offence, the gain effected by the offender and the demands of the injured party.

The police have a duty to conduct pre-trial investigations without undue delay. A head of investigation is appointed for each criminal case to be investigated who will remain responsible for the progress of the investigation.

Legislation

Finnish Penal Code

The Finish Penal Code provides some articles to manage the CIA Offences listed in the CSIRT Taxonomy.

In particular, art 38 declares that anyone who, unjustifiably, opens a letter or other closed message addressed to another, or obtains, or attempts to obtain, information about the content of a telephone call, a telegram, a message containing text, images or data or another comparable form of telecommunication message while it is being transmitted over a telephone network is punishable with a fine or a term of imprisonment for at most one year.

There is a specific provision in case someone defaces, destroys, hides or conceals a closed message of the type referred to in the first paragraph. The penalty is the same as in the previous paragraph.

Art. 28 of the Finnish Penal Code offers a general provision for unlawful use of chattels or machine equipment belonging to someone else and is punishable with a term of imprisonment for at most one year.

Art. 38 may be relevant to manage some CIA Offences like *Computer Fingerprinting*, *Unauthorised Access to Information* and *Unauthorised Access to in Transmission*: this article establishes that a person who unjustifiably opens a letter or other closed message addressed to another, or obtains, or attempts to obtain, information about the content of a telephone call, a telegram, a message containing text, images, or data or another comparable form of telecommunications messages while it is being transmitted over a telephone network is punishable with a term of imprisonment for at most one year, or with a fine. The same penalty is provided for a person who defaces, destroys, hides or conceals a closed message of the type referred to in the above-mentioned subparagraphs.

Art. 35 of the Finnish Penal Code establishes a general provision for serious damages to the property of someone else. The second paragraph of this article is relevant for the CIA Offences: it deals with the unjustified destruction or the serious damage of data recorded on a information device. The punishment in both cases is a fine for the petty offences, or a term of imprisonment from four months to four years of imprisonment in the case of aggravated damage to property.

The same penalties are provided by art. 33 of the Finnish Penal Code that deals with general forgery offences, an article that may be useful in managing the *Unauthorised Modification of Information*. In the article there is the same distinction provided as in art 35: simple forgery, aggravated forgery and petty forgery. The level of punishment is related to the level of forgery.

The 1894 Law on the Disturbance of Communication is very old but can be applied in order to punish some CIA Offences like Malicious Code and Denial of Service. The Law establishes that anyone who intentionally prevents or interferes with the use of general telegraph or telephone installation must be punished with at most two years in prison.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Art 38: a person who unjustifiably: (1) opens letter or other closed message addressed to another, (2) obtains or attempt to obtain information about the content of a telephone call, a telegram, a message containing text, images or data or other comparable form of telecommunications message while it is being transmitted over a telephone network, (3) defaces, destroys, hides or conceals a closed message of the type referred to section 1 or a telemessage of the type referred to in section 2,	A fine Imprisonment for a term not to exceed 1 year
Malicious Code	Disturbance of Communication (21.04.1894): anyone who intentionally prevents or interferes with the use of general telegraph or telephone installations	At most 2 years of prison	Art 35: anyone who unjustifiably destroys the property of another shall be charged with damage to property Anyone who unjustifiably destroys or conceals or hides data recorded on an information device or other recording in order to cause damage to another	Damage to property: a fine or imprisonment for a term not to exceed 1 year Aggravated damage to property: from 4 months' to four years' imprisonment Simple property offences: a fine
Denial of Service	Disturbance of Communication (21.04.1894): anyone who intentionally prevents or interferes with the use of general telegraph or telephone installations	Imprisonment for a term not to exceed two years	Art 35: anyone who unjustifiably destroys the property of another shall be charged with damage to property Anyone who unjustifiably destroys or	Damage to property: a fine or imprisonment for at most 1 year Aggravated damage to property: from 4 months to four years of imprisonment

			conceals or hides data recorded on an information device or other recording in order to cause damage to another	Simple property offences: a fine
Account Compromise			Art 28: anyone who unjustifiably uses the chattels or immobile machine equipment of another shall be charged with unauthorised use	Imprisonment for a term not to exceed 1 year
Intrusion Attempt			Art 28: anyone who unjustifiably uses the chattels or immobile machine equipment of another shall be charged with unauthorised use	Imprisonment for a term not to exceed 1 year
Unauthorised Access to Information			Art 38: a person who unjustifiably: (1) opens a letter or other closed message addressed to another, (2) obtains or attempts to obtain information about the content of a telephone call, a telegram, a message containing text, images or data or another comparable form of telecommunication message while it is being transmitted over a telephone network, (3) defaces, destroys, hides or conceals a closed message of the type referred to section 1 or a telemessage of the type referred to in section 2,	A fine Imprisonment for a term not to exceed 1 year
			Art 28: anyone who unjustifiably uses the chattels or immobile machine equipment of another shall be charged with unauthorised use	Imprisonment for a term not to exceed 1 year

Unauthorised Access to Transmissions			Art 38: a person who unjustifiably: (1) opens letter or other closed message addressed to another, (2) obtains attempt to obtain information about the content of a telephone call, a telegram, a message containing text, images or data or another comparable form of telecommunication message while it is being transmitted over a telephone network, (3) defaces, destroys, hides or conceals a closed message of the type referred to subparagraph 1 or a telemessage of the type referred to in subparagraph 2,	A fine Imprisonment for a term not to exceed 1 year
Unauthorised Modification of Information			Art 33: Forgery Offences 1_Forgery 2_Aggravated Forgery 3_Simple Forgery Art 35: Damage to propriety 1_Damage to Propriety 2_Aggravated Damage to Propriety 3_Simple Damage To propriety	Damage to property: a fine or imprisonment for a term not to exceed 1 year Aggravated damage to property: from 4 months to four years of imprisonment Simple property offences: a fine
Unauthorised Access to Communication System			Art 28: anyone who unjustifiably uses the chattels or immobile machine equipment of another shall be charged with unauthorised use	Imprisonment for a term not to exceed 1 year

Forensics

Reporting & Law Enforcement Organisations

National Bureau of Investigation, Computer Crime Squad
Jokiniemenkuja 4,
P.O.Box 285 Fin-01301
Vantaa,
Finland
T: +358-0-8388 6254
+358-0-8388 6267
F: +358 0 8388 6230

Other Reporting Mechanisms

(The Finnish data protection agency (*www.tietosuoja.fi/1560.htm*).
www.tietosuoja.fi (Tietosuojaviranomaiset)

France

The French judicial system is based on a written law derived mainly from laws passed in Parliament by the deputies and senators. The Civil Code, the Penal code and the other Codes as well as European and International laws are the essential tools of those involved in the judicial system.

France's leading police body dealing with computer crime is the Office Central de Lutte contre Criminalite liee aux Technologies de l'Information ed de la Communication (OCLCTIC). Other police agencies have specialist high tech crime sections, normally within their Financial and Economic Sections. The judicial police in Paris has a large specialist cyberpolice unit, the SEFTI (Service d'Enquête sur les Fraudes aux Technologies de l'Information - Investigation Service for Technology and Information Fraud.

Legislation

Penal Code: sec 186-1 | 323-1; 323- 2; 323- 3

The French Penal Code offers several articles that relate to CIA Offences.

In particular art 186-1 of the French Penal Code deals with unauthorised interception and establishes that someone who intercepts, orders the interception or facilitates the interception of a message, transmitted or received by a telecommunication system, or uses or discloses their contents shall be punished with a fine or a term of imprisonment of 1 year. There is a special provision if the offender is a public official: in this case the term of imprisonment is up to 5 years.

Another important article in the French Penal Code that can be used handle CIA Offences is article 323 sections 1, 2 and 3. Art 323-1 deals with fraudulent access to all or part of an automated data processing system, if it results in the suppression or an alteration of data entered in the system or any alteration to the functioning of the system.

This is the most widely applied article and it is useful to handle CIA Offences such as Malicious Code, Account Compromise, Intrusion Attempt, Unauthorised Access to Information and Unauthorised Access to a Communication System. The penalty for this offence is a fine or a term of imprisonment up to 2 years.

Art 323-2 deals with the alteration of data or any interference with the functioning of an automated data processing system. This article can handle the Denial Of Service offence. The penalty for this offence is a fine or a term of imprisonment up to 3 years.

Art 323-3 of the French Penal Code deals with the fraudulent introduction of data into an automated data processing system. The penalty for this offence is a fine or a term of imprisonment up to 3 years.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Section 186-1: someone who intercepts, orders to intercept or facilitates the interception of messages sent out, transmitted or received or received by a telecommunications system, or uses or discloses their contents.	A fine (special provision for public officials, agents or an authorised telecommunication operator)
				1 year's imprisonment 5 year's if the person is a public official, an agent or an authorised telecommunications operator
Malicious Code			Section 323-1: fraudulent access to all or a part of an automated data processing system if this results in the suppression or alteration of data entered into the system or any alteration to the functioning of the system	A fine
				2 years' imprisonment
			Section 323-2: alteration of data or any other interference with the functioning of an automated data processing system	A fine
				3 years' imprisonment
			Section 323-3: fraudulent introduction of data into an automated data processing system.	A fine
				3 years' imprisonment
Denial of Service			Section 323-2: alteration of data or any other interference with the functioning of an automated data processing system.	A fine
				3 years' imprisonment
Account Compromise			Section 323-1: fraudulent access to al or a part of an automated data processing system if this results in the suppression or	A fine

			alteration of data entered into the system or any alteration to the functioning of the system.	2 years' imprisonment
Intrusion Attempt			Section 323-1: fraudulent access to al or a part of an automated data processing system if this results in the suppression or alteration of data entered into the system or any alteration to the functioning of the system.	A fine 2 years' imprisonment
Unauthorised Access to Information			Section 323-1: fraudulent access to al or a part of an automated data processing system if this results in the suppression or alteration of data entered into the system or any alteration to the functioning of the system	A fine 2 years' imprisonment
			Section 186-1: Someone who intercepts, orders to intercept or facilitates the interception of messages sent out, transmitted or received by a telecommunications system, or uses or discloses their contents	A fine (special provision for public officials, agents or an authorised telecommunication operator) 1 year's imprisonment 5 years if the person is a public official, an agent or an authorised telecommunications operator
Unauthorised Access to Transmissions			Section 186-1: Someone who intercepts, orders to intercept or facilitates the interception of messages sent out, transmitted or	A fine (special provision for public officials, agents or an authorised telecommunication operator)

			received by a telecommunications system, or uses or discloses their contents	1 year's imprisonment 5 years if the person is a public official, an agent or an authorised telecommunications operator
Unauthorised Modification of Information			Section 186-1: Someone who intercepts, orders to intercept or facilitates the interception of messages sent out, transmitted or received by a telecommunications system, or uses or discloses their contents	A fine (special provision for public officials, agents or an authorised telecommunication operator) 1 year's imprisonment 5 years if the person is a public official, an agent or an authorised telecommunications operator
Unauthorised Access to Communication System			Section 323-1: fraudulent access to al or a part of an automated data processing system if this results in the suppression or alteration of data entered into the system or any alteration to the functioning of the system.	A fine 2 years' imprisonment

Forensics

There is a free or informal system of evidence in France. Art 427 of the Code de Procédure Pénale states that apart from the cases where the law provides otherwise, offences may be proven by any means of proof, and it is for the judge to decide according to his inner conviction. This is known as the principle of the freedom of means of proof (le principe de la liberté des preuves). Exceptions to this principle are, for example, if admitting the evidence would contravene the defendant's rights under the European Convention on Human Rights.

The Code de Procédure Pénale also sets out detailed rules for carrying out police procedures such as the conduct of interviews and powers of searches and seizure.

Reporting & Law Enforcement Organisations

OCLCTIC (Office Centrla de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)
101 Rue des Trois Fontnot
F-92000
Nanterre
France
T: +33 1 40 97 80 14
F: +33 1 47 21 00 95
E: oclctic-sec.dcpjaef@interieur.gouv.fr

Gendarmerie Nationale
E: gendarmerie@dial.oleane.com
W: www.defense.gouv.fr/gendarmerie/

Commission Nationale de l'Informatique et des Libertés (CNIL)
21, rue St-Guillaume
75340 Paris
cedex 7
T: +33 (0)153 73 22 22
F: +33 (0) 153 73 22 00
W: www.cnil.fr

The judicial police in Paris has a large specialist cyberpolice unit, called SEFTI (Service d'Enquête sur les Fraudes aux Technologies de l'Information – Investigation Service for Technology and Information Fraud) which has 21 people – 9 investigating officers, 11 police and 1 administrator.[43]

One national unit dealing with cybercrime is the Central Office for the Fight against IT and Communications Crime (Brigade Centrale de Repression de la Criminalite Informatique), located in the Sub-department of Economic and

[43] http://www.prefecture-police-paris.interieur.gouv.fr/carrieres/Metiers/cyberpolice.htm

Financial Affairs of the Central Police Investigation Department (itself part of the General National Police Department). Formed in June 1994, the formation of the unit reflected an increased desire to deal with these new aspects of criminality.

In 1999, the then Prime Minister proposed the introduction of a new specialist national central unit specifically to deal with computer crime. This was later put into law with the Decree of 15 May 2000, which formally set up Office Central de Lutte contre Criminalite liee aux Technologies de l'Information ed de la Communication (OCLCTIC).[44] OCLCTIC is a specialised office very similar to the UK NHTCU.

The missions of OCLCTIC are twofold. First, to carry out operational investigative activities and provide high tech assistance to other investigations. Second to provide a strategic set of services in the provision of training, co-ordination and support of other computer crime activities and to act as the central point of contact for international and national organisations. OCLCTIC maintains direct liaison with the following bodies:

- Brigade of IT Fraud investigation BEFTI, from the Direction Regionale de la Police Judiciaire responsible to the Paris Police Prefecture.
- Department of Territorial Surveillance
- National Gendarmerie
- Customs

The 19 Regional Police Investigation Services in France each have a Criminal Section and a Financial and Economic Section. The Specialist Hi-Tech Crime Investigators reside within each Financial and Economic Section. Their mission is to carry out high tech investigations in their geographic area (either self initiated or in support of other investigative activities). Training is provided by OCLCTIC and outside experts – engineers, IT advisors and legal and judicial experts.

Other Reporting Mechanisms

In 1998 the French Internet Service Provider Association www.afa-france.com settled AFA Point de Contact www.pointdecontact.net, a hotline against Child porn and racial hatred, the only one of that kind in France, which enables Internet users to find useful information and help to understand how to deal with such contents.

AFA Point de Contact is funded by the French Internet Service Provider Association www.afa-france.com with support funding from the EU Safer Internet Action Plan europa.eu.int/ISPO/iap/

[44] Decree No 20000-405 15 May

Germany

Germany belongs to the Roman law tradition. Its legal system has also been influenced by Germanic law. The main source of law is the Constitution or Basic Law (Grundgesetz). Much German law was codified in the nineteenth century, to some extent influenced by French codification. German codification itself has influenced other legal systems, notably that of Greece and Japan.

There are five categories of courts in Germany. The ordinary courts deal with civil and criminal matters. The administrative courts deal with proceedings involving public authorities do not fall under jurisdiction of the social or finance courts. Finally, there are labour courts for employment issues. The Federal Constitutional Court is a separate entity and rules on constitutional disputes.

In general, the individual Länder have responsibility for law enforcement and public security. The police branches under Länder jurisdiction include the general police force which deals with public order and minor offences and the criminal police which deals with more serious offences. The state level criminal police forces are supported by the Federal Criminal Police Office, particularly in cases of interregional or international criminal matters. The Federal Criminal Police Office is the national central agency for Interpol and Europol.

Legislation

Sec 202a – sec 303 a, b

CIA Offences in Germany are managed through various articles of the Penal Code.

Due to the wide definition of illicit behaviour within the German Penal Code, it is possible to cover all the typologies of Incident Classification listed in the CSIRT Taxonomy referring to three main articles Sec. 202a, Sec. 303a and Sec. 303b.

Sec. 202a deals with data espionage and with the case of someone who obtains data, which are not meant for him, without authorisation. There is a provision for the case in which the subject obtains data not for a direct benefit but for the benefit of someone else.

In Sec. 202a there is a strict definition of data, meaning only information that is stored or transmitted electronically or magnetically or in any other form not directly visible. The punishment for Data Espionage is a fine or a period of imprisonment not exceeding three years.

Sec. 303a takes into consideration the Alteration of Data. This is defined as including erasure, suppression, rendering useless, or altering data. The definition of data is the same as the one used in Sec 202a, namely information stored or transmitted electronically or magnetically or in any form

not directly visible. Sec. 303a provides for a term of imprisonment not exceeding two years or a fine. Attempts will also be punished.

Sec. 303b is an important article in the German Penal Code that covers CIA Offences such as Denial of Service and Malicious Code. It deals in general with Computer Sabotage and states that it is a crime to interfere in data processing that is essential for other business. The interference may be committed under the provision of Sec. 303a or by destroying, damaging, rendering useless, removing or altering a computer system or a data carrier. The punishment may be a fine or a term of conviction not exceeding five years. As for Sec. 303a the attempt is also punishable.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Section 202 a: Unauthorised procuring of data not meant for the offender or specially protected against unauthorised access	A fine Up to 3 years' imprisonment
Malicious Code			Section 303-b: Interfering with a data processing activity which is of vital importance for another enterprise, another business or public authority by destroying, removing, or altering a data processing system or data carrier or rendering it useless (or Section 303a- depending on the victim or the damage caused)	A fine Up to 5 years' imprisonment (or up to 2 years' imprisonment)
Denial of Service			Section 303-b: Interfering with a data processing activity which is of vital importance for another enterprise, another business or public authority by destroying, removing, or altering a data processing system or data carrier or rendering it useless	A fine Up to 5 years' imprisonment
Account Compromise			Section 202 a: Unauthorised procuring of data not meant for the offender or specially protected against unauthorised access	A fine Up to 3 years' imprisonment
Intrusion Attempt			Section 202 a: Unauthorised procuring of data not meant for the offender or specially protected against unauthorised access	A fine Up to 3 years' imprisonment

Unauthorised Access to Information			Section 202 a: Unauthorised procuring of data not meant for the offender or specially protected against unauthorised access	A fine Up to 3 years' imprisonment
Unauthorised Access to Transmissions			Section 202 a: Unauthorised procuring of data not meant for the offender or specially protected against unauthorised access	A fine Up to 3 years' imprisonment
Unauthorised Modification of Information			Section 303-b: Interfering with a data processing activity which is of vital importance for another enterprise, another business or public authority by destroying, removing, or altering a data processing system or data carrier or rendering it useless (or section 303-a:depending on the victim or the damage caused)	A fine Up to 5 years' imprisonment (or up to 2 years imprisonment)
Unauthorised Access to Communication System			Section 202 a: Unauthorised procuring of data not meant for the offender or specially protected against unauthorised access	A fine Up to 3 years' imprisonment

Forensics

Reporting & Law Enforcement Organisations

Bundeskriminalamt
(Federal Criminal Police Office)
Information Technology Crime Unit (Referat OA 34-2)
Thaerstraße 11
65173 Wiesbaden
Germany
T: +49 (0) 611-55-15908
F: +49 (0) 611-55-15725
E: oa34-2@bka.bund.de
W: www.bka.de

Bundeskriminalamt
(Federal Criminal Police Office)
Technical Service Centre for Information and Communication Technologies
(Referat KI 26-TeSIT)
Thaerstraße 11
65173 Wiesbaden
Germany
T: +49 (0) 611-55-14289
F: +49 (0) 611-55-45274
E: ki26-tesit@bka.bund.de
W: www.bka.de

Within the German law enforcement community, the Federal Police Authority (BKA) has responsibility at a national level for IT crime. Two units undertake four main activities – computer forensics (in support of other criminal investigations), and Internet investigations or "patrols" are dealt with by the KI 26-TeSIT unit. In addition the OA 34-2 unit undertakes co-operation and information gathering through the various national and international agencies such as the state police forces as well as Interpol, Europol and the G8.

Each state police also has specialised units dealing with computer crime which conduct investigations and – depending on the structure – separate computer forensic units which may be called upon to undertake examinations of hardware seized in other operations.

Greece

Greece has a Civil Law tradition. Is governed by the Constitution of 1975 and is for the most part codified.

The administration of justice comes under the Ministry of Justice. There are three courts: civil, administrative and criminal. The civil and administrative courts are organised in the same way, but the criminal courts are classified according to the type of offence to be tried.

Law enforcement is undertaken by the Ministry of Public Security. Policing is carried out by the Hellenic Police.

Legislation

Penal Code Art 370 – 2

In the Greek Penal Code art 370 c.2 deals with Unauthorised Access to a Computer System and establishes that anyone who obtains access to data recorded on a computer or in the external memory of a computer transmitted by telecommunication system shall be punished with a fine or by imprisonment for up to 3 months, under the condition that this act has been committed without right, especially in violation of prohibitions or of security measures taken by the legal holder.

If the offender is in the service of the legal holder of the data, the act of the proceeding paragraph shall be punished only if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee.

No other CIA Offences legislation available.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting				
Malicious Code				
Denial of Service				
Account Compromise			Art 370 c2: Anyone who unlawfully obtains access to data recorded on a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder If the offender is in the service of the legal holder of the data, the act of the proceeding paragraph shall be punishable only if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee	A fine Up to 3 months' imprisonment

Intrusion Attempt			Art 370 c2: Anyone who unlawfully obtains access to data recorded on a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder If the offender is in the service of the legal holder of the data, the act of the proceeding paragraph shall be punishable only if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee	A fine Up to 3 months' imprisonment
Unauthorised Access to Information			Art 370 c2: Anyone who unlawfully obtains access to data recorded on a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder. If the offender is in the service of the legal holder of the data, the act of the proceeding paragraph shall be punishable only if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee	A fine Up to 3 months' imprisonment
Unauthorised Access to Transmissions				
Unauthorised Modification of				

Information				
Unauthorised Access to Communication System			Art 370 c2: Anyone who unlawfully obtains access to data recorded on a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder. If the offender is in the service of the legal holder of the data, the act of the proceeding paragraph shall be punishable only if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee	A fine Up to 3 months' imprisonment

Forensics

Reporting & Law Enforcement Organisations

Information Technology Crimes
173 Alexandras Ave
GR-115 22 Athens
Greece
T: +30-1-6456440
F: +30-1-6430238

Hellenic Data Protection Authority,
Omirou 8,
PC 10564,
Athens
T:+030 210 3352604
F: +030 210 3352617
contact@dpa.gr
www.dpa.gr

The ELAS Computer Crime Task Force was formed in 2000.

Other Reporting Mechanisms

None

Ireland

Ireland has a Common Law tradition, having been increasingly influenced by English law from the 12 century until the creation of the Irish Free State. The Constitution of 1922 carried all previous English legislation into Irish law and consequently some pre-1922 UK legislation is still in force in Ireland.

Judges are appointed for life by the President on the advice of the government. District Courts hear minor criminal and civil cases. More serious cases are heard by the Circuit Court. The High Court has full original jurisdiction and determining power in all matters of law or fact. It also hears appeals from the Circuit Court in civil cases. When hearing criminal appeals it is known as the Central Criminal Court. The Supreme Court is the court of final appeal.

Ireland's National Police Service, Garda Siochana (Guardians of the Peace), is headed by a government appointed Commissioner. He is responsible to the Minister for Justice, Equality and Law Reform. The Commissioner's management team includes two Deputy Commissioners and 10 Assistant Commissioners. The Garda is responsible for all police functions in the state. It has some 11,230 personnel, including 1,700 non-uniformed detectives. Uniformed officers are unarmed, whereas detectives carry firearms.

Legislation

Criminal Damage Act 1991 Sec. 5

Under Irish legislation, most of the CIA Offences listed in the CSIRT Taxonomy are handled by Sec.5 of the 1991 Criminal Damage Act. This section deals with unauthorized access and establishes that a person who, without lawful excuse, operates a computer within the State with intent to access any data kept either within or outside the State, or outside the State with intent to access any data kept within the State, whether or not he accesses any data, shall be guilty of an offence.

The penalty provided for this illicit conduct is a fine or a term of imprisonment not exceeding 3 months. This section applies also whether or not the person intends to access any particular data or any particular category of data or data kept by any particular person.

Criminal Justice (Theft and Fraud Offences Act) Act 2001.

Section 9 A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years.

As can be seen this section is very broad and encompasses a broad list of offences.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting				
Malicious Code	Section 9 A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.	A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years.		
Denial of Service	Section 9 A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.	A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years.		
Account Compromise	Criminal Damage Act 1991 Section 5: (1) A person who without lawful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence	A fine		

	(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	A term of imprisonment up to 3 months		
Intrusion Attempt	Criminal Damage Act 1991 Section 5: (1) A person who without lawful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence	A fine		
	(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	A term of imprisonment up to 3 months		
Unauthorised Access to Information	Criminal Damage Act 1991 Section 5: (1) A person who without lawful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the	A fine		

	State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence (2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.	A term of imprisonment up to 3 months		
Unauthorised Access to Transmissions				
Unauthorised Modification of Information				
Unauthorised Access to Communication System	Criminal Damage Act 1991 Section 5: (1) A person who without l\awful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence (2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	A fine A term of imprisonment up to 3 months		

Forensics

Reporting & Law Enforcement Organisations

Computer Crime Investigation Unit, Garda Bureau of Fraud Investigation
Harcourt Square,
Harcourt Street
DUBLIN 2
Ireland
T: +353-1-6663708
+353-1-6663746
Fax+353-1-4752658
E: cciuhs@iol.ie

The Garda Computer Crime Investigation Unit is located within the Garda Bureau of Fraud Investigation. It is a national reference centre for Law Enforcement requiring assistance in the investigation of computer related crime. The unit has expertise in forensic examination of computer hardware and storage devices. Interestingly, PABX fraud is highlighted specifically in the CCIU crime prevention advice.

The Garda Information Technology Division (the operational IT / IS support unit) also provides support to investigations in an operational capacity.

Other reporting mechanisms

The Internet Advisory Board (IAB) co-ordinates activities of the www.hotline service, designed to fulfil reporting considerations for content related crimes.[45] At a general level the IAB monitors illegal and harmful use of the Internet, but this is content related. It also tries to assist in the self-regulation of the ISP industry in Ireland.

[45] Internet Advisory Board at: http://www.iab.ie/

Italy

Italy belongs to the civil law tradition. It is has been influenced on Roman law and the Napoleonic Code. It is based on the Constitution of 1948 and five Codes.

Civil justice is decided by the Judge of Peace (Giudice di pace), the Tribunal (Tribunale) that may be composed by a single magistrate or a by a three member panel and the Court of Appello (Corte d'Appello). Criminal cases are heard by the Judge of Peace (that works as Lower Court for minor criminal offences). the Tribunal (Tribunale) and the Court of Appeal (Corte d'appello), acting respectively as first and appellate judge, deal with all crimes but the homicide and other crimes involving very long time imprisonment indictment. These case are ruled by the Court of Assize (Corte d'Assise) and, as appellate court, the Appelate Court of Assize (Corte d'assise d'appello).

In addition, there is a Court of Cassation (Corte di Cassazione) based in Rome, which hears criminal and civil appeals on points of law only.

The Constitutional Court (Corte Costituzionale) also based in Rome, is the body ruling on the conformity of ordinary laws (included criminal ones) to the Italian Constitution.

Italy's main three law enforcement bodies are Guardia di Finanza (inder the authority of Finance Ministership), Arma dei Carabinieri reporting to the Ministership of Defense and State Police is under the authority of the Minister of the Interior.

All the three bodies are organised in a vertical structure. Apart from the General HeadQuarter (Comando Generale) located in Rome, Guardia di Finanza and Carabinieri are organised in Multi region Head Quarter (Comando Interregionale), Regional Quarter (Comando Regione), Provincial Head Quarter Quarter (Nucleo Provinciale) and (for Carabinieri only) local station (Comando Stazione Carabinieri). The Polizia di Stato is organised at three levels: the Questure, Interregionals and Offices. The Questore is the senior State Police official in each province. The Questure is organised into three main offices: The Secretariat Office of the Questore, which deals with public order and security, the Criminal Police Division and the Administrative and Immigration Police. The State Police Interregional Directorates deal with health and safety in the work place as well as planning and coordination functions. Thirdly there are local police stations under the authority of the Questore. All three law enforcement bodies have a computer crime branch.

A further important operational sector of the State Police is made up of the Specialities, of which the Postal and Telecommunications Police is one.

Legislation

Penal Code art 615 sec.3, 4, 5 – art 420 sec 2 – art 635 sec. 2

Italy has several specific provisions against CIA Offences in its penal code.

In particular, article 615 sec.3 deals with unauthorised access to a computer or telecommunication system and establishes that is illicit conduct to enter without authorisation into a computer or telecommunication system protected by security measures, or to remain in it against the expressed or implied will of the one who has the right to exclude access. For all these situations there is a general provision of punishment not exceeding three years of imprisonment.

The penalty is from one to five years of imprisonment in specific situations: if the crime is committed by a public official or by an officer of a public service through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices, even without a licence, the profession of a private investigator, or with abuse of the capacity of a system operator.

The same punishment is provided in cases in which the culprit uses violence upon things or people, or he is armed and if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or rather the destruction or the damage of the data, the information or the programs contained in it.

Finally if the unauthorised access concerns a computer or telecommunication systems of military interest or concerning public order or public security or civil defence or other public interest, the penalty - respectively - is from one to five years or from three to eight years of imprisonment.

Article 615 sec. 4 deals with the illegal possession and diffusion of Access Codes to Computer or Telecommunication Systems and establishes that it is illegal to obtain a profit for himself or for another or to cause damage by reproducing, transmitting or delivering codes, key-words or other means for access to a computer or telecommunication system protected by safety measures, or providing information or instructions that fit to the above purpose. The punishment is a term of imprisonment not exceeding one year and a fine.

Art.615 sec. 5 of the Italian Penal Code covers the diffusion of programs aimed at damaging or interrupting a computer system. This article establishes that it is illicit to transmit or deliver a computer program with the aim and the effect of damaging a computer or telecommunication system, the data or the programs contained or pertinent to it, or leading to the partial or total interruption or an alteration in its working. The punishment is a term of imprisonment not exceeding two years and a fine.

The Italian Penal Code provides two other general articles: art. 420, sec 2 and art. 635, sec 2.

Art 420 sec.2, establishes that it is a crime to damage or destroy public interest informatics infrastructures or public databases or programs that have

a public utility. In addition, it is an offence to cause the interruption of public interest informatics infrastructures. The punishment is a term of imprisonment from three to eight years.

Art 635 sec.2 deals with damage to computer systems and establishes that whoever, without right, damages or destroys computer systems or programs or information or data is punishable with a term of imprisonment from six months to three years. If the crime is committed by abuse of power of a system administrator, the penalty is from one year to four years of imprisonment.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Art 615 (4): Distribution, communication or provision to others of software produced by oneself or another, with intent to cause damage to or interruption of or alteration of a computer or a telematic system or computer program	A fine A term of imprisonment not to exceed 2 years
Malicious Code			Art 420: Destruction of, or causing damage to 1 - computer or telematic systems 2 - computer program 3 - data	A term of imprisonment of not less than 3 years and not more than 8 years
			Art 615 (5): Distribution communication or provision to others of software produced by oneself or another, with the intent of causing damage to or to interruption or alteration of a computer or a telematic system or computer program	A fine A term of imprisonment of not more than 5 years
			Art 635 (2): destruction of, causing damage to, or rendering partially or totally unusable: 1 - computer or telematic systems 2 - computer program 3 - data	A term of imprisonment of not less than 6 months and not more than 3 years 4 years if there are aggravating circumstances
Denial of Service			Art 420: Destruction of, or causing damage to 1 - computer or telematic systems 2 - computer program 3 – data	A term of imprisonment of not less than 3 years and not more than 8 years
Account Compromise			Art 615: (3) Gaining authorised access to a computer or telematic system or, if the access was accidental, remaining within the system	A term of imprisonment of not less than 3 years and not more than 8 years 1 to 5 years if there are aggravating circumstances

Intrusion Attempt			Art 615: (3) Gaining authorised access to a computer or telematic system or, if the access was accidental, remaining within the system	3 years' imprisonment
				1 to 5 years if there are aggravating circumstances
Unauthorised Access to Information			Art 615 (4): Distribution, communication or provision to others of software produced by oneself or another, with intent to cause damage to or interruption of or alteration of a computer or a telematic system or computer program	A fine
				A term of imprisonment of not more than 2 years
			Art 615: (3) Gaining authorised access to a computer or telematic system or, if the access was accidental, remaining within the system 1 computer or telematic systems 2 computer program 3 data	3 years' imprisonment
				1 to 5 years if there are aggravating circumstances
Unauthorised Access to Transmissions			Art 615 (4): Distribution, communication or provision to others of software produced by oneself or another, with intent to cause damage to or interruption of or alteration of a computer or a telematic system or computer program	A fine
				A term of imprisonment of not more than 2 years
Unauthorised Modification of Information			Art 615: (3) Gaining authorised access to a computer or telematic system or, if the access was accidental, remaining within the system	3 years' imprisonment
				1 to 5 years if there are aggravating circumstances
Unauthorised Access to Communication System			Art 615: (3) Gaining authorised access to a computer or telematic system or, if the access was accidental, remaining within the system	3 years' imprisonment
				By 1 to 5 years if there are aggravating circumstances

Forensics

Forensics is still at an early developed stage[46] and the criminal Courts often tend to underestimate the relevance of properly acquired digital evidence, focusing more on the merit of the infringement[47].

Computer Searches and Seizure are still a very debated issues[48]. The main stream of Italian court decisions accept the seizing of a whole system while only searching for data (often seizing contents belonging to third parties or not related to the investigations[49]). A contrary decision has been issued by the Court of Turin [50] on Sept. 2000.

On July, 9 2003 the Criminal Court of Civitavecchia (Rome) dealing with an online child pornography case appointed a Court expert to revise and examine the conformity of the Polizia Postale investigation techniques to the international accepted standards. This seems to be the first case in Italy dealing with this matter.

A debate is arising about the need of open source forensic software and the effectiveness of ISP data retention in criminal investigations [51].

---

[46] Andrea Monti Attendibilità dei sistemi di computer forensic in ICT-Security n.ro 9 del 10-01-03 - http://www.ictlaw.net/internal.php?sez=art&IdT=7&IdTA=5&IdA=248&lang=1

[47] See, for instance, State vs Pinto – Court of Giulianova (Teramo) - decision n.112/02 http://www.ictlaw.net/internal.php?sez=giuris&IdT=2&IdTG=18&IdG=3 in which the Public Prosecutor just performed remote (US hosted)website access through an untrained law enforcement officer, using a private IAP facility to obtain evidence of alleged defamatory contents. See also State vs Russo - Court of Avezzano – decision n.1185/03 in which the liability for defamation has been established on logfile analysys and user backtracking relying upon unverified logfile sent by fax, without log file matching with data contained in the suspected PC, and no searching of the alleged offensive text.

[48] See A.Monti Computers, freedom and privacy in Italy in Proceedings of the Computer Freedom and Privacy 10th conference, Toronto, 2000 http://www.cfp2000.org/papers/monti.pdf and ALCEI Sequestri di computer, lo scandalo continua on http://www.alcei.it/sequestri/cs990615.html

[49] See the press articles http://www.ecn.org/inr/massa/rassegna.htm related to the seizing of the website of a political activist association, Isole nella rete, accused of defamatory statement against the Turkish government. The seize shutted down too the sites of other NGO not involved in the investigation

[50] See Court of Turin Case n. 26495/99 – Ordinanza of Sept. 2 2000 http://www.ictlaw.net/internal.php?sez=giuris&IdT=7&IdTG=6&IdG=52 in which the court ruled against the seize of a whole computer while only searching for data.

[51] See Andrea Monti "The Legal Duty of IAP's to Preserve Traffic Data : a Dream or a Nightmare ?" in the Proceedings of CTOSE Conference "Collecting and Producing Electronic Evidence in Cybercrime Cases" University of Namur (BE) May, 8-9 2003 - http://www.ctose.org/info/NamurDocs/Monti.ppt

Reporting & Law Enforcement Organisations

Servizio Polizia Postale e delle Comunicazioni Divisione Investigativa
Viale Europa N.175
ROMA
Italy
T: +39 06 59588001
+39 3486080512
F: +39 06 59587817
E: polizia.comunicazioni@mininterno.it
W: http://www.poliziadistato.it/pds/english/specialist.htm

Data Protection Agency
Piazza di Monte Citorio n. 121
Roma
00186
T: (+39) 06.69677.1
F: (+39) 06.69677.785
E: garante@garanteprivacy.it
W:www.garanteprivacy.it

In Italy the Postal and Communication Police is the national authority for dealing with cyber-crime. It is structured into a main central office in Rome, a branch office in Naples (residing within the Board for the Security of Communications) and 19 Regional Divisions and 76 Provisional Sections. The Postal and Communication Police deal with a wide variety of criminal activity, both content and cyber-crime related. Examples are on-line paedophilia, computer hackers, credit card fraud the spread of computer viruses and copyright infringement. Moreover, for prevention purposes, the Postal and Communications Police has set up an Internet monitoring activity regarding phenomena such as organisations of different types that could be involved in criminal conducts or racial hatred. International co-operation on trans-national crime (including but not limited to cyber-crime) is handled by the DCPC (Central Criminal Police Direction), which co-ordinates the police forces within Italy as well as the Carabinieri and the Financial Guards (Finance Police). The Postal and Communication Police fall under the authority of the DCPC.

Furthermore, both the Carabinieri and the Financial Guards have specialised IT investigation bodies. The GAT (Gruppo Anticrimine Tecnologico or Anti Tech Crime Group) of the Financial Guards is the best known of these units as it has concluded a number of successful investigations. It is widely expected that this unit is a priority for further investment in dealing with this aspect of criminality in Italy.

Other Reporting Mechanisms

Stop-It is a body dealing with reporting of illegal and harmful content. It co-operates with the Postal and Communication Police, who are forwarded

reports. Stop-it is partnered with the Italian Association of Internet Service Providers and Italian ISP Tiscali S.p.A. It also regularly collaborates with other NGOs, including Arci[52], Ecpat Italia[53], Confconsumatori[54] and Movimento Consumatori.[55]

On 12 July 2002, the Italian Government established a Technical Committee for a Safer Use of the Internet. Its aims to create and manage a strategy with the objectives of creating a 'safe Internet for all environment'. It pays a particular attention to certain categories of users, such as elderly, disabled, minors, people belonging to minorities, etc.

[52] http://www.arci.it
[53] http://www.ecpat.it/
[54] http://www.confconsumatori.com/
[55] http://www.movimentoconsumatori.it/

Luxembourg

Luxembourg law is based on Roman law. Its administrative law is based largely on the French and Belgian systems. Its civil law derives from the Napoleonic code, commercial law on a modified version of French commercial law and its tax law based on post 1945 German tax law.

There are four types of court; Justice de Paix, Tribunal d'Arrondissement, Cour d'Appel and the Cour de Cassation. The Cour de Cassation is the court of final appeal and decides on points of law only.

The Police Corps and the Gendarmerie were amalgamated as of 1 January 2000 to form the Police Grand-Ducale, which carries out all police functions throughout the Grand Duchy. It is under the authority of the Ministry of the Interior.

Legislation

Penal Code art 509-1 / 509-2 / 509-3 | *Art 524*

The Luxemburg Penal Code contains several articles related to CIA Offences.

In particular art 509-1 deals with fraudulent access to all or part of a data processing system and fraudulently remaining logged into such a system. The penalty for this conduct is a fine or a term of imprisonment from 2 months to 1 year. If such action results in the deletion or the alteration of data stored on the system, or if the system is damaged, the penalty is a fine or a term of imprisonment from 2 months to 2 years.

Art 509-2 deals with the situation in which a person deliberately obstructs or alters the functioning of an automatic data processing system. The penalty in this case is a fine or a term of imprisonment from 3 months to 3 years.

Art 509-3 handles the integrity and quality of data. This article establishes that a person, who knowingly, and without right, directly or indirectly introduces data into an electronic data processing system or deletes or alters data stored in that system, or alters the system's operation or data transmission mode commits an offence. The punishment for this conduct is a fine or a term of imprisonment from 3 months to 3 years.

Art 524 of the Luxemburg Penal Code deals with the hindering of telephone communications by any means, an offence that can be punished by a fine or a term of imprisonment from 1 month to 3 years.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			509-1: fraudulent access to all or a part of a data processing system or to remain logged into such a system	A fine A term of imprisonment from 2 months to 1 year
Malicious Code			Art 509-2: deliberately hindering of an automatic data processing system	A fine A term of imprisonment from 3 months to 3 years
Denial of Service			Art 509-2: deliberately hindering of an automatic data processing system	A fine A term of imprisonment from 3 months to 3 years
Account Compromise			509-1: fraudulent access to all or a part of a data processing system or to remain logged into such a system	A fine A term of imprisonment from 3 months to 3 years
Intrusion Attempt			509-1: fraudulent access to all or a part of a data processing system or to remain logged into such a system	A fine A term of imprisonment from 2 months to 1 year
Unauthorised Access to Information			509-1: fraudulent access to all or a part of a data processing system or to remain logged into such a system	A fine A term of imprisonment from 2 months to 1 year
Unauthorised Access to Transmissions			509-1: fraudulent access to all or a part of a data processing system or to remain logged into such a system	A fine A term of imprisonment from 2 months to 1 year

Unauthorised Modification of Information			Art 509-3: to introduce, directly or indirectly, knowingly and without lawful excuse, data into an electronic data processing system or to delete or to alter data stored in that system, or to alter the system option or the data transmission mode	A fine A term of imprisonment from 3 months to 3 year
Unauthorised Access to Communication System			509-1: fraudulent access to all or a part of a data processing system or to remain logged into such a system	A fine A term of imprisonment from 2 months to 1 year

Forensics

Luxembourg follows France in its adherence to free or informal principles of evidence.

Reporting & Law Enforcement Organisations

Service de Police Judiciaire
L-2957
Luxembourg City
Grand-Duché de Luxembourg
T: +352-4997 6040
+352-4997 6805
F: +352-4997 6099
E: spj.dire@police.etat.lu

Commission National pour la Protection des Données
68, route de Luxembourg
L-4221
Esch-sur-Alzette
Luxembourg
T: +352 26 10 601
F: + 352 26 10 6029
E: info@cnpd.lu
W: www.cnpd.lu

Currently, a single investigator is responsible for white collar fraud and high tech crime investigations.

Other reporting mechanisms

None

The Netherlands

Dutch law belongs to the civil law tradition. French codification was imposed in 1810/11 and remained in place until 1836 when they were replaced by national codes. The French penal code, however, remained in place until 1886 before it was replaced. Its replacement was greatly influenced by its German counterpart.

The formal organisation of the police is laid out in the 1993 Police Act. There are 25 regional police regions. Each region has its own force under the administrative management of the mayor of the largest town in the region. The Ministry of the Interior has overall responsibility for the regional police forces.

In addition to the regional forces there is a National Police Force (Korps landelijke politiediensten –KLPD). The national force includes the Criminal Investigation Police (Regionale receherche dientst) and a national cybercrime unit, the Digital Investigations Group (Groep Digitaal Rechercheren or GDR).

Legislation

Penal Code: 138a | 139a | 139b | 139c | 139d | 139e | 161-6, 7 | 350a | 350b | 351

The Dutch Penal Code contains a large number of articles that are useful to deal with CIA Offences.

Art 138a deals with Unauthorised Access and establishes that any person who intentionally and unlawfully accesses an automated data storage or processing system or part of such a system shall be guilty of an offence if he breaks through a security system, or obtains access by technical means using false signals or a false key or by assuming a false identity. The penalty for this offence is a fine or a term of imprisonment not exceeding 6 months.

The second paragraph of art 138a deals with the situation in which an offender copies or records, for himself or for another person, data stored in an automated system to which he has unlawfully gained access. The penalty for this offence is heavier than the one provided in the first paragraph: there is a fine or a term of imprisonment up to 4 years.

The third paragraph of art 138a establishes that if the offences described in paragraph 1 and 2 are committed through a telecommunication system and if the offender makes use of the processing capacity of an automated system with the aim of obtaining an unlawful advantage for himself or gains access to the automated system of a third party via the automated system to which has gained access, the penalty is a fine or a term of imprisonment up to four years.

The subsections of article 139 can be used to deal with Unauthorised Interception related to a large number of different conducts.

Art 139a establishes that any person who intentionally uses a technical device to eavesdrop on or record a conversation conducted in a dwelling, an enclosed room or enclosed premises using an automated system shall commit an offence if he eavesdrops on a conversation other than on the orders of a participant in the conversation or records a conversation other than on the orders of such a participant without participating in it himself. The penalty for this offence is a fine or a term of imprisonment up to 6 months.

The second paragraph of the article establishes that a person who intentionally uses a technical device to tap or to record data being transferred in a dwelling, enclosed place or premises by means of an automated system has committed an offence. The penalty is a fine or a term of imprisonment up to 6 months.

The third paragraph of article 139a deals with exemptions, for example when the eavesdropping is allowed by a special joint order of the Prime Minister, the Minister of Justice and the Minister of Home Affairs for a period of no more than 3 months and in cases where this action is required in the interests of State security.

Art 139b establishes that a person who, with the aim of eavesdropping on or recording a conversation being conducted in a place other than a dwelling, an enclosed place or enclosed premises commits an offence if he eavesdrops on the conversation other than on the orders of a participant in that conversation or records the conversation other than on the orders of a participant and without participating in it himself, can be punished with a fine or a term of imprisonment not exceeding 3 months.

The same penalty is provided in the second paragraph of article 139b for an offender who intentionally uses a technical device to secretly tap or record data being transferred other than in a dwelling, enclosed place or premises by means of an automated system or telecommunication. The exemptions listed in art 139a par.3 also apply here.

Art 139c states that it an offence for a person to intentionally use a technical device to tap or to record data being transferred over a telecommunications infrastructure or terminal equipment connected thereto, when the data is not intended for him alone, for his own benefit or for the benefit of others or of the person on whose orders he is acting. The penalty for this offence is a fine or term of imprisonment not exceeding 1 year.

This article is not applied to tapping or recording data received via a radio receiver, unless a special effort has been made or a prohibited receiver has been used in order to make the reception possible, or on the orders of a person entitled to use the telecommunication connection, except in instances of obvious misuse.

The last case in which paragraph 1 is not applied is when it is carried out in the interests of State security, as listed in the exemptions in the third paragraph of article 139a.

Art 139d establishes that any person who ensures that a technical device is present in a particular place with a view to its being unlawfully used to eavesdrop on, tap or record a conversation, telecommunication or any other form of data transfer by an automated system, shall be liable to a fine or a term of imprisonment not exceeding 6 months.

Art 139e establishes that any person who has an object at his disposal on which he knows or may reasonably be expected to know that data has been recorded which was obtained by unlawfully eavesdropping on, tapping or recording a conversation, telecommunication or other form of data transfer by an automated system shall be liable to a fine or a term of imprisonment not exceeding 6 months.

The same penalty is provided in the case of any person who intentionally discloses to another person data that he has obtained unlawfully by eavesdropping on, tapping or recording a conversation, telecommunication or other form of data transfer by an automated system, or which he knows or may reasonably be expected to know has come to his knowledge as a result of such eavesdropping, tapping or recording, or finally, any person who intentionally makes an object as defined above available to another person.

Art 161-6 deals with the situation in which a person intentionally destroys, damages or renders unusable any automated data storage or processing system or any telecommunications installation, or disrupts the operation or functioning of such a system or installation, or renders ineffective any safety measures taken with regard to such a system or installation. The penalty for this offence is a fine or a term of imprisonment not exceeding 6 months if the offender prevents or impedes the storage or processing of data that is being undertaken for the benefit of the public or disrupts the telecommunication infrastructure. The term of imprisonment is up to 6 years if the offence could seriously endanger goods or the supply of services and up to 15 years if the offence causes a person's death.

Art 161-7 deals with the situation in which a person is to blame for an automated data storage or processing system or communication installation being destroyed, damaged or rendered unusable, or for any disruption to the operation or functioning of such a system or installation, or renders ineffective any safety measures taken with regard to such a system. The penalty is a fine or a term of imprisonment up to 3 months if the offence prevents or impedes the storage or processing of data for the benefit of the public, disrupts the telecommunication infrastructure, or seriously endangers goods or the supply of services. The term of imprisonment is up to 6 months if the offence endangers the life of a person; it does not exceed one year if the offence causes a person's death.

Art 350a and art 350b of the Dutch Penal Code are related to damage to computer data and computer programs. In particular, art 350a establishes that any person who intentionally and unlawfully changes, deletes, renders unusable or inaccessible or adds to data which is stored, processed or transmitted by an automated system has committed an offence. The penalty is a fine or a term of imprisonment not exceeding 2 years. The term of imprisonment is up to 4 years if a person commits the offence described in the first paragraph using a telecommunications infrastructure to gain unlawful access to an automated system and causes serious damage to the data.

The same penalty is provided in paragraph 3 of the same article, in the case in which a person intentionally and unlawfully makes available or distributes data which is intended to cause damage by multiplying in an automated system. This provision does not have to be applied if the action described in par.3 causes limited damage.

Art 350b establishes that any person who is to blame for data, stored, processed or transferred in an automated system being unlawfully changed, deleted, rendered unusable or inaccessible or added to, has committed an offence. The penalty for this conduct is a fine or a term of imprisonment not exceeding 1 month. The same penalty is provided if the person is to blame for unlawfully making available or distributing data that are intended to do damage by multiplying in an automated system.

Art 351 of the Dutch Penal Code deals with the situation in which a person intentionally destroys, damages, or renders unusable railway or electricity equipment, automated data, storage processing systems, telecommunications flood protection, water discharge, gas and water supply or sewerage installations in so far they are used for general benefit of the public, or national defence installations. The penalty in this case is a fine or a term of imprisonment not exceeding 3 years.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Art 139 a: 1_it is unlawful to intentionally use a technical device to eavesdrop on or record a conversation conducted in a dwelling, an enclosed room or enclosed premises using an automated system. 2: it is unlawful to intentionally use a technical device to tap or to record data being transferred in a dwelling, enclosed place or premises by means of an automated system	A fine Up to 6 months' imprisonment
			Art 139 b: 1_it is unlawful to secretly use a technical device with the aim of eavesdropping on or recording a conversation which is being conducted in a place other than a dwelling, an enclosed place or enclosed premises 2_it is unlawful to intentionally and secretly use a technical device to tap or to record data being transferred other than in a dwelling, enclosed place, or premises by means of an authorised system or telecommunications.	A fine Up to 3 months' imprisonment

			Art 139 c: it an offence for a person to intentionally use a technical device to tap or to record data being transferred over a telecommunications infrastructure or terminal equipm ent connected thereto, when the data is not intended for him alone, for his own benefit or for the benefit of others or of the person on whose orders he is acting.	A term of imprisonment of 1 year
			Art 139 d: a person who ensures that a technical device is present in a particular place with a view to its being unlawfully used to eavesdrop on, tap or record a conversation, telecommunication or any other form of data transfer by an automated system is liable for an offence.	Up to 6 months' imprisonment

			Art 139 e: 1_any person who has an object at his disposal on which he knows or may reasonably be expected to know that data has been recorded which was obtained by unlawfully eavesdropping on, tapping or recording a conversation, telecommunication or other form of data transfer by an automated system shall be liable of an offence. 2_any person who intentionally discloses to another person data that he has obtained unlawfully by eavesdropping on, tapping or recording a conversation, telecommunication or other form of data transfer by an automated system, or which he knows or may reasonably be expected to know has come to his knowledge as a result of such eavesdropping, tapping or recording, or finally, any person who intentionally makes an object as defined above available to another person	Up to 6 months' imprisonment
Malicious Code			Art 225: Forgery	A fine

			(general provision) Art 350: Destruction (general provision) Art 16-6: it is unlawful to intentionally destroy or render unusable any automated data storage or processing system or any telecommunication installation, or to disrupt the operation or functioning of such a system or installation, or to render ineffective any safety measures taken with regard to such system or installation	A term of imprisonment from 6 months to 15 years (on a scale of 4 levels of gravity)
			Art 161-7: it is unlawful to destroy or render unusable any automated data storage or processing system or any telecommunication installation, or to disrupt the operation or functioning of such a system or installation, or to render ineffective any safety measures taken with regard to such system or installation	A fine A term of imprisonment from 3 months to 1 year (on a scale of 3 levels of gravity)
			Art 350 a:	A fine

			1) It is unlawful to intentionally and without right to change, delete, render unusable or inaccessible or add to data which is stored, processed or transmitted by an automated system 2) It is unlawful to commit the offence in par. 1 using telecommunication infrastructure to gain unlawful access to an automated system causing serious damage to data 3) It is unlawful to intentionally and without right make available or distribute data which are intended to cause damage by multiplying in an automated system	A term of imprisonment from 2 to 4 years
			Art 350 b: 1_ It is unlawful to change without right, or to delete, or render unusable or inaccessible or add to data which is stored, processed or transmitted by an automated system. 2_ it is unlawful to make without right available or to distribute data which are intended to cause damage by multiplying in an automated system.	A fine A term of imprisonment not to exceed 1 month
			Art 351: it is an	A fine

			offence to intentionally and unlawfully destroy, damage, render unusable railway or electricity equipment, automated data, storage or processing systems, or telecommunications flood protection, water discharge, gas, water and wind supply and sewerage installations in so far they are used for the general benefit of the public	A term of imprisonment not to exceed 3 years
Denial of Service			Art 225: Forgery (general provision) Art 350: Destruction (general provision) Art 16-6: it is unlawful to intentionally destroy or render unusable any automated data storage or processing system or any telecommunication installation, or to disrupt the operation or functioning of such a system or installation, or to render ineffective any safety measures taken with regard to such system or installation	A fine A term of imprisonment from 6 months to 15 years (on a scale of 4 levels of gravity)
			Art 161-7: it is unlawful to destroy	A fine

			or render unusable any automated data storage or processing system or any telecommunication installation, or to disrupt the operation or functioning of such a system or installation, or to render ineffective any safety measures taken with regard to such system or installation	A term of imprisonment from 3 months to 1 year (on a scale of 3 levels of gravity)
Account Compromise			Art 138 a: 1_it is an offence to intentionally and unlawfully access to an automated data storage or processing system or part of such a system breaking through a security system or obtaining access by technical means using false signal or a false key or assuming a false identity 2_ it is unlawful to commit the offence in par. 1 to copy or record for himself or for a third person, data stored in an automated system 3_ such acts are punished if committed through the telecommunication infrastructure if the offender: a) makes use of the processing capacity of an automated system with the aim of obtaining an unlawful advantage for himself b) gains access to the automated system of a third party via the automated system to which he has gained access	A fine A term of imprisonment from 6 months to 4 years
Intrusion Attempt			Art 138 a:	A fine

			1_it is an offence to intentionally and unlawfully access to an automated data storage or processing system or part of such a system breaking through a security system or obtaining access by technical means using false signal or a false key or assuming a false identity 2_ it is unlawful to commit the offence in par. 1 to copy or record for himself or for a third person, data stored in an automated system 3_ such acts are punished if committed through the telecommunication infrastructure if the offender: a) makes use of the processing capacity of an automated system with the aim of obtaining an unlawful advantage for himself b) gains access to the automated system of a third party via the automated system to which he has gained access	A term of imprisonment from 6 months to 4 years.
Unauthorised Access to Information			Art 138 a: 1_it is an offence to intentionally and unlawfully access to an automated data storage or processing system or part of such a system breaking through a security system or obtaining access by technical means using false signal or a false key or assuming a false identity 2_ it is unlawful to commit the offence in par. 1 to copy or record for himself or for a third person,	A fine

			data stored in an automated system 3_ such acts are punished if committed through the telecommunication infrastructure if the offender: a) makes use of the processing capacity of an automated system with the aim of obtaining an unlawful advantage for himself b) gains access to the automated system of a third party via the automated system to which he has gained access	Up to 6 months' imprisonmnent
			Art 139 a: 1_it is unlawful to intentionally use a technical device to eavesdrop on or record a conversation conducted in a dwelling, an enclosed room or enclosed premises using an automated system. 2: it is unlawful to intentionally use a technical device to tap or to record data being transferred in a dwelling, enclosed place or premises by means of an automated system.	A fine UP to 6 months' imprisonment
			Art 139 b:	A fine

			1_it is unlawful to secretly use a technical device with the aim of eavesdropping on or recording a conversation which is being conducted in a place other than a dwelling, an enclosed place or enclosed premises 2_it is unlawful to intentionally and secretly use a technical device to tap or to record data being transferred other than in a dwelling, enclosed place, or premises by means of an authorised system or telecommunications.	Up to 3 months' imprisonment
			Art 139 c: it an offence for a person to intentionally use a technical device to tap or to record data being transferred over a telecommunications infrastructure or terminal equipment connected thereto, when the data is not intended for him alone, for his own benefit or for the benefit of others or of the person on whose orders he is acting.	1 year's imprisonment
			Art 139 d: a person who ensures that a technical device is present in a particular place with a view to its being unlawfully used to eavesdrop on, tap or record a conversation, telecommunication or any other form of data transfer by an automated system is liable for an offence.	Up to 6 months' imprisonment

			Art 139 e: 1_any person who has an object at his disposal on which he knows or may reasonably be expected to know that data has been recorded which was obtained by unlawfully eavesdropping on, tapping or recording a conversation, telecommunication or other form of data transfer by an automated system shall be liable of an offence. 2_any person who intentionally discloses to another person data that he has obtained unlawfully by eavesdropping on, tapping or recording a conversation, telecommunication or other form of data transfer by an automated system, or which he knows or may reasonably be expected to know has come to his knowledge as a result of such eavesdropping, tapping or recording, or finally, any person who intentionally makes an object as defined above available to another person	Up to 6 months' imprisonment
Unauthorised			Art 225: Forgery	A fine

Access to Transmissions			(general provision) Art 350: Destruction (general provision) Art 16-6: it is unlawful to intentionally destroy or render unusable any automated data storage or processing system or any telecommunication installation, or to disrupt the operation or functioning of such a system or installation, or to render ineffective any safety measures taken with regard to such system or installation	A term of imprisonment from6 months to 15 years (on a scale of 4 levels of gravity)
			Art 161-7: it is unlawful to destroy or render unusable any automated data storage or processing system or any telecommunication installation, or to disrupt the operation or functioning of such a system or installation, or to render ineffective any safety measures taken with regard to such system or installation	A fine A term of imprisonment from 3 months to 1 year (on a scale of 3 levels of gravity)
Unauthorised Modification of			Art 350 a:	A fine

Information			1_It is unlawful to intentionally and without right to change, delete, render unusable or inaccessible or add to data which is stored, processed or transmitted by an automated system. 2_ it is unlawful to commit the offence in par.1 using telecommunication infrastructure to gain unlawful access to an automated system causing serious damage to data 3_ it is unlawful to intentionally and without right, make available or distribute data which are intended to cause damage by multiplying in an automated system.	A term of imprisonment from 2 to 4 years
			Art 350 b: 1_ It is unlawful to change without right, or to delete, or render unusable or inaccessible or add to data which is stored, processed or transmitted by an automated system. 2_ it is unlawful to make without right available or to distribute data which are intended to cause damage by multiplying in an automated system.	A fine
				A term of imprisonment not exceeding 1 month
			Art 351: it is an	A fine

			offence to intentionally and unlawfully destroy, damage, render unusable railway or electricity equipment, automated data, storage or processing systems, or telecommunications flood protection, water discharge, gas, water and wind supply and sewerage installations in so far they are used for the general benefit of the public	A term of imprisonment not exceeding 3 years
Unauthorised Access to Communication System			Art 138 a: 1_it is an offence to intentionally and unlawfully access to an automated data storage or processing system or part of such a system breaking through a security system or obtaining access by technical means using false signal or a false key or assuming a false identity 2_ it is unlawful to commit the offence in par. 1 to copy or record for himself or for a third person, data stored in an automated system 3_ such acts are punished if committed through the telecommunication infrastructure if the offender: a) makes use of the processing capacity of an automated system with the aim of obtaining an unlawful advantage for himself b) gains access to the automated system of a third party via the automated system to which he has gained access	A fine A term of imprisonment from 6 months to 4 years

Forensics

There is a free or informal system of evidence in the Netherlands.

The admissibility of digital evidence is quite widespread; it is looked upon as a common form of evidence. The judges are aware of the existence of digital investigation expertise (both via law enforcement and independent experts) whom they call upon in court proceedings. However, the police do occasionally find themselves short of people and in some cases an investigator may not have all digital equipment checked for relevant information or evidence, simply due to the timescales.

The GDR does not outsource forensic investigations, carrying out all activity by trained staff, but it will call upon expertise from the Dutch Forensic Laboratory for assistance. Tools are often developed in house and distributed to colleagues within other forces. The presence of an R+D capability ensures that the unit stays ahead of the technology curve, constantly seeking to identify what technologies will prove useful to the unit's mission. Furthermore, the unit can deal with exceptionally large amounts of data, up to 2 terabytes.

There are no special considerations when it comes to presenting digital evidence in court and digital evidence is admissible as documentary evidence. In regard to forensic best practice, it is known that the unit co-ordinates with Interpol and Europol on a regular basis, particularly in respect of the development of best practice guides.

Dutch procedure is similar to US and British forensic procedure, making great care to observe the chain of evidence principles. This is particularly true in respect of tools and hardware/software.

Reporting & Law Enforcement Organisations

Korps Landelijke Politiediensten (Dutch National Police),
Divisie Centrale Recherche Informatie,
Recherche Advies en Ontwikkeling,
Informatietechnologie en Criminaliteit
Groep Digitaal Recherceren (Digital Investigaitons Group)
Postbus 3016
2700 KX
ZOETERMEER
The Netherlands
T: +31-79-459344
F: +31-79-458790

College bescherming persoonsgegevens (CBP) Registratiekamer (Personal Data Register)
Postbus 93374
2509 AJ Den Haag
Bezoekadres (alleen volgens afspraak)

Prins Clauslaan 20
2595 AJ Den Haag
Telefoon: 070-381 1300
Telefax: 070-381 1301
E-mail: info@cbpweb.nl
www.cbpweb.nl

There are about 100 individuals in the Netherlands with digital investigation skills and experience.

Government digital investigation expertise in the Netherlands is structured according to the following format: At the top is the Nederlands Forensisch Instituut (Dutch Forensic Lab). Below this is the national cybercrime unit the Korps landelijke politiediensten – Groep Digitaal Rechercheren (Dutch National Police Force – Digital Investigations Group) composed of 23 people split into Advisors, Internet Investigators (monitoring of dynamic traffic), digital investigators (hardware and computer forensic specialists) and research and development. Under the GRP, the 7 Bureau Digitale Expertise operate on behalf of several police regions. In the 26 regional police headquarters there may be organic digital investigation teams – a local Bureau Digitale Recherche.

Content related crime is handled by the FIOD-ECD (a special department of the Dutch Tax Administration).

GDR also works with national scientific institutes e.g. TNO Fysisch en Elektronisch Laboratorium (TNO-FEL) and maintains strong links with governmental and commercial CSIRTs.

The National Bureau for Digital Investigations (Landelijk Project Digitale Opsporing), established by Dutch Law Enforcement, coordinates national efforts on educational matters as well as Research and Development.

No obligations exist to inform any other Law Enforcement units about the collection of digital evidence (unless the investigations are of a joint nature). The unit prioritises incidents according to threat to life and limb and generally will not deal with every complaint relating to port scans, DDoS attacks or minor fraud (e.g. Nigerian 419 scam). In 2002 there were around 330 cases which were investigated by GDR. These were a variety and included hacking cases as well as fraud and assistance in other investigations.

Other Reporting Mechanisms

None

Portugal

Portugal has a Civil Law tradition. The ultimate source of law is the Constitution. There are three levels of court: the district court, court of appeal and supreme court. The Portuguese Criminal Police was established by decree in 1945.

Legislation

Cybercrime Law 109/1991 art 5, 6, 7, 8, 9

Portugal enacted a law on computer crime in 1991, the CRIMINALIDADE INFORMATICA – Lei 109-1991 (L.109/91). Several articles deal with all the typologies of Incident Classification listed in the Taxonomy.

In particular, art 5 of L.109/91 deals with damage to computer data and establishes that it is unlawful to intentionally cause damage with the total or partial suppression or deletion of data or a program, in order to obtain an illegitimate benefit for the offender himself or for a third person. The penalty for this illicit conduct is a fine or a term of imprisonment from 3 to 10 years, on a scale based on the gravity of the offence. Attempts are also punishable.

Art 6 of L.109/91 deals with computer sabotage and establishes that it is unlawful to introduce, modify, erase and suppress data or programs or to intervene by other means into a system with the intention of impeding or disturbing the functioning of the system. The penalty in this case is a fine or a term of imprisonment up to five years. If serious damage is caused the penalty is a term of imprisonment from 1 to 5 years.

Art 7 of L.109/91 deals in general with unauthorised access and establishes that it is unlawful to access, without right, a system with the intention of obtaining an illegitimate benefit or advantage for oneself or a third person. Attempts are also punishable. The penalty for this offence is a fine or a term of imprisonment up to 3 years if the access is committed by overcoming the security measures, or a term of imprisonment up to 5 years if the access is carried out to obtain industrial or commercial secrets, protected by law or to obtain a large economic benefit.

Art 8 of L. 109/91 deals with unauthorised interception and establishes that it is unlawful to intercept a communication process, without authorisation, using technical devices within a system or within a network. Attempts are also punishable. The penalty provided is a fine or a term of imprisonment not exceeding 3 years.

Incident Classification	Law		Criminal Code	
			Description	
Target Fingerprinting	Art 8 Cybercrime Law: is unlawful to intercept or attempt to intercept, without authorisation, using technical devices, a communication process within a system	A fine Up to 3 years' imprisonment		
Malicious Code	Art 6 Cybercrime Law: it is unlawful to introduce to modify, to erase, to suppress data or programs or to by other means intervene in a system, with intent to impede or disturb the functioning of the system	A fine 1 to 10 years' imprisonment (depending on the gravity of the conduct)		
	Art 5 Cybercrime Law: it is unlawful to intentionally cause damage with the total or partial suppression or deletion of data or program, in order to gain an illegitimate benefit for him or for third party. The attempt s hall also be punishable	A fine 1 to 10 years' imprisonment (depending on the gravity of the conduct)		
Denial of Service	Art 6 Cybercrime Law: it is unlawful to introduce to modify, to erase, to suppress data or programs or to by other means to intervene in a system, with intent to impede or disturb the functioning of the system	A fine From 1 to 10 years imprisonment (depending on the gravity of the conduct		
Account Compromise	Art 7 Cybercrime Law: it is unlawful to access without authorisation a system with intent to gain an illegitimate benefit or advantage for oneself or for a third party. The attempt is also punishable.	A fine A term of imprisonment from 3 or 5 years or from 1 to 10 years if the damage is very consistent		
Intrusion Attempt	Art 7 Cybercrime Law: it is unlawful to access without	A fine		

	authorisation a system with intent to gain an illegitimate benefit or advantage for oneself or for a third party. The attempt is also punishable	A term of imprisonment from 3 or 5 years or from 1 to 10 years if the damage is very consistent		
Unauthorised Access to Information	Art 7 Cybercrime Law: it is unlawful to access without authorisation a system with intent to gain an illegitimate benefit or advantage for oneself or for a third party. The attempt is also punishable	A fine A term of imprisonment from 3 or 5 years or from 1 to 10 years if the damage is very consistent.		
	Art 8 Cybercrime Law: is unlawful to intercept or attempt to intercept, without authorisation, using technical devices, a communication process within a system	A fine Up to 3 years' imprisonment		
Unauthorised Access to Transmissions	Art 8 Cybercrime Law: is unlawful to intercept or attempt to intercept, without authorisation, using technical devices, a communication process within a system	A fine Up to 3 years' imprisonment		
Unauthorised Modification of Information	Art 6 Cybercrime Law: it is unlawful to introduce to modify, to erase, to suppress data or programs or to by other means intervene in a system, with intent to impede or disturb the functioning of the system	A fine From 1 to 10 years' imprisonment (depending on the gravity of the conduct)		
Unauthorised Access to Communication System	Art 7 Cybercrime Law: it is unlawful to access without authorisation a system with intent to gain an illegitimate benefit or advantage for oneself or for a third party. The attempt is also punishable.	A fine A term of imprisonment from 3 or 5 years or from 1 to 10 years if the damage is very consistent		

Forensics

Reporting & Law Enforcement Organisations

Gabinete Nacional da Interpol
Rua Gomes Freire, nº 213, 3º 1050-178 Lisboa
T: +351 21 359 58 00
F: +351 21 357 58 44
E: dcci.gni@pj.pt

Secção de Investigação de Criminalidade Informática e Telecomunicações (SICIT)
Rua Alexandre Herculano 42-A
1250-011
LISBOA
Portugal
T: +351-21 353 69 28
F: +351-21 316 01 31
E: dciccef@pj.pt
W: www.pj.pt

Comissão Nacional de Protecção de Dados – National Commission for Data Protection (CNPD)
Rua de São Bento, nº 148,
3º 1200
LISBOA
T: 213928400
F: 213976832
E: geral@cnpd.pt
W: www.cnpd.pt

Other Reporting Mechanisms

None

Spain

Spain belongs to the civil law tradition. The main source of law is the Civil Code, which states that written rules of law created by the state are pre-eminent.

There are two police forces with national deployment. The Guardia Civil (Civil Guard) is responsible for issues such as customs and crowd control and crime within rural areas. The Cuerpo Nacional de Police (National Police Corps) deals with serious criminal investigations, criminal activity in large urban areas and international relationships. Municipal police generally deal with minor offences and traffic control.

Legislation

Lei Organica 23 November 1995 art.197 – art.198 – art.199 – art.256 – art 263 – art 264

In Spain computer crimes are normally handled using the Lei Organica 10/95 (L. 10/95), some of these articles are related to the CIA Offences listed in the CSIRTs Taxonomy.

In particular art 197 of L. 10/95 deals with unauthorised access and illegal access to information. In its first paragraph, it establishes that it is unlawful to discover the secrets or to violate the privacy of another without the consent of the latter, or to take possession of that individual's papers, letters, electronic mail, messages or any other personal documents. It is also unlawful to intercept his or her telecommunications or to use technical devices to listen, transmit, record or reproduce sounds or images or any other communication signal. The penalty for this offence is a fine or a term of imprisonment between 1 and 4 years.

The second paragraph of the same article establishes that the same penalty is applicable to an individual who, without authorisation, seizes, uses or modifies to the detriment of a third party, private personal or family data of another individual that may be recorded on a computer, electronic device or media, or in any type of file or record, whether public or private.

If the data, facts or images mentioned in the previous paragraphs are divulged, revealed or transferred to third parties, the penalty is a term of imprisonment between 2 and 5 years.

Other paragraphs of art 197 provide for different punishments that are related to the gravity of the offence: the maximum is provided in the case where the data reveals the ideology, religion, health, racial origin or sexual inclination of the subject.

Articles 198 and 199 are related to 197 and they cover the situation where the offender is someone authorised to deal with the data but abuses his or her privileges. In particular art. 198 deals with the case in which the illicit conduct

of art 197 is committed by a public officer abusing his position. The penalty is a term of imprisonment up to 10 years.

Art. 199 deals with the case in which the illicit conduct of art 197 is committed by a person who has the authorisation to know about the data but abuses his position to reveal secrets.

Art. 263 handles the situation in which a person makes use of any telecommunication terminal equipment, without the consent of its authorised user, and causes damage to the latter. The punishment in this case is a term of imprisonment from 3 months to 1 year. The conduct is only considered an offence if a large amount of economic damage is caused.

Art. 264 deals with computer damage or sabotage and lists some of the illicit conduct that can cause the damage discussed in art 263. In particular paragraph 2 of art 264 establishes that a person who, by any means, destroys, alters or makes unusable electronic data, programs or documents on other people's materials in networks or in computer systems is punishable with a fine or a term of imprisonment from 1 to 3 years.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting	L.10/95 art 197 para 1: it is unlawful to discover the secrets or to violate the privacy another without the consent of the latter, or to take possession of that individual's papers, letters, electronic mail, message or any other personal documents. It is also unlawful to intercept his or her telecommunications or to use technical devices for listening, transmitting, recording or reproducing sounds or images or any other communication signal	A fine		
		A term of imprisonment from 1 to 4 years		
Malicious Code	1.10/95 art 264 para 2: a person who, by any means destroys, alters or makes unusable electronic data, programs or documents of another person's contents in networks or in computer system	A fine		
		A term of imprisonment from 1 to 3 years		
Denial of Service	1.10/95 art 264 para 2: a person who, by any means destroys, alters or makes unusable electronic data, programs or documents of another person's contents in networks or in computer system	A fine		
		A term of imprisonment from 1 to 3 years		
Account Compromise	L.10/95 art 197 para: a person who, without	A fine		

	authorisation, seizes, uses or modifies to the detriment of a third party, such private, personal or family data of another individual as may be recorded on computer, electronically or by other medium, or in any type of file or record, whether public or private shall be guilty of an offence	A term of imprisonment from 1 to 4 years		
Intrusion Attempt	L.10/95 art 197 para: a person who, without authorisation, seizes, uses or modifies to the detriment of a third party, such private, personal or family data of another individual as may be recorded on computer, electronically or by other medium, or in any type of file or record, whether public or private shall be guilty of an offence	A fine		
		A term of imprisonment from 1 to 4 years		

Unauthorised Access to Information	L.10/95 art 197 para 1: it is unlawful to discover the secrets or to violate the privacy another without the consent of the latter, or to take possession of that individual's papers, letters, electronic mail, message or any other personal documents. It is also unlawful to intercept his or her telecommunications or to use technical devices for listening, transmitting, recording or reproducing sounds or images or any other communication signal L. 10/95 art 197 para 2: a person who, without authorisation, seizes use or modifies to the detriment of a third party, such private personal or family data of another individual as may be recorded on computer, electronically or by other medium, or in any type of file or record, whether public or private shall be guilty of an offence.	A fine		
		A term of imprisonment from 1 to 4 years		
Unauthorised Access to Transmissions	L.10/95 art 197 para 1: it is unlawful to discover the secrets or to violate the	A fine		

	privacy another without the consent of the latter, or to take possession of that individual's papers, letters, electronic mail, message or any other personal documents. It is also unlawful to intercept his or her telecommunications or to use technical devices for listening, transmitting, recording or reproducing sounds or images or any other communication signal	A term of imprisonment from 1 to 4 years		
Unauthorised Modification of Information	L. 10/95 art 197 para 2: a person who, without authorisation, seizes use or modifies to the detriment of the a third party, such private personal or family data of another individual as may be recorded on computer, electronically or by other medium, or in any type of file or record, whether public or private shall be guilty of an offence	A fine		
		A term of imprisonment from 1 to 4 years		
Unauthorised Access to Communication System	L. 10/95 art 197 para 2: a person who, without authorisation, seizes use or modifies to the detriment of a third party , such private personal or family data of another individual as may be recorded on computer, electronically or by other medium, or in any type of file or record, whether public or private shall be guilty of an offence	A fine		
		A term of imprisonment from 1 to 4 years		

Forensics

Reporting & Law Enforcement Organisations

Cuerpo Nacional de Policia.
Comisaria General de Policia Judical
Unidad Central de Policia Judicial
Unidad de Investigation de la Delincuencia en Tecnologias de la Informacion
(PAGINA PRINCIPAL DE LA BRIGADA DE INVESTIGACIÓN TECNOLÓGICA.)
C/ Julian Gonzalez Segador s/n 28043,
Madrid,
Spain
T: +34 91.5822753
+34 91 5822755
+34 91 5822848
F: +34 91 5822756
E: delitos.tecnologicos@policia.es
W: www.mir.es/policia/uiti/

Guardia Civil – Departamento de Delitos de Alta Tecnología
E: uco@gcivil.mir.es
W: www.guardiacivil.org/

Data Protection Agency (Agencia de Protección de Datos)
C/ Sagasta, 22
28004 Madrid
W: https://www.agenciaprotecciondatos.org/

The Technical Investigation Agency (Brigade of Technological Investigation) was formed in 2000 to execute, co-ordinate and carry out investigations relating to technology and computer crime. It deals with both content and computer related crime.

Other Reporting Mechanisms

None

Sweden

Sweden is a constitutional law country. Sweden has two parallel types of court - general courts, which deal with criminal and civil matters, and general administrative courts, which deal with administrative matters. There are three levels of general courts - the district courts (*tingsrätt*), the courts of appeal (*hovrätt*) and the Supreme Court (*Högsta domstolen*). There are also three levels of administrative courts – the county courts (*länsrätt*), the administrative courts of appeal (*kammarrätt*) and the Supreme Administrative Court (*Regeringsrätten*).

A free or informal system of evidence exists in Sweden. Digital evidence in Sweden can be submitted under standard documentary evidence rules or as separate evidence.

Each of Sweden's 21 police state departments has trained computer crime investigators. A national capability is provided by the IT Crime Squad, based at the National Criminal Investigation Department.

Legislation

Penal Code Ch 4 sec. 8 – 9 – 9 a –9 b –9 c | Ch 12 sec. 1 – 3 | Ch 13 sec. 4 – 5

CIA Offences in Sweden are mainly managed through the Swedish Penal Code and in particular through chapter 4 which deals with "Crime Against Liberty and Peace", chapter 12 which deals with "Crime Inflicting Damage" and chapter 13 that deals with "Crimes Involving public Danger".

Chapter 4 of the Swedish Penal Code is the one most frequently used to handle CIA Offences. Sec 8 deals with the *"breach of postal or telecommunication secrecy*": it is a provision dealing with unauthorised access to a communication or its unauthorised interception.

Other provisions relating to CIA offences are sec 9, 9 a and 9 c of the same chapter. In particular, sec 9 deals with *"intrusion into a safe depository*" establishing that it is an offence to open letters or telegrams or to otherwise obtain access to something kept under seal or lock or otherwise enclosed.

Sec 9a establishes that it is an offence to unlawfully and secretly listen to or record by technical means for sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which the person doing the listening has improperly obtained access. All these conducts are defined as *"eavesdropping"*.

Sec 9 c deals with the *"breach of data secrecy"*, the case in which a person unlawfully obtains access to record automatic data processing activities or unlawfully alters or erases or inserts such a recording device.

Chapter 12 of the Swedish Penal Code deals with the infliction of damage: the first section deals with persons who destroy or damage property to the detriment of another's right thereto. The penalty provided is a fine or a term of imprisonment up to 6 months. The third section of the article deals with causing serious damage that causes a risk to anyone's life or health. In this case the penalty is a term of imprisonment of up to 4 years.

Another important chapter of the Swedish Penal Code that has to be taken into consideration in relation to CIA Offences is Ch. 13 which deals in general with "Crimes Involving Public Danger."

Ch 13 Sec 4 establishes that a person who destroys or damages property of considerable importance for the defence of the Realm, public subsistence, the administration of justice or public administration, or the maintenance of public order and security in the Realm, or by some other action, not limited to the withholding of labour or encouraging such action, seriously disrupts or obstructs the use of such property, shall be sentenced for sabotage.

This provision also applies to someone who destroys or damages or seriously disrupts or obstructs public traffic or the use of telegraph, telephone, radio or other similar public services or use of an installation for the supply of water, light, heat or power to the public. The penalty for this offence is a term of imprisonment up to 4 years.

Sec 5 of chapter 13 deals with the serious sabotage, a sabotage that could cause serious danger to the Realm, or to the lives of a number of persons or to property of special importance. The penalty for this offence is a term of imprisonment from 2 to 10 years or life.

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Target Fingerprinting			Ch 4 sec 8: A person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the form of mail or as a telecommunication, shall be sentenced for *breech of postal telecommunication secrecy* Ch 4 sec 9: A person who, in a case not covered by section 8, unlawfully opens a letter or a telegram or otherwise obtains access to something kept under seal or lock or otherwise enclosed, shall be sentenced for *intrusion into a safe depository* Ch 4 sec 9a: A person who in a case other than as stated in Section 8, unlawfully and secretly listens to records by technical means for sound reproduction speech in a room, a conversation between others or discussions at a conference or other meting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for *eavesdropping* Ch 4 sec 9 c: A person who, in cases other then	A fine A term of imprisonment of up to 2 years

			those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes information that is being processed by electronic or similar means for use with automatic data processing.	
Malicious Code		.	Ch 13 Sec 4: A person who destroys or damages property of considerable importance for the defence of the Realm, public subsistence, the administration of justice or public administration, or the maintenance of public order and security in the Realm, or by some other action, not limited to the withholding of labour or encouraging such action, seriously disturbs or obstructs the use of such property, shall be sentenced for *sabotage*. This shall also apply, if a person otherwise, by inflicting damage or by other action of the type described above, seriously disturbs or obstructs public traffic or the use of telegraph, telephone radio or other similar public service or use of an installation for the supply of water, light, heat or power to the public	A term of imprisonment of up to 4 years

			Ch 13 sec 5: If a crime as defined in section 4 is considered gross, imprisonment for at least two and at most ten years, or for life, shall be imposed for gross sabotage. In assessing whether the crime is gross, special attention shall be paid to whether it caused danger to the security of the Realm, to the lives of a number of persons, or to property of special importance	A term of imprisonment from 2 to 10 years or life
			Ch12 sec 1: A person who destroys or damages property, real or moveable to the detriment of another's right thereto shall be sentenced for *inflicting damage*	A fine
				A term of imprisonment of up to 6 months
			Ch 12 sec 3: If the crime defined in section 1 is regarded as gross, imprisonment for at most four years shall be imposed for *gross infliction of damage.* In assessing whether the crime is gross, special attention shall be paid to whether the act gave rise to an extreme risk anyone's life or health or the damage was to something of great cultural or financial importance or was otherwise a particularly keenly felt loss	A term of imprisonment of up to 4 years

Denial of Service			Ch 13 Sec 4: A person who destroys or damages property of considerable importance for the defence of the Realm, public subsistence, the administration of justice or public administration, or the maintenance of public order and security in the Realm, or by some other action, not limited to the withholding of labour or encouraging such action, seriously disturbs or obstructs the use of such property, shall be sentenced for *sabotage*. This shall also apply, if a person otherwise, by inflicting damage or by other action of the type described above, seriously disturbs or obstructs public traffic or the use of telegraph, telephone radio or other similar public service or use of an installation for the supply of water, light, heat or power to the public.	A term of imprisonment of 4 years
			Ch 13 sec 5: If a crime as defined in section 4 is considered gross, imprisonment for at least two and at most ten years, or for life, shall be imposed for *gross sabotage.* In assessing whether the crime is gross, special attention shall be paid to whether it caused danger to the security of the Realm, to the lives of a number of persons, or to property of special importance	A term of imprisonment from 2 to 10 years or for life
Account Compromise			Ch 4 sec 9 c: A person who, in cases other then those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a	A fine

			recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes information that is being processed by electronic or similar means for use with automatic data processing	A term of imprisonment for at most 2 years
Intrusion Attempt			Ch 4 sec 9 c: A person who, in cases other then those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes information that is being processed by electronic or similar means for use with automatic data processing	A fine A term of imprisonment for at most 2 years
Unauthorised Access to Information			h 4 sec 8: A person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the	A fine

			form of mail or as a telecommunication, shall be sentenced for *breech of postal telecommunication secrecy* Ch 4 sec 9: A person who, in a case not covered by section 8, unlawfully opens a letter or a telegram or otherwise obtains access to something kept under seal or lock or otherwise enclosed, shall be sentenced for *intrusion into a safe depository* Ch 4 sec 9a: A person who in a case other than as stated in Section 8, unlawfully and secretly listens to records by technical means for sound reproduction speech in a room, a conversation between others or discussions at a conference or other meting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for *eavesdropping* Ch 4 sec 9 c: A person who, in cases other then those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes information that is being processed by electronic or similar means for use with automatic data processing.	A term of Imprisonment of up to 2 years

Unauthorised Access to Transmissions			Ch 4 sec 8: A person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the form of mail or as a telecommunication, shall be sentenced for *breech of postal telecommunication secrecy* Ch 4 sec 9: A person who, in a case covered by section 8, unlawfully opens a letter o a telegram or otherwise obtains access to something kept under seal or lock or otherwise enclosed, shall be sentenced for *intrusion into a safe depository* Ch 4 sec 9a: A person who in a case other than as stated in Section 8, unlawfully and secretly listens to records by technical means for sound reproduction speech in a room, a conversation between others or discussions at a conference or other meting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for *eavesdropping*. Ch 4 sec 9 c: A person who, in cases other then those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes information that is being processed by electronic or similar means for use with automatic data processing.	A fine A term of imprisonment up to 2 years

Unauthorised Modification of Information			Ch 4 sec 9a: A person who in a case other than as stated in Section 8, unlawfully and secretly listens to records by technical means for sound reproduction speech in a room, a conversation between others or discussions at a conference or other meting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for *eavesdropping*	A fine A term of imprisonment up to 2 years
Unauthorised Access to Communication System			Ch 4 sec 9 c: A person who, in cases other then those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes information that is being processed by electronic or similar means for use with automatic data processing.	A fine A term of imprisonment up to 2 years

Forensics

A free or informal system of evidence exists in Sweden. This proves both a benefit and a problem for law enforcement as anything digital in nature can be submitted and the burden of proof rests on the evidence itself rather than adherence to procedural stipulations. Hence decisions can go one way or the other and are more acutely dependent on the testimony and performance of expert witnesses in explaining the relevance of the written evidence to the judge and jury.

Digital evidence in Sweden can be submitted under standard documentary evidence rules or as separate evidence (in the case of computer code or programs, for example). In the testimony of both law enforcement and expert witnesses, the need to preserve confidentiality about methods (particularly regarding encryption) is specifically highlighted in police training.

Internally within the Police, digital evidence and computer forensic best practice is taken from the Interpol CCM and a Swedish version, published openly by the National Police College called 'The Handbook for Search and Siezure'. Furthermore, use is made of an Interpol handbook on Internet monitoring.

Reporting & Law Enforcement Organisations

IT Crime Squad
National Criminal Investigation Department
Box 12256,
S-102 26
Stockholm,
Sweden
T: +46 8 4014525
F: +46 8 6505566
E: rikskriminalpolisen@rkp.police.se
W: http://www.rkp.police.se

Datainspektionen (Data Inspection Board)
Box 8114,
104 20
Stockholm
T: +46 08-657 61 00
F: +46 08-652 86 52
E: datainspektionen@datainspektionen.se
W: www.datainspektionen.se

There is great emphasis placed on Computer Crime awareness at the individual officer level in Law Enforcement in Sweden. All officers are given a basic understanding of computer crime and dealing with computer evidence (at a basic level) when they pass through Police College.

At the local level, there are 21 independent state police departments which cover geographic regions. In each unit there are 1 or 2 specially trained investigators. This may be more in the major departments with other local experts being present. Furthermore, each regional state unit is able to call upon the national unit for support if required. The IT crime squad forms part of the National Criminal Investigation Department. There are 15 officers in the Squad, which are a mix police and 'special profile techncians'. The IT Crime Squad is divided into subunits concerned with search and siezure and internet surveillence which mirrors the structure of other national units (e.g. the UK NHTCU).

The responsibilities are first and foremost to local police units in each state department, but also to international liasion, specifically with Interpol and Europol and the G-8 24/7 reporting point. This unit does not, however, cover national intelligence related liason regarding computer crime, which is handled by Swedish National Security (Sweden's internal intelligence agency).

In the Swedish National Forensic Laboratory there are five engineering staff who deal exclusively with computer forensics. They are a resource that can be called upon by the National unit and state forces.

The Police College undertakes a basic level of digital and computer evidence awareness in basic training but a special 13 week course also exists for specialist investigators. This consists of a 10 week introductory course with regards to computing and information technology, covering operation of Information Technology at an advanced level. A further 3 weeks provide training on legal considerations, software and forensic tools. Other advanced training courses are available on a topical basis (e.g. the rise in popularity of Distributed Denial of Service attacks). Opportunities are available for CSSIP qualification, but as the state departments pay for this, it is not mandatory.

The level of sophistication is quite high and outside civilian experts are only called in 5 to 6 times a year for specific assistance on investigations. The IT Crime Squad also co-operates with the military, intelligence services and other national research agencies (e.g. the FOA – Swedish Defence Research Establishment). This co-operation is normally along the lines of seminars and workshops as well as the more obvious operational assistance.

Some prioritisation of cases must go on as there is no capacity to cover all computer crime cases. Ongoing serious criminality is a large concern as is cases involving serious economic and financial loss and threat to life and health.

In 20023 there were about 600 investigations. Around 100 of these led to prosecutions, the majority of which were successful due to an policy insistence within the local police units in Sweden that no effort is expended on a case unless a high probability of success. However, there is no formal system in place to track the number of investigations that turn into successful prosecutions.

The IT Crime Squad is currently working on a series of handbooks and guidelines for the judiciary and legal professions, to try and raise awareness and improve education on the subject of presentation and interpretation of all forms of digital evidence.

United Kingdom

England and Wales are common law countries. The most distinctive feature of a common law country is that judge made law remains an important source of law. This is in contrast to civil law countries that have codified their laws with the result that legislation is the only source of law. There are many areas of English and Welsh law which have been codified or where case law has been overridden by express legislation, but in many areas such as contract law and damages judge made law remains predominant and an independent source of law. Scotland is not a common law jurisdiction, but generally uses the same criminal legislation as England and Wales and is increasingly tending towards a mix of common law and those on the statute books. English law also generally applies to Northern Ireland.

Common law is developed by individual judicial decisions. This is known as case law and precedent. Where a legal issue has been decided by a superior court lower courts are bound to follow it in subsequent cases.

Free/Informal evidentiary rules exist in the UK. There is no Criminal Code (since there is no written Constitution) but case law determines criminal activity, in addition to substantive law contained within thematic legislation.

There are 43 forces in England and Wales which include the largest force the Metropolitan Police. There are 8 forces in Scotland.

Other major forces include the British Transport Police who are responsible for the policing of the UK Rail Network. The Force is also responsible for policing the London Underground and some smaller local metro and tram systems.

The Police Service of Northern Ireland (formerly the Royal Ulster Constabulary or RUC) covers Northern Ireland

There are a number of Central Services such as the National Criminal Intelligence Service (NCIS) and the National Crime Squad.

The National Hi-Tech Crime Unit, which reports to the National Crime Squad, provides a national capability to deal with computer crime.

Legislation

Computer Misuse Act 1990; Regulation of Investigatory Powers Act 2000

The United Kingdom has a different legal system from the other EU Member States: it is based on Common Law, which is a different way of ruling law.

CIA Offences are mainly managed in the UK by the Computer Misuse Act (CMA), which was enacted in 1990 and it is largely composed of three paragraphs.

The first paragraph deals with “unauthorised access to computer material” and establishes that a person is guilty of an offence if he causes a computer to perform any function with the intent to secure access to any program or data held in any computer; the access he wants to secure is unauthorised and he knows, at the time he causes the computer to perform the function, that is the case.

UK law makes no distinction between computers and networks with security and those without.

To commit an offence, the access has to be made causing a computer to perform any function that:

1. alters or erases a program or data;
2. copies and moves the data onto a storage medium other than the one in which the data are held or to a different location in the storage medium where the data are held;
3. in general uses the data;
4. has an output of any kind.

The penalty for this offence could be a fine or a term of imprisonment not exceeding 6 months or both

The second paragraph of the CMA deals with the “unauthorised access with the intent to commit another offence” and establishes that a person is guilty of an offence under section 1 of the CMA, with the intent:
1. to commit an offence to which this section applies;
2. to facilitate the commission of such an offence (whether by himself or by another person), and the offence he intends to commit or facilitate is referred to below in this section as the further offence

In this section there is a different provision for the punishment: as in the previous section there is a penalty of a fine or a term of imprisonment up to 6 months, but there is also a provision for up to 5 years of imprisonment.

The third paragraph of the CMA deals with the “unauthorised modification of computer material” and establishes that a person is guilty of an offence if he does any act which causes an unauthorised modification of the contents of any computer and at the time when he does the act he has the requisite intent and the requisite knowledge.

The requisite is an intent to cause a modification of the contents of any computer in and by doing so, for example, impairs the operation of any computer, or prevents or hinders access to any program or data held in a computer, or impairs the operation of any such program or the reliability of any such data.

The intent need not be directed at any particular computer, or any particular program or data of any particular kind, or any particular modification of any kind.

The requisite knowledge, means that the offender knows that the modification he intends to cause is unauthorised.

The penalty in this section is the same of the second section.

The CIA Offences of Target Fingerprinting, Unauthorized Access to Information and Unauthorized Access to Transmission, are also managed by the Regulatory of Investigation Act 2000 (RIPA).

The first paragraph of this Act states that it is an offence to intercept intentionally and without authorization, any communication in the course of transmission by the means of "a public telecommunication system" (b).

Paragraph 2 of the article defines the meaning and (the localization) of private/public telecommunication system (2-1) and the meaning of interception: "a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he (2-2a) so modifies or interferes with the system, or its operation, (2-2b) so monitors transmissions made by means of the system, or (2-2c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system".

The RIPA 2000 states also that a person who is guilty of this offence shall be liable for a term of imprisonment not exceeding two years or to a fine, or to both, or on summary conviction, to a fine not exceeding the statutory maximum (par 7).

Incident Classification	Law		Criminal Code	
	Description	Punishment	Description	Punishment
Computer Fingerprinting	RIPA 2000 sec 1: A person is guilty of an offence if intentionally and without authorization intercepts any communication in the course of its transmission by means of (a) public postal service or (b) a public telecommunication system.	A fine Up to 2 years' imprisonment		
	CMA Sec 2. A person is guilty of an offence if: a) he causes a computer to perform any function with intent to secure access to any program or data held in a computer b) the access he intent to secure is unauthorised c) he knows at the time when he causes the computer to perform the function that this the case. 1(2) The intent a person has to commit an offence under this section need not be directed at a any particular program or data b a program or data of any particular kind c a program or data held in any particular computer	A fine Up to 6 months of imprisonment		
Malicious Code	CMA Sec 3: A person is guilty of an offence if: a) he does any act which causes the unauthorised modification of the contents of any computer and b) at the time when he does the act he has the requisite intent and the requisite knowledge 3(2) For the purposes of subsection 3(1) b above requisite intent is an intent to cause a modification of the contents of any computer and by so doing a) to impair the operation of any computer b) to prevent or hinder	A fine		

	access to any program or data held in any computer or c) impair the operation of any such program or the reliability of any such data 3(3) The intent need not be directed at a) any particular computer b) any particular program or data or a program or data of any particular kind c) any particular modification or modification of any particular kind 3(4) For the purpose of subsection 1b above, the requisite knowledge is knowledge that any modification he tends to cause is unauthorised. 3(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intent effect of it a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary	A term of imprisonment from 6 months to 5 years		
Denial of Service	CMA Sec 3: A person is guilty of an offence if: a) he does any act which caus es the unauthorised modification of the contents of any computer and b) at the time when he does the act he has the requisite intent and the requisite knowledge 3(2) For the purposes of subsection 3(1) b above requisite intent is an intent to cause a modification of the contents of any computer and by so doing a) to impair the operation of any computer	A fine		

	b) to prevent or hinder access to any program or data held in any computer or c) impair the operation of any such program or the reliability of any such data 3(3) The intent need not be directed at a) particular computer b) any particular program or data or a program or data of any particular kind c) any particular modification or modification of any particular kind 3(4) For the purpose of subsection 1b above, the requisite knowledge is knowledge that any modification he tends to cause is unauthorised. 3(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intent effect of it a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary	A term of imprisonment from 6 months to 5 years		
Account Compromise	CMA Sec 1: A person is guilty of an offence if a) he causes a computer to perform any function with intent to secure access to any program or data held in a computer b) the access he intends to secure is unauthorised or c) he knows at the time when he causes the computer to perform the function that this is the case 1(2) The intent a person has to commit an offence under this section need not be directed at a) any particular program or data b) a program or data of any particular kind or c) a program or data or data in any particular computer	A fine A term of imprisonment not exceeding 6 months		

Intrusion Attempt	CMA Sec 1: A person is guilty of an offence if a) he causes a computer to perform any function with intent to secure access to any program or data held in a computer b) the access he intends to secure is unauthorised or c) he knows at the time when he causes the computer to perform the function that this is the case 1(2) The intent a person has to commit an offence under this section need not be directed at a) any particular program or data b) a program or data of any particular kind or c) a program or data or data in any particular computer	A fine A term of imprisonment not exceeding 6 months		
Unauthorised Access to Information	RIPA 2000 sec 1: A person is guilty of an offence if intentionally and without authorization intercepts any communication in the course of its transmission by means of (a) public postal service or (b) a public telecommunication system.	A fine A term of imprisonment up to 2 years		
	CMA Sec 1: A person is guilty of an offence if a) he causes a computer to perform any function with intent to secure access to any program or data held in a computer b) the access he intends	A fine		

	to secure is unauthorised or c) he knows at the time when he causes the computer to perform the function that this is the case 1(2) The intent a person has to commit an offence under this section need not be directed at a) any particular program or data b) a program or data of any particular kind or c) a program or data or data in any particular computer	A term of imprisonment up to 5 years		
Unauthorised Access to Transmissions	RIPA 2000 sec 1: A person is guilty of an offence if intentionally and without authorization intercepts any communication in the course of its transmission by means of (a) public postal service or (b) a public telecommunication system.	A fine A term of imprisonment of up to 2 years		
Unauthorised Modification of Information	CMA Sec 3: A person is guilty of an offence if: a) he does any act which causes the unauthorised modification of the contents of any computer and b) at the time when	A fine		

	he does the act he has the requisite intent and the requisite knowledge 3(2) For the purposes of subsection 3(1) b above requisite intent is an intent to cause a modification of the contents of any computer and by so doing a) to impair the operation of any computer b) to prevent or hinder access to any program or data held in any computer or c) impair the operation of any such program or the reliability of any such data 3(3) The intent need not be directed at a) any particular computer b) any particular program or data or a program or data of any particular kind or c) any particular modification or modification of any particular kind 3(4) For the purpose of subsection 1b above, the requisite knowledge is knowledge that any modification he tends to cause is unauthorised. 3(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intent effect of it a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary	A term of imprisonment from 6 months to 5 years		
Unauthorised Access to Communication System	CMA Sec 1: A person is guilty of an offence if a) he causes a computer to perform any function with intent to secure access to any program or data held in a computer b) the access he intends to secure is unauthorised or c) he knows at the time when he causes the computer to perform the function that this is the case 1(2) The intent a person	A fine A term of imprisonment not exceeding 6 months		

	has to commit an offence under this section need not be directed at a) any particular program or data b) a program or data of any particular kind or c) a program or data or data in any particular computer			

Forensics

Evidence collection is governed by the Police and Criminal Evidence Act 1984 (PACE 84) and guidelines set out in publications such as the Association of Chief Police Officers (ACPO) 'Good Practice Guide for Computer Based Evidence' and the Interpol Computer Crime Manual.

Computer evidence is widely accepted in the criminal justice system and has been used in many prosecutions.

Generally speaking in the UK, computer evidence falls under the same rules as other evidence. That is to say, according to the rules of Documentary Evidence,

> '...the onus is on the prosecution to show to the court that the evidence produced is no more and no less than when it was first taken into the possession of police.'

The ACPO Good Practice Guide states that investigators should be careful to ensure that no data change takes place on media that is expected to be relied upon in court. No access of original data must take place and all investigative work must be completed on an image of the drive. In circumstances where it is necessary to access original data held on a target computer, the person doing so must be competent to do so and must be prepared to give evidence explaining his actions. The guide establishes that care must be taken to preserve a chain of custody and an audit trail of all process applied to computer based evidence, which should be examinable by a third party who should be able to come to the same result. Responsibility for adherence to these principles is placed with the principle investigating officer.

There is a high degree of expertise in forensic investigation in the United Kingdom and two universities run special course for forensic investigators. In addition, law enforcement can call upon a dynamic and thriving commercial market of forensic investigation specialists as well as formidable national resources held by national intelligence agencies. Outsourced commercial digital forensic investigators play a small but not rare role in providing expert testimony and other expertise to law enforcement.

Reporting & Law Enforcement Organisations

National Hi-Tech Crime Unit
PO Box 10101
London E14 9NF
T: +44 (0)870 241 0549
F: +44 (0)870 241 5729
E: admin@nhtcu.org
W: www.nhtcu.org

Information Commissioner
Wycliffe House
Water Lane

Wilmslow
Cheshire
SK9 5AF
T: 01625 545 740
01625 545 745
F: 01625 524 510
E: data@dataprotection.gov.uk
W: http://www.informationcommissioner.gov.uk

In the United Kingdom there is now a single Law Enforcement authority – the National Hi-Tech Crime Unit (NHCTU) – responsible for investigation of cyber-crime. This was formed in April 2001 to be the central point of contact, for cyber-crime investigations. It is staffed by personnel from the National Crime Squad, National Criminal Intelligence Service and HM Customs and Excise. The Unit also undertakes a liaison role with other computer crime units in UK regional police forces (Constabularies).

The Unit has four separate arms:

- Investigations
- Intelligence
- Tactical and Technical Support
- Digital Evidence (Forensic Retrieval)

NHTCU has two separate areas of note in its forensics arm:

Network Monitoring: Monitoring and investigation of traffic in a dynamic real time environment

Hard disk investigation: Forensic procedures based around the forensic examination of seized hard disks.

The NHCTU can also call upon the resources of national intelligence agencies and research organisations if required – specifically QinetiQ (formerly part of the Defence Evaluation and Research Agency) and DSTL (Defence Science and Technology Laboratories) and the Government Communications Head Quarters (GCHQ).

The NHTCU has established a Confidential Reporting Charter designed to allay concerns voiced by businesses and commercial organisations that notification of computer security incidents will invariably result in adverse publicity. This has had some success of late, and the Unit is putting much effort into outreach to commercial stakeholders.

In addition to the national unit, there are individual Computer Crime Units, dealing with Computer and Content related crimes, in each constabulary. The most experienced of these is the Metropolitan Police's Computer Crime Unit.

The Metropolitan Police Unit is part of the Specialist Crime operational command unit within the Metropolitan Police's Specialist Operations

Command. The Computer Crime Unit works together with other specialist units, both within the Metropolitan Police and at a national and international level.

In addition, the UK Forensic Science Service maintains expertise in digital evidence, although it is believed their expertise is less called upon with the advent of the national unit.

Other Reporting Mechanisms

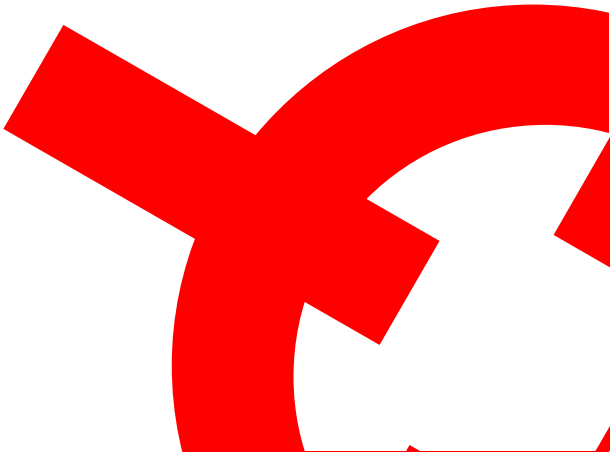
In addition to the formal channels through Law Enforcement there are a number of additional reporting processes being established. Chief of these is the Warning Advice and Reporting Point (WARP) concept, developed by the National Infrastructure Security Co-ordination Centre (NISCC). London Connects (an organisation designed to deliver e-Government to Greater London) has piloted the first WARP.[56] NISCC itself provides a reporting channel for the collection of intelligence, particularly from critical industry sectors.

In addition to these mechanisms, the Internet Watch Foundation (IWF) is an independent body responsible for reporting of illegal (child pornography or criminally racist) content.

The Information Commissioner can be referred to in the instance of the use and exploitation of personally identifiable information. Similarly, local Trading Standards bodies afford some level of consumer protection in regard to online activities (goods and services).

[56] http://www.lcwarp.org

Glossary and Links



Glossary

Attack: a series of steps taken by an attacker to achieve an unauthorized result"[57]

Attacker: an individual who attempts one or more attacks in order to achieve an objective"[58]

Computer data: any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function. [59]

Evidence: an indication, a sign, the facts available as proving or supporting a notion"[60]; "information given personally or drawn from a document etc. and tending to give a fact; testimony; admissible in court"[61]

Event "An action directed at a target which is intended to result in a change of state (status) of the target" [(IEEE96:373)[62]

Information System: any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance. [63]

IT security incident: Any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability [NIST-800-3]

Legal person: any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations. [64]

Target: a computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork"[65]

Victim: a person who is injured or killed by another or as a result of an event or circumstance[66]

---

[57] *A Common Language for Computer Security Incidents;* John D. Howard amd Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]

[58] *A Common Language for Computer Security Incidents;* John D. Howard amd Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]

[59] *Council Framework Decision on attacks against information systems* (12 May 2003)

[60] *The Oxford Reference Dictionary;* Oxford University Press, 1986

[61] *The Oxford Reference Dictionary;* Oxford University Press, 1986

[62] *A Common Language for Computer Security Incidents;* John D. Howard amd Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]

[63] *Council Framework Decision on attacks against information systems* (12 May 2003)

[64] *Council Framework Decision on attacks against information systems* (12 May 2003)

[65] *A Common Language for Computer Security Incidents;* John D. Howard amd Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]

[66] *The Oxford Reference Dictionary;* Oxford University Press, 1986

Vulnerability: a weakness in a system allowing unauthorized action [(NRC91:301; Amo94:2)[67]
Without right: access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under domestic legislation.[68]

[67] *A Common Language for Computer Security Incidents;* John D. Howard amd Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]
[68] *Council Framework Decision on attacks against information systems* (12 May 2003)

Quick Links and Sources

Online Resources

TF-CSIRT (Task Force Computer Security Incident Response Teams) available at:
http://www.terena.nl/tech/task-forces/tf-csirt/ (visited 18th June 2003)

Cyber Tools Online Search for Evidence (CTOSE) IST-32624 available at:
http://www.ctose.org (visited 18th June 2003)

Forum of Incident Response Teams (FIRST) available at:
http://www.first.org (visited 18th June 2003)

Digital Signature Law Survey, Simone van der Hof, University of Tilburg, Netherlands February 2003 available at:
http://rechten.kub.nl/simone/ds-lawsu.htm (visited 18th June 2003)

Crypto Law Survey version 21.0, Bert Jaap Koops, University of Tilburg, Netherlands October 2002 available at:
http://rechten.uvt.nl/koops/cryptolaw/index.htm (visited 18th June 2003)

Checklist of Legal Issues DFN Society available at
http://www.dfn.de/service/ra/checkliste/ChecklisteRZ.html

The Association of Internet Hotline Providers in Europe (INHOPE) available at: http://www.inhope.org/ (visited 23rd June 2003)

Report on Second Training Workshop Deliverable No D3 - Annex A – Training Materials TRANSITS (Training of Network Security Incident Teams Staff) IST-2001-39118 TERENA (Trans-European Networking Association) June 2003. Report available at http://www.ist-transits.org

RFC2350 Best Current Practice; Expectations for Computer Security Incident Response; N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, June 1998

RFC2828 Internet Security Glossary by R. Shirey. May 2000.

Guidelines for Evidence Collection and Archiving by Dominique Brezinski, Tom Killalea - July 2000. available at: http://www.terena.nl/tech/projects/cert/i-taxonomy/archive/draft-ietf-grip-prot-evidence-01.txt (visited 18th June 2003)

EU Data Protection Surveys Matrix, 2002, Coudert Brothers LLP

European Directory of Hotlines for Reporting Inappropriate Content, European Commission 2002, available at:
http://europa.eu.int/information_society/programmes/iap/projects/hotlines/index_en.htm (visited 23rd June 2003)

Legal Texts

Austrian Penal Code (Austrian)

http://www.sbg.ac.at/ssk/docs/stgb/stgb_index.htm

Belgium

http://www.moniteur.be/index_fr.htm (Source du Droit - Legislation consolidée)

Denmark

No references

Finnish Penal Code (English)

http://wings.buffalo.edu/law/bclc/finnish.htm

France Penal Code (France)

http://www.adminet.com/code/index-CPENALLL.html

German Penal Code (German /English)

http://wings.buffalo.edu/law/bclc/StGBframe.htm

German Penal Code (German only)

http://www.bib.uni-mannheim.de/bereiche/jura/gesetze/stgb-inh.html

Ireland

http://www.bailii.org/ie/legis/num_act/

Italy

http://www.usl4.toscana.it/dp/isll/lex/cp.htm

Greece

http://www.et.gr/

Luxembourg

http://www.etat.lu/LEGILUX/DOCUMENTS_PDF/CODES/CODE_PENAL/CodePenal_PageAccueil.pdf

Portuguese Penal Code (Portuguese)

http://www.cea.ucp.pt/lei/penal/penalind.htm

Dutch Penal Code (Dutch)

http://www.win.tue.nl/~aeb/jura/Strafrecht/Wetboek_van_Strafrecht/

Spain

http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

Sweden

http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf

UK

http://www.uk-legislation.hmso.gov.uk/acts.htm#acts

Hardcopy Resources

Interpol Computer Crime Manual Interpol, November 2000

Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations - "Search and Seizure Manual" Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, US Department of Justice, July 2002

Good Practice Guide for Computer Based Evidence Version 2.0 Association of Chief Police Officers Computer Crime Group, London, June 1999

A Common Language for Computer Security Incidents; John D. Howard amd Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]

The Oxford Reference Dictionary; Oxford University Press, 1986

Annexes

Annex A

International and European Supranational Law relating to Privacy and Data Protection

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11

Rome, 4.XI.1950

The text of the Convention had been amended according to the provisions of Protocol No. 3 (ETS No. 45), which entered into force on 21 September 1970, of Protocol No. 5 (ETS No. 55), which entered into force on 20 December 1971 and of Protocol No. 8 (ETS No. 118), which entered into force on 1 January 1990, and comprised also the text of Protocol No. 2 (ETS No. 44) which, in accordance with Article 5, paragraph 3 thereof, had been an integral part of the Convention since its entry into force on 21 September 1970. All provisions which had been amended or added by these Protocols are replaced by Protocol No. 11 (ETS No. 155), as from the date of its entry into force on 1 November 1998. As from that date, Protocol No. 9 (ETS No. 140), which entered into force on 1 October 1994, is repealed and Protocol No. 10 (ETS No. 146) has lost its purpose.

The governments signatory hereto, being members of the Council of Europe,

Considering the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10th December 1948;

Considering that this Declaration aims at securing the universal and effective recognition and observance of the Rights therein declared;

Considering that the aim of the Council of Europe is the achievement of greater unity between its members and that one of the methods by which that aim is to be pursued is the maintenance and further realisation of human rights and fundamental freedoms;

Reaffirming their profound belief in those fundamental freedoms which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the human rights upon which they depend;

Being resolved, as the governments of European countries which are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law, to take the first steps for the collective enforcement of certain of the rights stated in the Universal Declaration,

Have agreed as follows:

Article 1 – Obligation to respect human right

The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.

Section I – Rights and freedoms

Article 2 – Right to life

Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which this penalty is provided by law.

Deprivation of life shall not be regarded as inflicted in contravention of this article when it results from the use of force which is no more than absolutely necessary:

a. in defence of any person from unlawful violence;
b. in order to effect a lawful arrest or to prevent the escape of a person lawfully detained;
c. in action lawfully taken for the purpose of quelling a riot or insurrection.

Article 3 – Prohibition of torture[1]

No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

Article 4 – Prohibition of slavery and forced labour[1]

No one shall be held in slavery or servitude.

No one shall be required to perform forced or compulsory labour.

For the purpose of this article the term "forced or compulsory labour" shall not include:

a. any work required to be done in the ordinary course of detention imposed according to the provisions of Article 5 of this Convention or during conditional release from such detention;
b. any service of a military character or, in case of conscientious objectors in countries where they are recognised, service exacted instead of compulsory military service;
c. any service exacted in case of an emergency or calamity threatening the life or well-being of the community;
d. any work or service which forms part of normal civic obligations.

Article 5 – Right to liberty and security[1]

Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:
a. the lawful detention of a person after conviction by a competent court;
b. the lawful arrest or detention of a person for non-compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law;
c. the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so;
d. the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority;
e. the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants;
f. the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition.

Everyone who is arrested shall be informed promptly, in a language which he understands, of the reasons for his arrest and of any charge against him.

Everyone arrested or detained in accordance with the provisions of paragraph 1.c of this article shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial.

Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful.

Everyone who has been the victim of arrest or detention in contravention of the provisions of this article shall have an enforceable right to compensation.

Article 6 – Right to a fair trial[1]

In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

Everyone charged with a criminal offence has the following minimum rights:
a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
b. to have adequate time and facilities for the preparation of his defence;
c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 7 – No punishment without law[1]

No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed.

This article shall not prejudice the trial and punishment of any person for any act or omission which, at the time when it was committed, was criminal according to the general principles of law recognised by civilised nations.

Article 8 – Right to respect for private and family life[1]

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 9 – Freedom of thought, conscience and religion[1]

Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.

Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.

Article 10 – Freedom of expression[1]

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 11 – Freedom of assembly and association[1]

Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national

security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.

Article 12 – Right to marry[1]
Men and women of marriageable age have the right to marry and to found a family, according to the national laws governing the exercise of this right.
Article 13 – Right to an effective remedy[1]
Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.
Article 14 – Prohibition of discrimination[1]
The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.
Article 15 – Derogation in time of emergency[1]

In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Articles 3, 4 (paragraph 1) and 7 shall be made under this provision.

Any High Contracting Party availing itself of this right of derogation shall keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefor. It shall also inform the Secretary General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed.

Article 16 – Restrictions on political activity of aliens
Nothing in Articles 10, 11 and 14 shall be regarded as preventing the High Contracting Parties from imposing restrictions on the political activity of aliens.
Article 17 – Prohibition of abuse of rights[1]
Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.
Article 18 – Limitation on use of restrictions on rights[1]
The restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.
Section II – European Court of Human Rights[2]
Article 19 – Establishment of the Court
To ensure the observance of the engagements undertaken by the High Contracting Parties in the Convention and the Protocols thereto, there shall be set up a European Court of Human Rights, hereinafter referred to as "the Court". It shall function on a permanent basis.
Article 20 – Number of judges
The Court shall consist of a number of judges equal to that of the High Contracting Parties.
Article 21 – Criteria for office

The judges shall be of high moral character and must either possess the qualifications required for appointment to high judicial office or be jurisconsults of recognised competence.

The judges shall sit on the Court in their individual capacity.

During their term of office the judges shall not engage in any activity which is incompatible with their independence, impartiality or with the demands of a full-time office; all questions arising from the application of this paragraph shall be decided by the Court.

Article 22 – Election of judges

The judges shall be elected by the Parliamentary Assembly with respect to each High Contracting Party by a majority of votes cast from a list of three candidates nominated by the High Contracting Party.

The same procedure shall be followed to complete the Court in the event of the accession of new High Contracting Parties and in filling casual vacancies.

Article 23 – Terms of office

The judges shall be elected for a period of six years. They may be re-elected. However, the terms of office of one-half of the judges elected at the first election shall expire at the end of three years.

The judges whose terms of office are to expire at the end of the initial period of three years shall be chosen by lot by the Secretary General of the Council of Europe immediately after their election.

In order to ensure that, as far as possible, the terms of office of one-half of the judges are renewed every three years, the Parliamentary Assembly may decide, before proceeding to any subsequent election, that the term or terms of office of one or more judges to be elected shall be for a period other than six years but not more than nine and not less than three years.

In cases where more than one term of office is involved and where the Parliamentary Assembly applies the preceding paragraph, the allocation of the terms of office shall be effected by a drawing of lots by the Secretary General of the Council of Europe immediately after the election.

A judge elected to replace a judge whose term of office has not expired shall hold office for the remainder of his predecessor's term.

The terms of office of judges shall expire when they reach the age of 70.

The judges shall hold office until replaced. They shall, however, continue to deal with such cases as they already have under consideration.

Article 24 – Dismissal

No judge may be dismissed from his office unless the other judges decide by a majority of two-thirds that he has ceased to fulfil the required conditions.

Article 25 – Registry and legal secretaries

The Court shall have a registry, the functions and organisation of which shall be laid down in the rules of the Court. The Court shall be assisted by legal secretaries.

Article 26 – Plenary Court

The plenary Court shall:

a. elect its President and one or two Vice-Presidents for a period of three years; they may be re-elected;
b. set up Chambers, constituted for a fixed period of time;
c. elect the Presidents of the Chambers of the Court; they may be re-elected;
d. adopt the rules of the Court, and
e. elect the Registrar and one or more Deputy Registrars.

Article 27 – Committees, Chambers and Grand Chamber

To consider cases brought before it, the Court shall sit in committees of three judges, in Chambers of seven judges and in a Grand Chamber of seventeen judges. The Court's Chambers shall set up committees for a fixed period of time.

There shall sit as an *ex officio* member of the Chamber and the Grand Chamber the judge elected in respect of the State Party concerned or, if there is none or if he is unable to sit, a person of its choice who shall sit in the capacity of judge.

The Grand Chamber shall also include the President of the Court, the Vice-Presidents, the Presidents of the Chambers and other judges chosen in accordance with the rules of the Court. When a case is referred to the Grand Chamber under Article 43, no judge from the Chamber which rendered the judgment shall sit in the Grand Chamber, with the exception of

the President of the Chamber and the judge who sat in respect of the State Party concerned.

Article 28 – Declarations of inadmissibility by committees
A committee may, by a unanimous vote, declare inadmissible or strike out of its list of cases an application submitted under Article 34 where such a decision can be taken without further examination. The decision shall be final.
Article 29 – Decisions by Chambers on admissibility and merits

If no decision is taken under Article 28, a Chamber shall decide on the admissibility and merits of individual applications submitted under Article 34.

A Chamber shall decide on the admissibility and merits of inter-State applications submitted under Article 33.

The decision on admissibility shall be taken separately unless the Court, in exceptional cases, decides otherwise.

Article 30 – Relinquishment of jurisdiction to the Grand Chamber
Where a case pending before a Chamber raises a serious question affecting the interpretation of the Convention or the protocols thereto, or where the resolution of a question before the Chamber might have a result inconsistent with a judgment previously delivered by the Court, the Chamber may, at any time before it has rendered its judgment, relinquish jurisdiction in favour of the Grand Chamber, unless one of the parties to the case objects.
Article 31 – Powers of the Grand Chamber
The Grand Chamber shall:

a. determine applications submitted either under Article 33 or Article 34 when a Chamber has relinquished jurisdiction under Article 30 or when the case has been referred to it under Article 43; and
b. consider requests for advisory opinions submitted under Article 47.

Article 32 – Jurisdiction of the Court

The jurisdiction of the Court shall extend to all matters concerning the interpretation and application of the Convention and the protocols thereto which are referred to it as provided in Articles 33, 34 and 47.

In the event of dispute as to whether the Court has jurisdiction, the Court shall decide.

Article 33 – Inter-State cases
Any High Contracting Party may refer to the Court any alleged breach of the provisions of the Convention and the protocols thereto by another High Contracting Party.
Article 34 – Individual applications
Chart of Declarations under former Articles 25 and 46 of the ECHR
The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.
Article 35 – Admissibility criteria

The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognised rules of international law, and within a period of six months from the date on which the final decision was taken.

The Court shall not deal with any application submitted under Article 34 that:

a. is anonymous; or
b. is substantially the same as a matter that has already been examined by the Court or has already been submitted to another procedure of international investigation or settlement and contains no relevant new information.

The Court shall declare inadmissible any individual application submitted under Article 34 which it considers incompatible with the provisions of the Convention or the protocols thereto, manifestly ill-founded, or an abuse of the right of application.

The Court shall reject any application which it considers inadmissible under this Article. It may do so at any stage of the proceedings.

Article 36 – Third party intervention

In all cases before a Chamber or the Grand Chamber, a High Contracting Party one of whose nationals is an applicant shall have the right to submit written comments and to take part in hearings.

The President of the Court may, in the interest of the proper administration of justice, invite any High Contracting Party which is not a party to the proceedings or any person concerned who is not the applicant to submit written comments or take part in hearings.

Article 37 – Striking out applications

The Court may at any stage of the proceedings decide to strike an application out of its list of cases where the circumstances lead to the conclusion that:

a. the applicant does not intend to pursue his application; or
b. the matter has been resolved; or
c. for any other reason established by the Court, it is no longer justified to continue the examination of the application.

However, the Court shall continue the examination of the application if respect for human rights as defined in the Convention and the protocols thereto so requires.

The Court may decide to restore an application to its list of cases if it considers that the circumstances justify such a course.

Article 38 – Examination of the case and friendly settlement proceedings

If the Court declares the application admissible, it shall:

a. pursue the examination of the case, together with the representatives of the parties, and if need be, undertake an investigation, for the effective conduct of which the States concerned shall furnish all necessary facilities;
b. place itself at the disposal of the parties concerned with a view to securing a friendly settlement of the matter on the basis of respect for human rights as defined in the Convention and the protocols thereto.

Proceedings conducted under paragraph 1.b shall be confidential.

Article 39 – Finding of a friendly settlement

If a friendly settlement is effected, the Court shall strike the case out of its list by means of a decision which shall be confined to a brief statement of the facts and of the solution reached.

Article 40 – Public hearings and access to documents

Hearings shall be in public unless the Court in exceptional circumstances decides otherwise.

Documents deposited with the Registrar shall be accessible to the public unless the President of the Court decides otherwise.

Article 41 – Just satisfaction

If the Court finds that there has been a violation of the Convention or the protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.

Article 42 – Judgments of Chambers

Judgments of Chambers shall become final in accordance with the provisions of Article 44, paragraph 2.

Article 43 – Referral to the Grand Chamber

Within a period of three months from the date of the judgment of the Chamber, any party to the case may, in exceptional cases, request that the case be referred to the Grand Chamber.

A panel of five judges of the Grand Chamber shall accept the request if the case raises a serious question affecting the interpretation or application of the Convention or the protocols thereto, or a serious issue of general importance.

If the panel accepts the request, the Grand Chamber shall decide the case by means of a judgment.

Article 44 – Final judgments

The judgment of the Grand Chamber shall be final.

The judgment of a Chamber shall become final:

a. when the parties declare that they will not request that the case be referred to the Grand Chamber; or
b. three months after the date of the judgment, if reference of the case to the Grand Chamber has not been requested; or
c. when the panel of the Grand Chamber rejects the request to refer under Article 43.

The final judgment shall be published.

Article 45 – Reasons for judgments and decisions

Reasons shall be given for judgments as well as for decisions declaring applications admissible or inadmissible.

If a judgment does not represent, in whole or in part, the unanimous opinion of the judges, any judge shall be entitled to deliver a separate opinion.

Article 46 – Binding force and execution of judgments

The High Contracting Parties undertake to abide by the final judgment of the Court in any case to which they are parties.

The final judgment of the Court shall be transmitted to the Committee of Ministers, which shall supervise its execution.

Article 47 – Advisory opinions

The Court may, at the request of the Committee of Ministers, give advisory opinions on legal questions concerning the interpretation of the Convention and the protocols thereto.

Such opinions shall not deal with any question relating to the content or scope of the rights or freedoms defined in Section I of the Convention and the protocols thereto, or with any other question which the Court or the Committee of Ministers might have to consider in consequence of any such proceedings as could be instituted in accordance with the Convention.

Decisions of the Committee of Ministers to request an advisory opinion of the Court shall require a majority vote of the representatives entitled to sit on the Committee.

Article 48 – Advisory jurisdiction of the Court

The Court shall decide whether a request for an advisory opinion submitted by the Committee of Ministers is within its competence as defined in Article 47.

Article 49 – Reasons for advisory opinions

Reasons shall be given for advisory opinions of the Court.

If the advisory opinion does not represent, in whole or in part, the unanimous opinion of the judges, any judge shall be entitled to deliver a separate opinion.

Advisory opinions of the Court shall be communicated to the Committee of Ministers.

Article 50 – Expenditure on the Court
The expenditure on the Court shall be borne by the Council of Europe.
Article 51 – Privileges and immunities of judges
The judges shall be entitled, during the exercise of their functions, to the privileges and immunities provided for in Article 40 of the Statute of the Council of Europe and in the agreements made thereunder.
Section III – Miscellaneous provisions[1, 3]
Article 52 – Inquiries by the Secretary General[1]
On receipt of a request from the Secretary General of the Council of Europe any High Contracting Party shall furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention.
Article 53 – Safeguard for existing human rights[1]
Nothing in this Convention shall be construed as limiting or derogating from any of the human rights and fundamental freedoms which may be ensured under the laws of any High Contracting Party or under any other agreement to which it is a Party.
Article 54 – Powers of the Committee of Ministers[1]
Nothing in this Convention shall prejudice the powers conferred on the Committee of Ministers by the Statute of the Council of Europe.
Article 55 – Exclusion of other means of dispute settlement[1]
The High Contracting Parties agree that, except by special agreement, they will not avail themselves of treaties, conventions or declarations in force between them for the purpose of submitting, by way of petition, a dispute arising out of the interpretation or application of this Convention to a means of settlement other than those provided for in this Convention.
Article 56 – Territorial application [1]

[4]Any State may at the time of its ratification or at any time thereafter declare by notification addressed to the Secretary General of the Council of Europe that the present Convention shall, subject to paragraph 4 of this Article, extend to all or any of the territories for whose international relations it is responsible.

The Convention shall extend to the territory or territories named in the notification as from the thirtieth day after the receipt of this notification by the Secretary General of the Council of Europe.

The provisions of this Convention shall be applied in such territories with due regard, however, to local requirements.

[4]Any State which has made a declaration in accordance with paragraph 1 of this article may at any time thereafter declare on behalf of one or more of the territories to which the declaration relates that it accepts the competence of the Court to receive applications from individuals, non-governmental organisations or groups of individuals as provided by Article 34 of the Convention.

Article 57 – Reservations[1]

Any State may, when signing this Convention or when depositing its instrument of ratification, make a reservation in respect of any particular provision of the Convention to the extent that any law then in force in its territory is not in conformity with the provision. Reservations of a general character shall not be permitted under this article.

Any reservation made under this article shall contain a brief statement of the law concerned.

Article 58 – Denunciation [1]

A High Contracting Party may denounce the present Convention only after the expiry of five years from the date on which it became a party to it and after six months' notice contained in a notification addressed to the Secretary General of the Council of Europe, who shall inform the other High Contracting Parties.

Such a denunciation shall not have the effect of releasing the High Contracting Party concerned from its obligations under this Convention in respect of any act which, being

capable of constituting a violation of such obligations, may have been performed by it before the date at which the denunciation became effective.

Any High Contracting Party which shall cease to be a member of the Council of Europe shall cease to be a Party to this Convention under the same conditions.

4 The Convention may be denounced in accordance with the provisions of the preceding paragraphs in respect of any territory to which it has been declared to extend under the terms of Article 56.

Article 59 – Signature and ratification[1]

This Convention shall be open to the signature of the members of the Council of Europe. It shall be ratified. Ratifications shall be deposited with the Secretary General of the Council of Europe.

The present Convention shall come into force after the deposit of ten instruments of ratification.

As regards any signatory ratifying subsequently, the Convention shall come into force at the date of the deposit of its instrument of ratification.

The Secretary General of the Council of Europe shall notify all the members of the Council of Europe of the entry into force of the Convention, the names of the High Contracting Parties who have ratified it, and the deposit of all instruments of ratification which may be effected subsequently.

Done at Rome this 4th day of November 1950, in English and French, both texts being equally authentic, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General shall transmit certified copies to each of the signatories.

Heading added according to the provisions of Protocol No. 11 (ETS No. 155).

New Section II according to the provisions of Protocol No. 11 (ETS No. 155).

The articles of this Section are renumbered according to the provisions of Protocol No. 11 (ETS No. 155).

Text amended according to the provisions of Protocol No. 11 (ETS No. 155).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Strasbourg, 28.I.1981

Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

Chapter I – General provisions

Article 1 – Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2 – Definitions

For the purposes of this convention:

a. "personal data" means any information relating to an identified or identifiable individual ("data subject");
b. "automated data file" means any set of data undergoing automatic processing;
c. "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;
d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3 – Scope

The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;
b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;
c. that it will also apply this convention to personal data files which are not processed automatically.

Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

Chapter II – Basic principles for data protection

Article 4 – Duties of the Parties

Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

These measures shall be taken at the latest at the time of entry into force of this

convention in respect of that Party.

Article 5 – Quality of data
Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 – Special categories of data
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 – Data security
Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 – Additional safeguards for the data subject
Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 – Exceptions and restrictions

No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
b. protecting the data subject or the rights and freedoms of others.

Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 – Sanctions and remedies
Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11 – Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

Chapter III – Transborder data flows

Article 12 – Transborder flows of personal data and domestic law

The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
b. when the transfer is made from its territory to the territory of a non-ing State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties

The Parties agree to render each other mutual assistance in order to implement this convention.

For that purpose:

a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;
b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

An authority designated by a Party shall at the request of an authority designated by another Party:

a. furnish information on its law and administrative practice in the field of data protection;
b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 – Assistance to data subjects resident abroad

Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

The request for assistance shall contain all the necessary particulars, relating *inter alia* to:

a. the name, address and any other relevant particulars identifying the person making the request;
b. the automated personal data file to which the request pertains, or its controller;
c. the purpose of the request.

Article 15 – Safeguards concerning assistance rendered by designated authorities

An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16 – Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;
b. the request does not comply with the provisions of this convention;
c. compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17 – Costs and procedures of assistance

Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

Chapter V – Consultative Committee

Article 18 – Composition of the committee

A Consultative Committee shall be set up after the entry into force of this convention.

Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19 – Functions of the committee

The Consultative Committee:

a. may make proposals with a view to facilitating or improving the application of the convention;
b. may make proposals for amendment of this convention in accordance with Article 21;
c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;
d. may, at the request of a Party, express an opinion on any question

concerning the application of this convention.

Article 20 – Procedure

The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

Chapter VI – Amendments

Article 21 – Amendments

Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Chapter VII – Final clauses

Article 22 – Entry into force

This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 23 – Accession by non-member States

After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States

entitled to sit on the committee.

In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24 – Territorial clause

Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25 – Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26 – Denunciation

Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27 – Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:

a. any signature;
b. the deposit of any instrument of ratification, acceptance, approval or accession;
c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24;
d. any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the Economic and Social Committee (2),
Acting in accordance with the procedure laid down in Article 189b of the Treaty (3), in the light of the joint text approved by the Conciliation Committee on 6 November 1997,

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community;

(2) Whereas confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights (in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms) and the constitutions of the Member States;

(3) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterised by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(4) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(5) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (5), called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasised the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (6);

(6) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(7) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users;

(8) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the telecommunications sector, must be harmonised in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 7a of the Treaty; whereas the harmonisation is limited to requirements that are necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

(9) Whereas the Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by the provisions of this Directive.

(10) Whereas these new services include interactive television and video on demand;

(11) Whereas, in the telecommunications sector, in particular for all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunications services;

(12) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;

(13) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons; whereas this protection is ensured within the framework of the applicable Community and national legislation;

(14) Whereas the application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges must not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort; whereas it is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission;

(15) Whereas service providers must take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network; whereas security is appraised in the light of the provision of Article 17 of Directive 95/46/EC;

(16) Whereas measures must be taken to prevent the unauthorised access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicly available telecommunications services; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications;

(17) Whereas the data relating to subscribers processed to establish calls contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons; whereas such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time; whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications services may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available telecommunications services about the types of further processing he intends to perform;

(18) Whereas the introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; whereas, at the same time, it may jeopardise the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills;

(19) Whereas it is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines; whereas it is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular helplines and similar organizations, have an interest in guaranteeing the anonymity of their callers; whereas it is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls; whereas the providers of publicly available telecommunications services must inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas the privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available telecommunications service;

(20) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available telecommunications service;

(21) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(22) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(23) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market;

(24) Whereas in particular, similarly to what is provided for by Article 13 of Directive 95/46/EC, Member States can restrict the scope of subscribers' obligations and rights in certain circumstances, for example by ensuring that the provider of a publicly available telecommunications service may override the elimination of the presentation of calling line identification in conformity with national legislation for the purpose of prevention or detection of criminal offences or State security;

(25) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(26) Whereas it is useful in the field of application of this Directive to draw on the experience of the Working Party on the protection of individuals with regard to the processing of personal data composed of representatives of the supervisory authorities of the Member States, set up

by Article 29 of Directive 95/46/EC;

(27) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology; whereas this procedure applies solely to specifications necessary to adapt the Annex to new technological developments, taking into consideration changes in market and consumer demand; whereas the Commission must duly inform the European Parliament of its intention to apply this procedure and whereas, otherwise, the procedure laid down in Article 100a of the Treaty shall apply;

(28) Whereas, to facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1 Object and scope

1. This Directive provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.
2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons.
3. This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2 Definitions
In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:
(a) 'subscriber` shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;
(b) 'user` shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;
(c) 'public telecommunications network` shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in whole or in part, for the provision of publicly available telecommunications services;
(d) 'telecommunications service` shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.

Article 3 Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.
2. Articles 8, 9 and 10 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to

subscriber lines connected to analogue exchanges.
3. Cases where it would be technically impossible or require a disproportionate investment to fulfil the requirements of Articles 8, 9 and 10 shall be notified to the Commission by the Member States.

Article 4 Security

1. The provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5 Confidentiality of the communications

1. Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14 (1).
2. Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evi dence of a commercial transaction or of any other business communication.

Article 6 Traffic and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.
2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.
3. For the purpose of marketing its own telecommunications services, the provi der of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.
4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.
5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

Article 7 Itemized billing

1. Subscribers shall have the right to receive non-itemized bills.
2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative modalities for communications or payments are available to such users and subscribers.

Article 8 Presentation and restriction of calling and connected line identification

1. Where presentation of calling-line identification is offered, the calling user must have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line

identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.
2. Where presentation of calling-line identification is offered, the called subscriber must have the possibility via a simple means, free of charge for reasonable use of this function, to prevent the presentation of the calling line identification of incoming calls.
3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the called subscriber must have the possibility via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.
4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.
5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.
6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9 Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available telecommunications service may override the elimination of the presentation of calling line identification:
(a) on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls; in this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public telecommunications network and/or publicly available telecommunications service;
(b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10 Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

Article 11 Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.
2. Notwithstanding paragraph 1, Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved does not act as a disincentive to the exercise of this right, and that, taking account of the quality requirements of the public directory in the light of the universal service, it is limited to the actual costs incurred by the operator for the adaptation and updating of the list of subscribers not to be included in the public directory.
3. The rights conferred by paragraph 1 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 12 Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.
2. Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing, by means other than those referred to in paragraph 1, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation.
3. The rights conferred by paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.

Article 13 Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.
2. Where provisions of this Directive can be implemented only by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Directive 83/189/EEC (7) which lays down a procedure for the provision of information in the field of technical standards and regulations.
3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and telecommunications (8).

Article 14 Extension of the scope of application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8(1), (2), (3) and (4), when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system, as referred to in Article 13(1) of Directive 95/46/EC.
2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.
3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.
4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.

Article 15 Implementation of the Directive

1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than 24 October 1998.
By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with Article 5 of

this Directive not later than 24 October 2000.
When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.
2. By way of derogation from Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.
3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.
4. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive.

Article 16 Addressees

This Directive is addressed to the Member States.

Done at Brussels, 15 December 1997.
For the European Parliament
The President
J. M. GIL-ROBLES
For the Council
The President
J.-C. JUNCKER

(1) OJ C 200, 22.7.1994, p. 4.
(2) OJ C 159, 17.6.1991, p. 38.
(3) Opinion of the European Parliament of 11 March 1992 (OJ C 94, 13.4.1992, p. 198). Council Common Position of 12 September 1996 (OJ C 315, 24.10.1996, p. 30) and Decision of the European Parliament of 16 January 1997 (OJ C 33, 3.2.1997, p. 78). Decision of the European Parliament of 20 November 1997 (OJ C 371, 8.12.1997). Council Decision of 1 December 1997.
(4) OJ L 281, 23.11.1995, p. 31.
(5) OJ C 257, 4.10.1988, p. 1.
(6) OJ C 196, 1.8.1989, p. 4.
(7) OJ L 109, 26.4.1983, p. 8. Directive as last amended by Directive 94/10/EC (OJ L 100, 19.4.1994, p. 30).
(8) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

ANNEX

List of data
For the purpose referred to in Article 6(2) the following data may be processed:
Data containing the:
- number or identification of the subscriber station,
- address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,
- type, starting time and duration of the calls made and/or the data volume transmitted,
- date of the call/service,
- other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the Economic and Social Committee (2),
Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;
(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection

of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the

purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful

instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such

third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1
Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2
Definitions

For the purposes of this Directive:
(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3
Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:
- in the course of an activity which falls outside the scope of Community law, such as those

provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

Article 4
National law applicable
1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5
Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I
PRINCIPLES RELATING TO DATA QUALITY

Article 6
1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II
CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7
Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is

party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III
SPECIAL CATEGORIES OF PROCESSING

Article 8
The processing of special categories of data
1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
2. Paragraph 1 shall not apply where:
(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.
7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression
Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV
INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10
Information in cases of collection of data from the data subject
Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11
Information where the data have not been obtained from the data subject
1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as
- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him
in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.
2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V
THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12
Right of access
Member States shall guarantee every data subject the right to obtain from the controller:
(a) without constraint at reasonable intervals and without excessive delay or expense:
- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or

inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI
EXEMPTIONS AND RESTRICTIONS

Article 13
Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.
2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII
THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14
The data subject's right to object
Member States shall grant the data subject the right:
(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.
Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15
Automated individual decisions
1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII
CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16
Confidentiality of processing
Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17
Security of processing
1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX
NOTIFICATION

Article 18
Obligation to notify the supervisory authority
1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.
2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),
thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.
3. Member States may provide that paragraph 1 does not apply to processing whose sole

purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.
4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).
5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19
Contents of notification
1. Member States shall specify the information to be given in the notification. It shall include at least:
(a) the name and address of the controller and of his representative, if any;
(b) the purpose or purposes of the processing;
(c) a description of the category or categories of data subject and of the data or categories of data relating to them;
(d) the recipients or categories of recipient to whom the data might be disclosed;
(e) proposed transfers of data to third countries;
(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.
2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20
Prior checking
1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21
Publicizing of processing operations
1. Member States shall take measures to ensure that processing operations are publicized.
2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.
The register shall contain at least the information listed in Article 19 (1) (a) to (e).
The register may be inspected by any person.
3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.
Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22
Remedies
Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for

any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23
Liability
1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24
Sanctions
The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25
Principles
1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
Member States shall take the measures necessary to comply with the Commission's decision.

Article 26
Derogations
1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).
Member States shall take the necessary measures to comply with the Commission's decision.
4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27
1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.
Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28
Supervisory authority
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.
These authorities shall act with complete independence in exercising the functions entrusted to them.
2. Each Member State shall provide that the supervisory authorities are consulted when

drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.
3. Each authority shall in particular be endowed with:
- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.
4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.
Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.
5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.
6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.
7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29
Working Party on the Protection of Individuals with regard to the Processing of Personal Data
1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.
It shall have advisory status and act independently.
2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.
Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.
3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.
4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.
5. The Working Party's secretariat shall be provided by the Commission.
6. The Working Party shall adopt its own rules of procedure.
7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31
The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the

processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.
3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.
4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33
The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.
The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34
This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.
For the European Parliament
The President
K. HAENSCH
For the Council
The President
L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.
(2) OJ No C 159, 17. 6. 1991, p 38.
(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).
(1) OJ No L 197, 18. 7. 1987, p. 33.

Annex B:

Computer Crime Legislation in Europe

Council of Europe *Convention on Cybercrime*
Budapest, 23.XI.2001

PREAMBLE

The member States of the Council of Europe and the other States signatory hereto, Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cybercrime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10 - 11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be

used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of

supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

a. the criminal offences established in accordance with articles 2-11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3. a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system

i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental

Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 - Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control;

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, "subscriber information" means any information, contained in

the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:

a. the type of the communication service used, the technical provisions taken thereto and the period of service;

b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and

b. computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to :

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data; and

d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other

measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data of specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed :

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a

view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1. a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7. a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 - 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in Articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. a. Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other.

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to grounds for refusal available under Article 25, paragraph (4), refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or

reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation, is available unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the furnishing of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that furnishes information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a. the authority that is seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceeding and a brief summary of related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information to identify the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data may, in respect of offences other than those established in accordance with Articles 2 – 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this Chapter.

3. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without obtaining the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time

collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted by their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

a. provision of technical advice;

b. preservation of data pursuant to Articles 29 and 30; and

c. collection of evidence, giving of legal information, and locating of suspects.

2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of

Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20 (d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition opened for signature in Paris on 13 December 1957 (ETS No. 24);

- the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 20 April 1959 (ETS No. 30);

- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Article 2, Article 3, Article 6, paragraph 1 (b), Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

Article 41 – Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this

Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and, following consultation with the non-member State Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The European Committee on Crime Problems (CDPC) shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article 40 or reservation made in accordance with Article 42;

e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Council of the European Union – *Framework decision on attacks against information systems*

Brussels, 12 May 2003

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 29, 30(1)(a), 31(1)(e) and 34(2)(b) thereof,

Having regard to the proposal of the Commission[69]

Having regard to the Opinion of the European Parliament[70],

Whereas:

(1) The objective of this Framework Decision is to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.

(2) There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, and therefore requires a response at the level of the European Union.

(3) An effective response to those threats requires a comprehensive approach to network and information security, as underlined in the *e*Europe Action Plan, in the Communication by the Commission "Network and Information Security: Proposal for a European Policy Approach" and in the Council Resolution of 6 December 2001 on a common approach and specific actions in the area of network and information security.

(4) The need to further increase awareness of the problems related to information security and provide practical assistance has also been stressed in the European Parliament Resolution of 5 September 2001.

(5) Significant gaps and differences in Member States' laws in this area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in the area of attacks against information systems. The trans-national and borderless character of modern information systems means that attacks against such systems are often trans-border in nature, thus underlining the urgent need for further action to approximate criminal laws in this area.

(6) The Action Plan of the Council and the Commission on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice[71], the Tampere European Council on 15-16 October 1999, the Santa Maria da Feira European

[69] OJ C 203 E, 27.8.2002, p. 109.

[70] Opinion delivered on 22 October 2002.

[71] OJ C 19, 23.1.1999, p.1.

Council on 19-20 June 2000, the Commission in the "Scoreboard" and the European Parliament in its Resolution of 19 May 2000 indicate or call for legislative action against high technology crime, including common definitions, incriminations and sanctions.

(7) It is necessary to complement the work performed by international organisations, in particular the Council of Europe's work on approximating criminal law and the G8's work on transnational cooperation in the area of high tech crime, by providing a common approach in the European Union in this area. This call was further elaborated by the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

(8) Criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism.

(9) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The personal data processed in the context of the implementation of this Framework Decision should be protected in accordance with the principles of the said Convention.

(10) Common definitions in this area, particularly of information systems and computer data, are important to ensure a consistent approach in Member States in the application of this Framework Decision.

(11) There is a need to achieve a common approach to the constituent elements of criminal offences by providing for common offences of illegal access to an information system, illegal system interference and illegal data interference.

(12) In the interest of combating computer-related crime, each Member State should ensure effective judicial cooperation in respect of offences based on the types of conduct referred to in Articles 2, 3, 4 and 5.

(13) There is a need to avoid over-criminalisation, particularly of minor cases, as well as a need to avoid criminalising right-holders and authorised persons.

(14) There is a need for Member States to provide sanctions for attacks against information systems. The sanctions thus provided for shall be effective, proportional and dissuasive.

(15) It is appropriate to provide for more severe penalties when an attack against an information system is committed within the framework of a criminal organisation, as defined in the Joint Action 98/733 JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member State of the European Union[72], or where it has caused serious damages, or has affected essential interests.

(16) Measures should also be foreseen for the purposes of cooperation between Member States with a view to ensuring effective action against attacks against information systems. Member States should therefore make use of the existing network of operational contact points referred to in the Council Recommendation of 25 June 2001 on contact points remaining a 24-hour service for combating high-tech crime, for the exchange of information.

(17) Since the objectives of this Framework Decision, ensuring that attacks against information systems be sanctioned in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial cooperation by removing potential complications, cannot be sufficiently achieved by the Member States, as rules have

[72] OJ L 351, 29.12.1998, p.1.
[73] Date to be inserted

to be common and compatible, and can therefore be better achieved at the level of the Union, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in that Article, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.

(18) This Framework Decision respects the fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union, and notably Chapters II and VI thereof,

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1
Definitions

For the purposes of this Framework Decision, the following definitions shall apply:

(a) "Information System" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.

(b) "Computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.

(c) "Legal person" means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations.

(d) "Without right" means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the domestic legislation.

Article 2
Illegal access to Information Systems

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

Article 3
Illegal system interference

Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 4
Illegal data interference

Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at

least for cases which are not minor.

Article 5
Instigation, aiding and abetting and attempt

1. Each Member State shall ensure that the instigation of, aiding and abetting an offence referred to in Articles 2, 3 and 4 is punishable as a criminal offence.

2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence.

3. Each Member State may decide not to enforce paragraph 2 for the offences referred to in Article 2.

Article 6
Penalties

1. Each Member State shall take the necessary measures to ensure that the conduct referred to in Articles 2, 3, 4 and 5 is punishable by effective, proportional and dissuasive criminal sanctions.

2. Each Member State shall take the necessary measures to ensure that the conduct referred to in Articles 3 and 4 is punishable by criminal sanctions of a maximum of at least between 1 and 3 years of imprisonment.

Article 7
Aggravating circumstances

1. Each Member State shall take the necessary measures to ensure that the conduct referred to in Article 2(2) and the conduct referred to in Articles 3 and 4 is punishable by criminal sanctions of a maximum of at least between 2 and 5 years of imprisonment when committed within the framework of a criminal organisation as defined in Joint Action 98/733/JHA apart from the sanction level referred to therein.

2. A Member State may also take the measures referred to in paragraph 1 when the conduct has caused serious damages or has affected essential interests.

Article 8
Liability of legal persons

1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for conducts referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

(a) a power of representation of the legal person, or

(b) an authority to take decisions on behalf of the legal person, or

(c) an authority to exercise control within the legal person.

2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority.

3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the conduct referred to in Articles 2, 3, 4 and 5.

Article 9
Sanctions for legal persons

1. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(1) is punishable by effective, proportional and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions, such as:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice of commercial activities;

(c) placing under judicial supervision; or

(d) a judicial winding-up order.

2. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(2) is punishable by effective, proportional and dissuasive sanctions or measures.

Article 10
Jurisdiction

1. Each Member State shall establish its jurisdiction with regard to the conduct referred to in Articles 2, 3, 4 and 5 where the conduct has been committed:

(a) in whole or in part within its territory; or

(b) by one of its nationals; or

(c) for the benefit of a legal person that has its head office in the territory of that Member State.

2. When establishing its jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that it includes cases where:

(a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State which under its laws, does not as yet extradite or surrender its own nationals shall take the necessary measures to establish its jurisdiction over and to prosecute, where appropriate, the conduct referred to in Articles 2 to 5 in cases when it is committed by one of its nationals outside its territory.

4. Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the co-ordination of their action. Sequential account may be taken of the following factors:

. the Member State shall be that in the territory of which the acts have been committed according to paragraph 1(a) and paragraph 2;

. the Member State shall be that of which the perpetrator is a national;

. the Member State shall be that in which the perpetrator has been found.

5. A Member State may decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rules set out in paragraphs 1(b) and 1(c).

6. Member States shall inform the General Secretariat of the Council and the Commission accordingly where they decide to apply paragraph 5, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

Article 11
Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 2, 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they make use of the existing network of operational points of contact available twenty four hours a day and seven days a week.

2. Each Member State shall inform the General Secretariat of the Council and the Commission of its appointed point of contact for the purpose of exchanging information on offences relating to attacks against information systems. The General Secretariat shall notify that information to the other Member States.

Article 12
Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision by […][73].

2. By the same date Member States shall transmit to the General Secretariat of the Council and to the Commission the text of any provisions transposing into their national law the obligations imposed on them under this Framework Decision. By 31 December 2004 at the latest, on the basis of a report established on the basis of information and a written report by the Commission, the Council shall assess the extent to which Member States have complied with the provisions of this Framework Decision.

Article 13
Entry into force

This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.

Done at Brussels,

For the Council

The President

Annex 3

National Data Protection Legislation

DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
AUSTRIA	Data Protection Act of 2000	*Data may only be collected for a specific, explicit & legitimate purpose. * Data must be adequate, relevant not excessive, kept up – to – date and no longer the necessary. *Inaccurate or misleading data may not be processed. *Use of the data must be within the data controller authority. *Data must be processed fairly and lawfully.	Data may not be processed unless: *The data subject has given his explicit consent. *Processing necessary to protect the vital interests of the data subject is party. *Processing is necessary to comply with a legal obligation. *Processing is necessary to protect the vital interests of the data subject. *Processing relates for the performance of a task carried out in the public interest. *Processing is necessary to carry out the controller or a third party. *Data has previously been published.	Only permitted if: *Data subject provides explicit consent. * Processing necessary to protect the vital interests of the data subject (and consent cannot be obtained in due time) or another person. *Processing necessary to comply with employment law commitments. *Processing relates to data made public by the data subject or exercise or defense of legal claims. *Processing will serve the public interest. *Data required for medical services and used by relevant staff. *Processing relates to certain non-profit	*Data controllers must notify the data protection agency before initiating the data processing. *Non-sensitive data processing may be initiated after notification. Prior authorisation from the Data Protection Agency is required for processing. * Sensitive data. * Data related to creditworthiness.. *Data involving networks run by several data controllers where data access can be obtained by each of the controllers.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

				organisational data.				
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
AUSTRIA	Telecommunications Act of 1997	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications.	If the telecommunication operator offers this service, it must provide for the following purposes: * Conclusions, performance, modification or termination of the contract with subscribers. * Billing purposes. * Creation of directories. Content data must not be stored unless it is an essential part of the service. Telecommunications operators must ensure that data related to end-users is deleted upon termination of the call.	* Telecommunications operators must provide itemised bills only if requested by the end-user. * New Telecommunications Law Draft establishes that telecommunications operators must provide itemised bill unless the consumer does not request it.	* Subscribers have the right to be excluded, free-of-charge, from a directory. * Directories must not include more data than that specified in the law, unless the consumer consents.	Marketing activities using telecommunications means are not permitted unless the consumer has previously consented.		

DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
BELGIUM	.Law of 11 December 1998	* Data may only be collected for a specific, explicit and legitimate purpose. * Data must be adequate, relevant, not excessive, kept up-to-date and no longer than necessary. * Inaccurate or misleading data may not be processed. * Data must be processed fairly and lawfully.	Data may not be processed unless: * Processing is necessary for the performance of a contract to which the data subject is party. * Processing is necessary to comply with a legal obligation. * Processing is necessary to protect the vital interests of the data subject. * Processing is necessary for the performance of a task carried out in the public interest. * Processing is necessary to carry out the data controller or a third party legitimate interest.	Only permitted if.2 *The data subject provides its explicit written consent. * Processing is necessary to protect the vital interests of the data subject or another person. * Processing is necessary to comply with employment law commitments. * Processing relates to data made public by the data subject. *Processing relates to exercise or defense of legal claims. * Processing will serve the public interest.	Data controller must notify the Data Protection Agency before initiating the data processing unless: * Processing of data is necessary for the management of the wages or of the personnel of the operator. * Processing necessary for the accounting of the operator; * Processing necessary for the shareholders or partners of the operator. * Processing necessary for the client management. *Identification data necessary for	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

					contact.			
Telecommunications Requirements/Obligations								
Country	***Regulation***	***Confidentiality in Communications***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemised Billing***	***Use of Directions***	***Direct Maketing***	
BELGIUM	Royal Decree of 5 September 2001	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications. Operator must inform the users of the possibility of a breach in this confidentiality.	Telecommunications operators must provide subscribers with the possibility of deleting, on a all call per call basis, call identification.	Telecommunications operators must delete, after the completion of the call, any traffic data regarding users or subscribers that was used to connect the call. However, telecommunications operators may hold the following data for billing and interconnection payments and fraud detection purposes: number identification of the end user; address of the end user; the total of units to invoice in the accounting period; called number identification; type of call, starting time and duration of the	Telecommunications operators must provide itemised bills to the subscribers unless the subscribers request not to receive it. Subscribers also have the right to request a more detailed itemised bill.	Telecommunications operators must guarantee subscribers right of being excluded freed-of-charge from a directory.	Not specified.	

				calls and/or volume of data transmitted; date of the call or service; and other information regarding payments, such as advanced payments, payments by instalments and disconnection. The telecommunications operators may process billing data for purposes of marketing their own telecommunications services, provided the subscriber				
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
DENMARK	Act No. 429 of May 31, 2002	Data may only be collected for a specific explicit and legitimate purpose. Data must be adequate, relevant not excessive, kept up-to-date and no longer than	Data may not be processed unless: * The data subject provides its explicit consent. * Processing is necessary to protect the vital interests of	Only permitted if: * The data subject provides its explicit consent. * Processing in necessary to protect the vital interests of the data subject or	Only required fore processing of sensitive data.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

		necessary. Inaccurate or misleading data may not be processed.	the data subject or another person. * Processing is necessary to comply with employment law commitments. * Processing relates to data made public by the data subject. *Processing is necessary to the performance of a task carried out in the public interest. * Processing is necessary to carry out the data controller or a third party legitimate interest.	another person. * Processing is necessary to comply with employment law commitments. * Processing relates to data made public by the data subject. * Processing relates to exercise or defense of legal claims. * Processing serves the public interest.				
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
DENMARK	Telecommunications executive Order	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications.	If the telecommunication operator offers this service, it must provide for the following purposes: * Suppression if the	* Telecommunications operators must ensure that data related to end-user is deleted upon termination of the call.	* Itemised bills and fully itemised bills must be offered by the telecommunication operator no later than six (6) months after it initiates the	* Telecommunications operators must deliver number information data to other operators or companies that are entitles to request it.	Marketing activities using telecommunications means are not permitted, unless the consumer has previously consented.	

			identification of the calling line for outgoing calls. * Rejection of incoming calls where the calling number is not identified.	* Data may be processed and stored for purposes of billing, but only until the time period terminates for challenging the bill. * Billing data may be used by the operator for marketing its own services with prior consent of the end-user.	service.	* The end user has the right to be excluded from any directory.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
FINLAND	Personal Data Act	Data may only be collected for a specific explicit and legitimate purpose. Data must be adequate, relevant not excessive, kept up-to-date and no longer than necessary. Inaccurate or misleading data may not be processed.	Data may not be processed unless: * The data subject provides its explicit consent. * Processing is necessary to protect the vital interests of the data subject or another person. * Processing is necessary to comply	Only permitted if: * The data subject provides its explicit consent. * Processing in necessary to protect the vital interests of the data subject or another person. * Processing is necessary to comply with employment	Obligation to notify the Data protection Agency 30 days before initiating the processing is required if: * It involves sensitive data. * The data is processed for direct marketing or distant selling, or other direct advertising.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

			with employment law commitments. * Processing relates to data made public by the data subject. *Processing is necessary to the performance of a task carried out in the public interest. * Processing is necessary to carry out the data controller or a third party legitimate interest.	law commitments. * Processing relates to data made public by the data subject. * Processing relates to exercise or defense of legal claims. * Processing serves the public interest.	* The data is processed for the purpose of payment traffic or other comparable task undertaken by a third party on behalf of the data conmtroller.			
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
FINLAND	Telecommunications Act	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications. Operator must inform the users of the possibility of a breach in this confidentiality.	If the telecommunication operator offers this service, it must provide for the following purposes: * Suppression if the identification of the calling line for outgoing calls. * Suppression of the	* Telecommunications operators must ensure that data related to end-user is deleted upon termination of the call. * Billing data may be used by the operator for marketing its own services with prior	* Telecommunications operators must provide itemised bills only if requested by the end-user. * The telecommunications operator may not disclose the last three (3) numbers of	* Telecommunications operators must limit the data contained in directories to that which is necessary to identify the data subject, unless the data subject consents. * The subscriber has the right to object to	Marketing activities using telecommunications means are not permitted, unless the consumer has previously consented.	

			identification of the calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified. * Prevention of automatic call forwarding.	consent of the consumer. * Data may be processed and stored for purposes of billing, but only until the time period terminates for challenging the bill. .	the calls unless : (1) the calls are made to commercial numbers, or (2) the total amount of the bill is at least double the amount of the previous period's bill.	inclusion of his data in the directory , to rectify erroneous data and to prohibit the use of his data for marketing purposes.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
FRANCE	Law No. 78-17	Data must not be used for a purpose other than for which it was collected. Data processing must be made by human (not automatic) means and must not be collected in a fraudulent, unlawful or unfair manner. The purpose for using the data has to be conveyed to the user and the data	No consent is required.	May be collected or processed only with the data subject's consent.	Data controllers must notify the Data Protection Agency before collecting the data.	Data Subjects have the following rights related to the processing of their data: * Right to Information. * Right to access, modify or delete information. * Right to have their information safe and free from distortion, damage, or communication to unauthorised third parties.	Data controllers have a duty to maintain the data safe and free from distortion.	Follows guidelir

		may not be kept longer than necessary.						
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
FRANCE	Telecommunications Ordinance of 2001	Not specified.	Telecommunications operator must provide the end user, free-of-charge, to prevent call forwarding.	Billing data may be used by the operator for marketing its own services with prior consumer consent.	Not specified.	* Unrestricted data use. * The subscriber has the right to object to the inclusion of his information in the directory, to rectify erroneous data and to prohibit the use of his data for marketing purposes.	* Direct marketing by telephone or fax is not permitted unless the consumer has previously consented. * Telecommunications operators must provide users with the means to express their consent to receive marketing calls.	
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
GERMANY	Federal Data Protection Act	* Processing must have a legitimate business purposes and can only be	Data may not be processed unless: *The data subject	Only permitted if: *Data subject provides explicit	*Data controllers must notify the Data Protection Agency before initiating the	Data Subjects have the following rights related to the processing of their	Data controllers must take the technical and organisational	Follows guidelir

		used consistent with such purpose. * Processing must be permitted under the Act or other legal provision. * Processing is necessary for the performance of a contract to which the data subject is party.	has given his explicit consent. * Data has a legitimate business purpose. *Processing is necessary to comply with a legal obligation. Data maybe collected without data subject's consent if: * Collection is done pursuant to a legal obligation; an administrative requirement or the intended business purpose requires collection from third parties.	consent. * Processing necessary to protect the vital interests of the data subject (and consent cannot be obtained in due time) or another person. * Processing relates to data made public by the data subject. * Processing relates to exercise or defense of legal claims. *Processing relates to scientific research.	data processing.	data: * Right of Information. * Right of Access. * Right of ratification. * Right of Objection.	measures necessary to ensure the protection of data pursuant to the provisions of the Act and are expected to self-monitor.	
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
GERMANY	Various Telecommunications Regulations	Telecommunications operators must adopt the necessary measures to preserve the	Not specified.	The telecommunication operator may process traffic data for the following	* Telecommunications operators must provide itemised bills only if	Not specified.	* Limited exploitation of data for marketing purposes.	

		confidentiality of the communications, must only collect services and must notify customers and obtain their express consent.		purposes. * Conclusion, performance, modification or termination of the contract with subscribers. * Billing. * Creation of subscribers directories. Billing data may be used by the operator for marketing of its own services with prior consumer consent.	requested by the end-user.		* Provider may compile pseudonym-based user profiles provided user does not object. * Provider must inform users about their right to object. * Actual user profiles may not be combined with pseudonym profiles.	
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
GREECE	Law 2472/1997	* May only be collected for a specific explicit and legitimate purpose. * Must be adequate, relevant not excessive and must be kept up-to-date	Data may not be processed unless: * The data subject provides its explicit consent. * Processing is necessary for the	Prohibited unless an authorisation is obtained from the Data Protection Agency and if: * The data subject gives his explicit consent.	Data controllers must notify the Data Protection Agency before processing any data. A notification is required when:	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

		and no longer than necessary. * Inaccurate or misleading data may not be processed.	performance of a contract to which the data subject is party. * Processing is necessary to comply with a legal obligation. * Processing is necessary to protect the vital interests. *Processing is necessary to the performance of a task carried out in the public interest. * Processing is necessary to carry out the data controller or a third party legitimate interest.	* It is necessary to protect the vital interests of the data subject. * It relates to data made public by the data subject. * It relates to health matters. * It is necessary for national security, criminal matters or public health. * It relates to data used exclusively for research and scientific matters. * It relates to public figures.	* Processing relates to employment or project relationship. * Processing relates to client or suppliers data, provided that such data is not transferred or disclosed to third parties. *Processing is performed by associations, institutions and political parties involving data of their members. * Processing is by doctors bound by confidentiality. * Processing is performed by lawyers, notary public related to client services.	* Right of Objection. * Right of Judicial Protection		
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
GREECE	Law 2774/1999	Telecommunications operators will adopt the necessary measures to	If the telecommunication operator offers this service, it must	* Telecommunications operators must ensure that data	* Telecommunications operators must provide itemised	* Telecommunications operators must deliver number	Not specified.	

		preserve the confidentiality of the communications. Operator must inform users of the possibility of a breach in this confidentiality.	provide free-of-charge, the following: * Suppression if the identification of the calling line for outgoing calls. * Suppression of the identification of the calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified. *Override of incoming call identification to prevent malicious calls (not free-of-charge).	related to end-user is deleted upon termination of the call. * Traffic data maybe used by telecommunications operators for (1) the conclusion of the contract with the end-user, and (2) for billing purposes. * Billing data may be used by the operator for marketing its own services with prior consent. * Operators must provide opportunity for consumers to make anonymous payments.	bills unless requested by the end-user. * The telecommunications operator may not disclose the last three (3) numbers of the call.	information data to other operators or companies that are entitles to request it. * The end user has the right to be excluded from any directory.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
IRELAND	1998 Law & 2001 Regulation	* May only be collected for a specific, explicit and legitimate purpose.			*Data controllers must register with the Data Protection Commission if it	Data Subjects have the following rights related to the processing of their	The data controller must implement appropriate technical and	Follows guidelir

		* Must be adequate, relevant, not excessive, kept up-to-date and no longer than necessary. * Inaccurate or misleading data may not be processed.			involves: * Public sector body, financial institution, or an insurance company. * Sensitive data. * Direct marketing.	data: * Right of Information. * Right of Access. * Right of Ratification. * Right of Objection.	organisational measures to protect the data.	
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
	2002 Bill	* Must be kept secure and safe. * Must be provided upon request.	Data may not be processed unless: * The data subject has given his explicit consent. * Processing is necessary for the performance of a contract to which the data subject is party *Processing is necessary to comply with a legal obligation *Processing is necessary to protect the vital interests	Only permitted if: * The data subject gives his explicit consent. * It is necessary to comply with an obligation under the employment law. * There are reasons of substantial public interest.	Data controllers must notify the Data Protection Agency before collecting any data unless the Data Protection Agency establishes an exception.	The 2002 Bill updates the above mentioned rights.		

			* Processing is necessary to the performance of a task carried out in the public interest * Processing is necessary to carry out the data controller or a third party legitimate interest. * Protecting against injury or damage to individuals or loss or damage to property in cases where it is not possible to obtain the consent in advance.					
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
IRELAND	2002 Regulations	Not specified	If the telecommunication operator offers this service, it must provide free-of-charge, the following: * Suppression if the	* Telecommunications operators must ensure that the data related to end-users is deleted upon termination of call. * Billing data may	Not specified	* The end-user has the right to be excluded from any directory.	Consumers can register in a central 'opt-out' register to avoid direct marketing.	

			identification of the calling line for outgoing calls. * Suppression of the identification of the calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified. *Override of incoming call identification to prevent malicious calls (not free-of-charge).	only be kept for the period in which the operator is seeking payment from end-user.				
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
ITALY	Data Protection Act	*May only be collected for a specific, explicit & legitimate purpose. * Must be adequate, relevant not excessive, kept up – to – date and no	Data may not be processed unless: *The data subject has given his explicit consent. *Processing necessary for the	May only be processed under explicit written consent of the data subject.	*Data controllers must notify the Data Protection Agency before collecting the data unless processing. *Is necessary to comply with legal	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

		longer the necessary. *Inaccurate or misleading data may not be processed.	performance of a contract to which the data subject is party. *Processing is necessary to comply with a legal obligation. *Processing is necessary to protect the vital interests. . *Processing is necessary to the performance of a task carried out in the public interest. *Processing is necessary to carry out a legitimate interest of the data controller or a third part.		obligations. * Relates to data included or retrieved from public registers. * Relates to classification of correspondence. *Relates to data that is not intended for dissemination and intended for interoffice work.	* Right of Ratification. * Right of Objection.		
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
ITALY	Telecommunications Legislative Decree	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the	If the telecommunication operator offers this service, it must provide free-of-charge, the	* Telecommunications operators must ensure that data related to end-users is deleted upon	* Telecommunications operators must provide itemised bills only if requested by the	* Telecommunications operators must limit the data contained in directories to what is necessary to	Marketing activities using telecommunications are not permitted unless the consumer has	

		communications. Operators must inform the users and the Data Protection Agency if there is any breach in this confidentiality.	following: * Suppression of the identification of the calling line for outgoing calls. *Suppression of the identification of the calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified. * Prevention of automatic call forwarding.	termination of the call. * Billing data may be used by the operator for marketing its own services with prior consumer consent. *Billing data may only be kept for the period in which the operator is seeking payment fro the end-user.	end-user. * The telecommunications operator may not disclose the last three (3) numbers of the calls.	identify the data subject unless the data subject consents. * The end-user has the right to be excluded from any directory.	provided prior written consent.	

DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
LUXEMBURG	1979 law		As a general rule, a data controller is not to seek consent of data subject	Prohibited.	*Data controllers must apply for an authorisation from the Data Protection Agency. Approval tacitly issued within 4 months.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access.	The data controller must implement the technical and organisational measures to protect the data if it is imposed in the authorisation.	Only permitte authoris and wit subject implied consen

						* Right of Ratification.		
LUXEMBURG	2002 law	* May only be collected for a specific explicit and legitimate purpose. * Must be adequate, relevant not excessive and must be kept up-to-date and no longer than necessary. * Inaccurate or misleading data may not be processed. * Must be processed fairly and lawfully.	Data may not be processed unless: * The data subject provides its explicit consent. * Processing is necessary for the performance of a contract to which the data subject is party. * Processing is necessary to comply with a legal obligation. * Processing is necessary to protect the vital interests of the data subject. *Processing is necessary to the performance of a task carried out in the public interest. * Processing is necessary to carry out the data controller or a third party legitimate interest.	Only permitted if: * The data subject gives his explicit consent. * Processing is necessary to protect the vital interests of the data subject and person. * Processing is necessary to comply with employment law commitments * Processing relates to data made public by the data subject. * Processing relates to exercise or defense of legal claims. * Process serves the public interest. * Processing relates to non-profit organisation.	Data controllers must notify before initiating the data collection: In addition, specific authorisation is required where processing: *Relates to interconnection of data. *Relates to solvency of the data subject. *Relates to surveillance. *Relates to purpose other than for which is collected. *Relates to historical, statistical or scientific purposes.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of Rectification. * Right of Objection.		Follows guidelin

TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
LUXEMBURG	Telecommunications Act of 1997	Telecommunications operators an obligation to fulfil a duty of secrecy regarding communication.	Not implemented	Not implemented	Itemised bills will be mandatory from October 1 2002.	Telecommunications operators must limit the data contained in directories to what is necessary to identify the data subject unless the data subject consents.	Not specified.	

DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transl Data***
NETHERLANDS	Data Protection Act	Data may only be collected for a specific explicit and legitimate purpose. Data must be adequate, relevant not excessive, kept up-to-date and no longer than necessary. Inaccurate or misleading data may not be processed.	Data may not be processed unless: * The data subject provides its explicit consent. * Processing is necessary for the performance of a contract to which the data subject is party. * Processing is necessary to comply with a legal	Only permitted if: * The data subject provides its explicit consent. * Processing in necessary to protect the vital interests of the data subject or another person. * Processing is necessary to comply with employment law commitments.	Data controllers must notify the Data Protection Agency before initiating the data collection..	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of Ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follow guideli

		Must develop clear policies for retention and collection of data.	obligation. * Processing is necessary to protect the vital interests of the data subject. * Processing is necessary to carry out a legitimate interest of the data controller or a third party.	* Processing relates to data made public by the data subject. * Processing related to exercise or defense of legal claims. * Processing serves the public interest. * Sensitive data may also be processed for religious, racial and ethnic, political, health and scientific reasons under specific exceptions.				
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
NETHERLANDS	Telecommunications Act	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications. Operator must inform the users of the possibility of a breach in this	If the telecommunication operator offers this service, it must provide for the following purposes: * Suppression if the identification of the calling line for outgoing calls.	* Telecommunications operators must ensure that data related to end-user is deleted upon termination of the call. * Billing data may be used by the operator for	* Telecommunications operators must provide itemised bills only if requested by the end-user.	* Telecommunications operators must limit the data contained in directories to which is necessary to identify the data subject, unless the data subject consents. * The end-users	Marketing activities using telecommunications means are not permitted, unless the consumer has previously consented.	

		confidentiality.	* Suppression of the identification of the calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified.	marketing its own services with prior consent of the consumer. * Billing data may be kept only for the period in which the operator is seeking payment from the end-user. .		have the right (1) to be excluded from any directory (2) to omit part of their address, (3) to request that their data not be used for marketing purposes, and (4) to omit any reference to their sex.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
PORTUGAL	Protection of Personal Data Law	*May only be collected for a specific, explicit & legitimate purpose. * Must be adequate, relevant not excessive, kept up – to – date and no longer the necessary. *Inaccurate or misleading data may not be processed.	Data may not be processed unless: *The data subject has given his explicit consent. *Processing necessary for the performance of a contract to which the data subject is party. *Processing is necessary to comply with a legal obligation.	Only if it is expressly permitted by law or authorisation by the Data Protection Agency.	*Data controllers must notify the Data Protection Agency before initiating the data collection.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of Ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

			*Processing is necessary to protect the vital interests. . *Processing is necessary to the performance of a task carried out in the public interest. *Processing is necessary to carry out a legitimate interest of the data controller or a third part.					
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
PORTUGAL	Telecommunications Law	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications. Operators must inform the users and the Data Protection Agency if there is any breach in this confidentiality.	If the telecommunication operator offers this service, it must provide free-of-charge, the following: * Suppression of the identification of the calling line for outgoing calls. *Suppression of the identification of the	* Telecommunications operators must ensure that data related to end-users is deleted upon termination of the call. * Billing data may be used by the operator for marketing its own services with prior consumer consent.	* Telecommunications operators must provide itemised bills only if requested by the end-user. * The telecommunications operator may not disclose the last four (4) numbers of the calls.	* Telecommunications operators must limit the data contained in directories to what is necessary to identify the data subject unless the data subject consents. * End-users have the right (1) to be excluded from any directory, (2) to	Marketing activities using telecommunications are not permitted unless the consumer has provided prior written consent.	

			calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified. * Prevention of automatic call forwarding.	*Billing data may only be kept for the period in which the operator is seeking payment fro the end-user.		request that their data not be used fro marketing purposes, and (4) to omit any reference to thei sex.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
SPAIN	Personal Data Protection Organic Law	*May only be collected for a specific, explicit & legitimate purpose. * Must be adequate, relevant not excessive, kept up – to – date and no longer the necessary. *Inaccurate or misleading data may not be processed.	Data may not be processed unless: *The data subject has given his explicit consent. *Processing necessary for the performance of a contract to which the data subject is party. *Processing is necessary to comply with a legal obligation.	Only with explicit consent of the data subject.	*Data controllers must notify the Data Protection Agency before initiating the data collection.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of Ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

			*Processing is necessary to carry out the data controller or a third party legitimate interest. * Processing is necessary to protect vital interests of data subject.					
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
SPAIN	Telecommunications Royal Decree	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications. Operators must inform the users and the Data Protection Agency if there is any breach in this confidentiality.	If the telecommunication operator offers this service, it must provide free-of-charge, the following: * Suppression of the identification of the calling line for outgoing calls. *Suppression of the identification of the calling line for incoming calls. * Rejection of incoming calls	* Telecommunications operators must ensure that data related to end-users is deleted upon termination of the call. * Billing data may be used by the operator for marketing its own services with prior consumer consent. *Billing data may only be kept for the period in which the operator is seeking payment fro the end-	* Telecommunications operators must provide itemised bills only if requested by the end-user.	* Telecommunications operators must limit the data contained in directories to what is necessary to identify the data subject unless the data subject consents. * End-users have the right (1) to be excluded from any directory, (2) to omit part of their address, (3) to request that their data not be used for marketing purposes, and (4) to	Marketing activities using telecommunications are not permitted unless the consumer has previously consented.	

			where the calling number is not identified. * Prevention of automatic call forwarding.	user.		omit any reference to their sex.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
SWEDEN	Personal Data Act	*May only be collected for a specific, explicit & legitimate purpose. * Must be adequate, relevant not excessive, kept up – to – date and no longer the necessary. *Inaccurate or misleading data may not be processed.	Data may not be processed unless: *The data subject has given his explicit consent. *Processing necessary for the performance of a contract to which the data subject is party. * Processing is necessary to protect the vital interests of the data subject. *Processing is necessary to comply with a legal obligation. *Processing is	Data may not be processed unless: *The data subject has given his explicit consent. * Processing is necessary to protect the vital interests of the data subject or another person. * Processing is necessary to comply with employment law commitments. * Processing relates to data made public by data subject. *	*Data controllers must notify the Data Protection Agency before initiating the data collection.	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of Ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

			necessary to carry out the data controller or a third party legitimate interest. * Processing is done for purely private purposes. * Processing is necessary to carry out the data controller or a third party legitimate interest. *Processing outweighs the need for protecting data subject. * Processing is necessary pursuant to statute.					
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
SWEDEN	Telecommunications Act	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications. Operators must	If the telecommunication operator offers this service, it must provide free-of-charge, the following: * Suppression of the	* Telecommunications operators must ensure that data related to end-users is deleted upon termination of the call.	* Telecommunications operators must provide itemised bills only if requested by the end-user.	* Telecommunications operators must limit the data contained in directories to what is necessary to identify the data subject unless the data subject	Marketing activities using telecommunications are not permitted unless the consumer has previously consented.	

		inform the users and the Data Protection Agency if there is any breach in this confidentiality.	identification of the calling line for outgoing calls. *Suppression of the identification of the calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified. * Prevention of automatic call forwarding.			consents. * End-users have the right (1) to be excluded from any directory, (2) to omit part of their address, (3) to request that their data not be used for marketing purposes, and (4) to omit any reference to their sex.		
DATA PROTECTION REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***General Requirements***	***Data Processing Requirements***	***Use of Sensitive Data***	***Notification to the Data Protection Agency***	***Rights of Data Subject***	***Security Measures***	***Transb Data I***
UNITED KINGDOM	Personal Data Act 1998	*May only be collected for a specific, explicit & legitimate purpose. * Must be adequate, relevant not excessive, kept up – to – date and no longer the necessary. *Inaccurate or	Data may not be processed unless: *The data subject has given his explicit consent. *Processing necessary for the performance of a contract to which the data subject is party.	Data may not be processed unless: *The data subject has given his explicit consent. * Processing is necessary to protect the vital interests of the data subject or another person.	*Data controllers must notify the Data Protection Agency before initiating the data collection. Notification is not required when: * Data falls within definition of either a relevant filing system or non-automated	Data Subjects have the following rights related to the processing of their data: * Right of Information. * Right of Access. * Right of Ratification. * Right of Objection.	The data controller must implement appropriate technical and organisational measures to protect the data.	Follows guidelir

		misleading data may not be processed. * Must be fairly and lawfully processed.	*Processing is necessary to comply with a legal obligation. *Processing is necessary to carry out the data controller or a third party legitimate interest. * Processing is necessary to perform a public function.	* Processing is necessary to comply with employment law commitments. * Processing relates to exercise or defense of legal claims.	accessible records. * When processing is for public register. * When processing is for staff, administration, advertising, record keeping or non-profit use.			
TELECOMMUNICATIONS REQUIREMENTS/OBLIGATIONS								
Country	***Regulation***	***Confidentiality in Communication***	***Calling Line Identification***	***Use of Billing and Traffic Data***	***Itemized Billing***	***Use of Directories***	***Direct Marketing***	
UNITED KINGDOM	Telecommunications regulations 1999	Telecommunications operators must adopt the necessary measures to preserve the confidentiality of the communications.	If the telecommunication operator offers this service, it must provide free-of-charge, the following: * Suppression of the identification of the calling line for outgoing calls. *Suppression of the identification of the	* Telecommunications operators must ensure that data related to end-users is deleted upon termination of the call. * Billing data may be used by the operator for marketing its own services with prior consumer consent.	Not specified.	* Telecommunications operators must limit the data contained in directories to what is necessary to identify the data subject unless the data subject consents. The end-user has the right to be excluded of any directory.	Marketing activities using telecommunications are not permitted unless the consumer has previously consented.	

			calling line for incoming calls. * Rejection of incoming calls where the calling number is not identified.	*Billing data may only be kept for the period in which the operator is seeking payment fro the end-user.				