ISO/IEC JTC 1/SC 27/WG 5

Information technology - Security techniques - Identity management and privacy technologies

Convenorship/Secretariat: DIN, Germany

Document type: Standing Document

Title: Text for SC 27/WG 5 Standing Document 2 (WG 5 SD2) -- Privacy references list

Status: In accordance with Recommendation 2 (see SC 27 N17400 = WG 5 N800) of the 23rd SC 27/WG 5 meeting held in Hamilton, New Zealand, 18th - 22nd April 2017 this document is being circulated for STUDY AND COMMENT.

Experts and liaison organizations of ISO/IEC JTC 1/SC 27/WG 5 are kindly requested to send their comments/contributions on the above-mentioned document by 2017-10-20. PLEASE submit your comments / contributions on the hereby attached document via the SC 27WG 5 Consultation Application at: http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg5

PLEASE NOTE: For comments please use the SC 27 expert commenting template separately attached to this document.

Secretariat's note: As per Hamilton WG 5 Recommendation 3 the actual deadline for submitting comments was 2017-09-15 but it has been extended and closes by 2017-10-20.

Date of document: 2017-10-20

Source: WG 5 SD2 Editor (Benoit Poletti)

Expected action: COMM

Action due date: 2017-10-20

No. of pages: 1 + 94

Email of secretary: wg5sec@dlist.uni-frankfurt.de

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg5
WG5 Standing Document 2 – Privacy References List

**Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.
Copyright notice

This ISO document is a working draft or committee draft whose copyright has not yet been assigned to ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO’s member body in the country of the requester:

SC27 Secretariat
DIN - Deutsches Institut fuer Normung e.V.
Am DIN Platz
Burggrafenstrasse 6, D-10772 Berlin, Germany
Telephone: + 49 2601-2652
Facsimile: + 49 2601-4-2652
E-mail: krystyna.passia@din.de

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.
CONTENTS

Introduction ................................................................................................................................................. 5
1 Scope .......................................................................................................................................................... 6
  1.1 Purpose................................................................................................................................................ 6
  1.2 Target Audience .................................................................................................................................. 6
2 Normative references .................................................................................................................................. 6
3 Terms and definitions .................................................................................................................................. 7
4 Symbols and Abbreviated Terms ............................................................................................................. 8
5 Privacy regulations ..................................................................................................................................... 9
  5.1 Argentina ............................................................................................................................................... 9
  5.2 Australia .............................................................................................................................................. 9
  5.3 Belgium .............................................................................................................................................. 11
  5.4 Canada .............................................................................................................................................. 11
  5.5 China ............................................................................................................................................... 14
  5.6 Europe ............................................................................................................................................. 15
  5.7 France .............................................................................................................................................. 17
  5.8 Germany ........................................................................................................................................... 18
  5.9 Hong Kong ....................................................................................................................................... 20
  5.10 India .............................................................................................................................................. 21
  5.11 Ireland .......................................................................................................................................... 23
  5.12 Japan ............................................................................................................................................. 24
  5.13 Korea (Republic of) .......................................................................................................................... 26
  5.14 Luxembourg .................................................................................................................................. 28
  5.15 Mexico .......................................................................................................................................... 29
  5.16 Netherlands .................................................................................................................................... 32
  5.17 New Zealand .................................................................................................................................. 33
  5.18 Peru ............................................................................................................................................... 33
  5.19 Portugal ......................................................................................................................................... 34
  5.20 Slovenia ....................................................................................................................................... 37
  5.21 Spain ............................................................................................................................................. 38
  5.22 United Kingdom ............................................................................................................................... 39
  5.23 United States .................................................................................................................................. 41
6 Standards .................................................................................................................................................. 45
  6.1 Information security and PII protection ............................................................................................. 45
  6.2 Financial services ............................................................................................................................... 47
7 Guidelines .................................................................................................................................................. 48
  7.1 Financial services ............................................................................................................................... 48
  7.2 Health Sector .................................................................................................................................... 50
  7.3 Human Resources ............................................................................................................................... 54
  7.4 Marketing ....................................................................................................................................... 56
  7.5 Industry non-specific - Privacy policy establishment ......................................................................... 59
  7.6 Industry non-specific - Trans-border personal data flow ................................................................. 61
  7.7 Technology ..................................................................................................................................... 63
  7.8 Video surveillance .............................................................................................................................. 66
  7.9 Public privacy awareness .................................................................................................................... 68
  7.10 Privacy accreditation ........................................................................................................................ 72
8 Newsletters and forums .......................................................................................................................... 74
9 Organisations and associations .............................................................................................................. 78
10 Projects .................................................................................................................................................. 83
11 Data retention periods ........................................................................................................................... 84
  11.1 Belgium .......................................................................................................................................... 84
  11.2 France ............................................................................................................................................ 85
  11.3 Korea (Republic of) ........................................................................................................................ 87
  11.4 Luxembourg .................................................................................................................................. 88
  11.5 Netherlands ................................................................................................................................... 89
  11.6 Portugal ....................................................................................................................................... 91
  11.7 Slovenia ....................................................................................................................................... 93
  11.8 Switzerland .................................................................................................................................. 94
Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

WG5 SD2 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee 27, Security techniques.
Introduction

Since years 80, with the increase of information systems capacity, the Internet development and the amount of processed personally identifiable information, data privacy has become a major issue for individuals and organisations, as well as for regulatory authorities.

“Data privacy” term corresponds to the rights, recommendations and requirements of individuals, organisations and regulatory authorities with respect to the collection, use, disclosure and retention of personally identifiable information.

References have been published to describe data privacy issues and to determine when, how, and to what extent their personally identifiable information should be used, communicated and shared with others.

The WG5 Standing Document 2 “Privacy References List” provides introductory guidance on privacy-related references.

Please note that the content provided within the WG5 Standing Document 2 shall not be considered as:

- Legal interpretations.
- Having been legally validated by a global law firm or relevant lawyers.
1 Scope

The WG5 Standing Document 2 contains references with relevant descriptions to privacy-related:
   a) Privacy regulatory authorities and regulations.
   b) Standards.
   c) Guidelines.
   d) Newsletters and forums.
   e) Organisations and associations.
   f) Projects.
   g) Data retention periods.

The WG5 Standing Document 2 shall not be considered as:
   • Legal interpretations.
   • Having been legally validated by a global law firm or relevant lawyers.

1.1 Purpose

The WG5 Standing Document 2 provides introductory guidance on privacy-related references to assist individuals, organisations and regulatory authorities in:
   a) Identifying the adequate documentation to privacy issues, initiatives and risks.
   b) Developing privacy policies and practices.

1.2 Target Audience

The WG5 Standing Document 2 provides introductory guidance on privacy-related references to assist individuals, organisations and regulatory authorities in performing activities, which require knowledge and understanding of privacy-related references.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

SC 27 Standing Document 6 (SD 6), Glossary of IT Security Terminology
3 Terms and definitions

For the purposes of this document, following terms apply:

3.1 Data controller

individual person or entity who, according to local data protection and privacy legislation, controls the collection, transfer, modification, usage, storage, archiving, or disposal of personally identifiable information

3.2 Data protection officer

person monitoring the collection, transfer, usage, storage, archiving, and disposal of personally identifiable information within a company

NOTE: The data protection officer should ensure compliance with set privacy requirements by regularly assessing, planning, and acting on appropriate safeguarding mechanisms related to personally identifiable information. Furthermore, the data protection officer should instruct and sensitize employees and management on the specified privacy program of the company.

3.3 Personally identifiable information (PII)

any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

NOTE: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.4 Privacy officer

person monitoring the collection, transfer, usage, storage, archiving, and disposal of PII within a company

NOTE: The privacy officer shall ensure compliance with set privacy requirements by regularly assessing, planning, and acting on appropriate safeguarding mechanisms related to PII. Furthermore, the privacy officer shall instruct and sensitize employees and management on the specified privacy program of the company.
## 4 Symbols and Abbreviated Terms

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APEC</td>
<td>Asia Pacific Economic Co-operation</td>
</tr>
<tr>
<td>APPA</td>
<td>Asia Pacific Privacy Authorities</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>EPIC</td>
<td>Electronic Privacy Information Center</td>
</tr>
<tr>
<td>IAPP</td>
<td>International Association of Privacy Professionals</td>
</tr>
<tr>
<td>JPIPA</td>
<td>Japan enacted the Personal Information Protection Act</td>
</tr>
<tr>
<td>NADPO</td>
<td>National Association of Data Privacy Officers</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PRIME</td>
<td>Privacy and Identity Management for Europe</td>
</tr>
</tbody>
</table>
5 Privacy regulations

5.1 Argentina

Data privacy commissioner

Protección de Datos Personales
http://www.protecciondedados.com.ar/

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Argentina's Personal Data Protection Act of 2000

  This act defines appropriate privacy principles for handling private information including data quality, lawfulness of collection, and consent.

- Security measures for the treatment and maintenance of personal data contained in files, records, databanks or databases

5.2 Australia

Data privacy commissioner

Office of the Privacy Commissioner
Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Privacy Act 1988, Act No. 119 of 1988 (13)

  Following topics are addressed within this act:
  - list of privacy principles
  - applies to the government and private sector
  - governs how the government can collect personal information
  - governs disclosure and access of information

The section 14 of this act stipulates a number of privacy rights known as the Information privacy principles. These principles apply to Australian Government and Australian Capital Territory agencies or private sector organizations contracted to these governments. The principles govern when and how personal information can be collected by these government agencies.

The information must only be collected if relevant to the agencies’ functions. Australians have a right to know why such information about them is being acquired, and who will see the information. Those in charge of storing the information have obligations to ensure such information is neither lost nor exploited. An Australian will also have the right to access the information unless this is specifically prohibited by law.

For the purposes of this act, an act or practice is an interference with the privacy of an individual if the act or practice:
  - in the case of an act or practice engaged in by an agency (whether or not the agency is also a file number recipient, credit reporting agency or credit provider)—breaches an Information Privacy Principle in relation to personal information that relates to the individual;
  - in the case of an act or practice engaged in by a file number recipient (whether or not the file number recipient is also an agency, organisation, credit reporting agency or credit provider)—breaches a guideline under section 17 in relation to tax file number information that relates to the individual;
  - (ba) constitutes a breach of Part 2 of the Data matching Program (Assistance and Tax) Act 1990 or the guidelines in force under that Act;
  - (bb) constitutes a breach of the guidelines in force under section 135AA of the National Health Act 1953;
  - involves an unauthorised requirement or request for disclosure of the tax file number of the individual; or
  - (d) in the case of an act or practice engaged in by a credit reporting agency or credit provider (whether or not the credit reporting agency or credit provider is also an agency, organization or file number recipient)—constitutes a credit reporting infringement in relation to personal information that relates to the individual.
5.3 Belgium

Data privacy commissioner

Commission for the Protection of Privacy / Commission de la protection de la vie privée
www.privacycommission.be

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Amended Data Protection Law

This law is a transposition from the European Directive 95/46/EC.

5.4 Canada

Data privacy commissioner

Office of the Privacy Commissioner of Canada
www.privcom.gc.ca

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Privacy Act ( R.S., 1985, c. P-21 )

The federal Privacy Act, in place since 1983, protects the personal information collected by government institutions. Essentially, the Privacy Act is a code of ethics for the government's handling of our personal information. The Privacy Act ensures that Canadians can access information collected about them, and can challenge the accuracy of the information.
This act requires that information be:

- collected by government institutions in relation to operating programs or activities
- collected from the individual personally
- accurate and up to date
- subject to correction by the individual
- used only for the purpose for which it was originally collected

This act is Canadian federal legislation that came into effect on July 1, 1983. The act sets out rules for how institutions of the federal government must deal with personal information of individuals. Some salient provisions of the legislation are as follows:

- a government institution may not collect personal information unless it relates directly to an operating program or activity of the institution (section 4).
- with some exceptions, when a government institution collects an individual's personal information from the individual, it must inform the individual of the purpose for which the information is being collected (section 5(2)).
- with some exceptions, personal information under the control of a government institution may be used only for the purpose for which the information was obtained or for a use consistent with that purpose, unless the individual consents (section 7).
- with some exceptions, personal information under the control of a government institution may not be disclosed, unless the individual consents (section 8).
- every Canadian citizen or permanent resident has the right to be given access to personal information about the individual under the control of a government institution that is reasonably retrievable by the government institution, and request correction if the information is inaccurate (section 12).

The Privacy Commissioner of Canada receives and investigates complaints, including complaints that an individual was denied access to his or her personal information held by a government institution (section 29).

- Personal Information Protection and Electronic Documents Act (2000, c. 5)
  

The Personal Information Protection and Electronic Documents Act (PIPEDA) addresses the collection, storage and use of personal information by organizations in the private sector. Its provisions apply to information collected, used or disclosed by federally regulated agencies, such as telecommunications companies, ISPs, broadcasters, airlines and banks. PIPEDA also applies to federally regulated companies that conduct business online; and it extends to businesses in Nunavut, the Yukon and the Northwest Territories.

The law also applies to provincially-regulated private-sector organizations, such as insurance companies and retail stores, unless the province has passed "substantially similar" legislation.

At present, Quebec is the only province or territory that has been found by the Privacy Commissioner of Canada to have substantially similar legislation in place. However, Alberta and British Columbia have both passed private sector privacy
legislation which came into effect on January 1, 2004, though the Privacy Commissioner has yet to determine whether or not these acts are substantially similar to PIPEDA.

PIPEDA gives individuals the right to see and correct any personal information about them collected by companies in the course of their commercial activities. These provisions state that businesses must inform consumers of who is collecting the information, why the information is being gathered, and for what purposes it will be used.

Under the law’s guidelines, personal information can be collected about you only as long as it is:
✓ gathered with the knowledge and consent of the consumer
✓ collected for a reasonable purpose
✓ used only for the reasons for which it was gathered
✓ accurate and up to date
✓ open for inspection and correction by the consumer
✓ stored securely

The Personal Information Protection and Electronic Documents Act (abbreviated PIPEDA or PIPED Act) is a Canadian law relating to data privacy. It governs how private-sector organizations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA was passed in the late 1990s to promote consumer trust in electronic commerce. The act was also intended to reassure the European Union that Canadian privacy laws were adequate to protect the personal information of European citizens.

PIPEDA incorporates and makes mandatory provisions of the Canadian Standards Association’s Model Code for the Protection of Personal Information, developed in 1995.

The law gives individuals the right to:
✓ know why an organization collects, uses or discloses their personal information;
✓ expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented;
✓ know who in the organization is responsible for protecting their personal information;
✓ expect an organization to protect their personal information by taking appropriate security measures;
✓ obtain access to their personal information and ask for corrections if necessary; and
✓ complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

The law requires organizations to:
✓ obtain consent when they collect, use or disclose their personal information;
✓ supply an individual with a product or a service even if they refuse consent for the collection, use or disclosure of your personal information unless that information is essential to the transaction;
✓ collect information by fair and lawful means; and
have personal information policies that are clear, understandable and readily available.

Though this act requires that affected organizations comply with the CSA Model Code for the Protection of Personal Information, there are a number of exceptions to Code where information can be collected, used and disclosed without the consent of the individual. Examples include for investigations related to law enforcement or in the event of an emergency. There are also exceptions to the general rule that an individual shall be given access to his or her personal information.

5.5 China

On December 28th, 2012, the National People’s Congress Standing Committee’s Decision Concerning Strengthening Network Information Protection was published. The Decision in the statutory form protects the information security of individual citizens and legal persons, puts into place the network identity management system, clarifies the duties and responsibilities of the network service providers, and provides the government agencies responsibility of necessary supervision.

The summary of this Decision is as following:

I. The nation shall protect the electronic information that provides citizens' personal identity information and privacy.

II. When organizations collect and use the citizens' electronic information, they shall clarify the purpose, mode and scope of the collection and use of the information and get the related citizens' consent prior to information collection. They shall make public the rules of collecting and using the electronic information of individual citizens.

III. The organizations’ staff shall keep confidential the citizens' personal electronic information they have collected in work. They shall not leak, tamper, damage information, and sell or illegally provide the information to others.

IV. The organizations should adopt techniques or other necessary measures to ensure information security and prevent the leakage, damage and loss of the citizens' personal electronic information they have collected in work. In case of incidents happens, remedial measures shall be taken promptly.

V. The network service providers shall strengthen management of the information they have released to the users. When the information is forbidden by law, measures should be taken to immediately stop transmission of such information and eliminate it.

VI. If the citizen has evidence that his personal information is leaked, his privacy is spread, his legitimate rights and interests are infringed on, or he is harassed by electronic commercial information, the citizen has the right to require the network service providers to delete relevant information or take other necessary measures to stop it.
5.6 Europe

Article 29 Data Protection Working Party

Tasks of this Working Party

Article 29 Data Protection Working Party was set up to achieve several primary objectives:

- To provide expert opinion from member state level to the Commission on questions of data protection.
- To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities.
- To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.
- To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC.

URL(s)
http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

European directives

- Directive 95/46/EC ("Data Protection Directive")

  This directive relates to the protection of individuals rights with regard to processing of personal data and the free movement of such data.

  The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (art. 4) Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any online business trading with EU citizens would process some personal data and would be using equipment in the EU to process the data (i.e. the customer's computer). As a consequence, the website operator would have to comply with the European data protection rules.

- Directive 2002/58/EC on privacy and electronic communications
The Electronic Privacy Directive has been drafted specifically to address the requirements of new digital technologies and ease the advance of electronic communications services. This directive complements the Data Protection Directive and applies to all matters which are not specifically covered by that directive. In particular, the subject of this directive is the “right to privacy in the electronic communication sector” and free movement of data, communication equipment and services.

Position of the Council of the European Union

- Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Convention 108 from the Council of Europe

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

  Please note that this convention is an international agreement that surpasses European geographic boundaries, since it is open to non-European signatories, such as for instance Uruguay and Morocco.

- Modernisation project that relates to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp
5.7 France

**Data privacy commissioner**

Commission Nationale de l’Informatique et des Libertés


**Laws and regulations**

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Loi Informatique et Liberté (Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties)
  

  It is a law regarding data processing, data files and individual liberties.

  The principles that are addressed in it are the following:

  - **fair and lawful collection and processing:**
    any fraudulent, unfair or illegal collection of data is prohibited (Article 226-18 of the Penal Code: 5 years imprisonment, 300 000 € fine)

  - **purpose limitation:**
    data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes.
    Data (nature of the data recorded, categories of persons or organisations who may receive these data, and the retention period of those data) shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing (Articles 226-21 and 226-20 of the Penal Code: using personal data for purposes other than those that justified their collection, or storing them beyond a date justified by the purpose of the processing is punished, respectively, by 5 years’ imprisonment and a 300 000 € fine).

  - **accuracy of data:**
    data shall be accurate, complete and, where necessary, kept up-to-date. Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and incomplete with regard to the purposes for which they are obtained and processed;

  - **information of individuals:**
    the persons whose personal data are collected must be informed of (1) the identity of the data controller and of his representative, if any; (2) the purposes of the processing for which the data are intended; (3) whether replies to the
questions are compulsory or optional; (4) the possible consequences for him of the absence of a reply; (5) the recipients or categories of recipients of the data; (6) the rights granted to him by Section 2 Chapter V (rights of individuals in relation to the processing of data); (7) when applicable, the intended transfer of personal data to a State which does not belong to the European Union.

If the data are obtained by way of a questionnaire, the information provided for in Sub-sections (1), (2), (3) and (6) shall be directly mentioned on this questionnaire.

✓ reinforced protection of sensitive data:
personal data which reveal racial or ethnics origins, political, philosophical or religious opinions, or trade union affiliation of persons, or which concern their health or sexual life can only be collected and recorded with the express (written) agreement of the person concerned, with some exceptions such as public interest. Article 226-19 of the Penal Code punishes any breach of these provisions by 5 years' imprisonment and a 300,000 € fine.

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000824352&dateTexte

This legal document is a transposition from the European Directive 95/46/EC.

5.8 Germany

Data privacy commissioner

The Federal Commissioner for Data Protection and Freedom of Information
http://www.bfdi.bund.de

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) – Published September 1st 2009

The BDSG implements the European Directive 95/46/EC and transfers it into a national law.
The purpose of this act is, through technology-neutral regulation, to promote competition and efficient infrastructures in telecommunications and to guarantee appropriate and adequate services throughout the Federal Republic of Germany. The act addresses public telecommunications network operators and providers of publicly available telecommunications services.

This act serves to transpose the following EU Directives:


Privacy aspects are covered in the following clauses:

- chapter 2 - Access Regulation - § 17 - Confidentiality of Information
- PART 3 - CUSTOMER PROTECTION
  - section 47 - Provision of Subscriber Data
- chapter 2 – Numbering - Section 66 – Numbering
  - PART 6 - UNIVERSAL SERVICE - Section 85 - Suspension of Service
  - PART 7 - PRIVACY OF TELECOMMUNICATIONS, DATA PROTECTION, PUBLIC SAFETY
    - section 89 - Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy
    - section 90 - Misuse of Transmitting Equipment
- chapter 2 - Data Protection - Section 91 - Scope
  - section 92 - Transfer of Personal Data to Foreign Private Bodies
  - section 93 - Duty to Provide Information
  - section 94 - Consent by Electronic Means
  - section 95 - Contractual Relations
  - section 96 - Traffic Data
  - section 97 - Charging and Billing
  - section 100 - Faults in Telecommunications Systems and Telecommunications Service Fraud
  - section 102 - Line Identification Presentation and Restriction
  - section 109 - Technical Safeguards
The Telemedia Act (Telemediengesetz - TMG) – Published February 26th 2007  

The TMG applies for all electronic information- and communications services. TMG does not overrule the TKG. TMG regulates the telemedia; i.e. electronic media information that is part of a commercial service offering.

The TMG replaces TDG and TDDSG. It also incorporates several statements/obligations of the Mediendienstestaatsvertrages (MDStV).

Privacy aspects are covered in the following clauses:
- section 3 – Responsibility - §7 General principles
- section 4 – Data Protection - § 11 Provider-User Relationship
- § 12 Principles
- § 13 Duties of the Service Provider
- § 14 Personal base data
- § 15 Personal usage data

Further data protection laws persist within the 16 countries (Länder) of Germany, in the criminal act (StGB), in the information freedom act (IFG), Ordinance concerning the Technical and Organizational Implementation of Measures for the Interception of Telecommunications (TKÜV).

5.9 Hong Kong

Data privacy commissioner

The Office of the Privacy Commissioner for Personal Data  
http://www.pcpd.org.hk

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- The Personal Data (Privacy) Ordinance Cap 486 of 1995 (as amended in 2012)  

PDPO governs the collection, processing, accuracy, retention, use, access and correction of personal data covering both the public and the private sectors. The six data protection principles of PDPO are:
1. Personal data shall be collected for a purpose directly related to a function and activity of the data user; lawful and fair collection of adequate data; persons shall be informed of the purpose for which the data are collected and to be used.

2. All practicable steps shall be taken to ensure the accuracy of personal data; data shall be deleted by data users and data processors upon fulfilment of the purpose for which the data are used.

3. Unless the person has given prior consent, personal data shall be used for the purpose for which they were originally collected or a directly related purpose.

4. All practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure by data users and data processors.

5. Formulates and provides policies and practices in relation to personal data.

6. Individuals have rights of access to and correction of their personal data. Data users should comply with data access or data correction request within the time limit, unless reasons for rejection prescribed in the Ordinance are applicable.

PDPO has a criminal provision prohibiting the use of personal data for direct marketing activities without the person’s consent (Part 6 A).

5.10 India

**Data privacy commissioner**

The mechanism for privacy protection in India at present is through the provisions of the Indian Information Technology (IT) Act 2000, as amended in 2008. According to the IT Act 2000, IT Secretaries (senior ranked government official with quasi judicial powers) of all the States and Union Territories have been bestowed upon with the responsibility of adjudicating cases pertaining to privacy violation in conformance with section 43A of the IT (Amendment) Act, 2008. They have the power to order compensation of up to 5 Crore Indian Rupees (INR) to the affected person, beyond which matters can be pursued in civil courts.

**Laws and regulations**

*Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.*

- The IT (Amendment) Act, 2008 (ITAA 2008):
  [http://deity.gov.in/content/cyber-laws](http://deity.gov.in/content/cyber-laws)
Enacted in year 2009, the section 43A of the ITAA 2008 mandates ‘body corporates’ in India to protect ‘sensitive personal data or information (SPDI)’ of individuals which is dealt with in a ‘computer resource’ by implementing ‘reasonable security practices’. There is a provision for compensating an individual whose privacy has been compromised because of negligence on part of the ‘body corporate’.

The Government of India notified rules under sec 43A in April 2011, defining SPDI and ‘reasonable security practices’ and very importantly laying out the rules for protection of SPDI.

Rule 3 of Section 43A of the ITAA 2008 defines what constitutes SPDI and includes personal financial information, medical records, biometric information, sexual orientation, physical & physiological conditions, among others.

The rules have also defined privacy principles via protection requirements (Rules 4, 5 & 6), these principles are (i) Privacy Policy (Notice) (ii) Choice & Consent (iii) Collection Limitation (iv) Use Limitation (v) Access & Correction (vi) Security (v) Disclosure (vi) Discrepancies & Grievance Redress.

Rule 7 facilitates transfer of SPDI by a body corporate to any other entity located within or outside India that ensures same level of data protection as provided for under the sec 43A Rules.

Rule 8 defines ‘reasonable security practices’ and recognizes ISO 27001 as one of the approaches which can be adopted by the organizations to design their information security programs for securing SPDI. This rule also has provision to recognize ‘codes of practices’ developed by industry associations. Through this rule, the Government has mandated audit of security practices followed by organizations by an independent government approved auditor.

Section 72A of the ITAA 2008 can potentially lead to criminal liability on the person (natural or juristic) if personal information of an individual is disclosed with an intent to cause wrongful loss or wrongful gain, without consent of the person subject and / or in breach of a lawful contract.

Right to Information (RTI)
http://www.ncl.nic.in/new/THE_RIGHT_TO_INFORMATION_ACT.pdf

Section 8 of the RTI Act exempts certain types of information from public disclosure to protect privacy of individuals. When contested, the Information Commissioners can use a public interest test to determine if the public’s right to information should supersede an individual’s right to privacy.
5.11 Ireland

Data privacy commissioner

Data Protection Commissioner
http://www.dataprotection.ie/

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Data Protection Act of 1988

  This act defines the use and disclosure of personal data (i.e. how data are handled, stored, collected, disclosed and managed in a specific manner).

  This act gives effect to the convention for the protection of individuals with regard to automatic processing of personal data done at Strasbourg on the 28th day of January, 1981, and for that purpose to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically.

  This act protects individuals with regard to automatic processing of personal data and to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically.

- Data Protection (Amendment) Act 2003

  This act is an amendment of the Data Protection Act of 1988.

- Consolidated Act between Data Protection (Amendment) Act 2003 and Data Protection Act of 1988
http://www.dataprotection.ie/viewdoc.asp?DocID=796&ad=1
5.12 Japan

Data privacy commissioner

Office of Personal Information Protection, Cabinet Office, Government of Japan
http://www.cao.go.jp/index-e.html

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Information Protection Act (JPIPA), 2003

- The Act on Regulation of the Transmission of Specified Electronic Mail (Act No. 26 of April 17, 2002 – updated on June 2008)
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/laws_d103.html
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/Specified-E-mail-index.pdf
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syoji/m_mail.html (Japanese only)

  This act relates on anti-spam mail.

  http://www.japaneselawtranslation.go.jp/law/detail_main?id=131&vm=4&re=

  The purpose of this act is to protect the rights and interests of individuals while achieving proper and smooth administrative management, in view of a remarkable increase in the use of personal information in administrative organs, by providing for the basic matters concerning the handling of personal information in such organs.

- Radio Act (Act No. 131 of May 2, 1950 – updated on June 24, 2011 under Act No. 74), in particular its clauses 59 and 109

  Clause 59 and 109 mandates the protection of secrecy and illegalized the unauthorized decryption of the encrypted communication.


  The clause 3 mandates that the communications service providers must not censor the communication.
The clause 4 mandates that the communications service providers must maintain the secrecy for the communication among the parties.

- Civil Code (Act No.89 of April 27, 1896 – updated on June 24, 2011 by Act No. 74), in particular its articles 709 and 710
  http://law.e-gov.go.jp/htmldata/M29/M29HO089.html (Japanese only)
  http://www.japaneselawtranslation.go.jp/law/detail/?re=01&yo=民法&ft=2&ky=&page=2

The article 709 defines damages in torts. “A person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence.”

The article 710 defines compensation for damages other than property as: “Persons liable for damages under the provisions of the preceding Article must also compensate for damages other than those to property, regardless of whether the body, liberty or reputation of others have been infringed, or property rights of others have been infringed.”

- The Act on the Use of Numbers to Identity a Specific Individual in the Administrative Procedure (Act No. 27 of May 31, 2013 -- Updated June 25, 2014 under Act No. 83)
  http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/en3.pdf (English)

Guidelines

- Guidelines for the online notice and consent from consumers

- Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information

These guidelines specify pursuant to Article 8 of the Act the necessary matters concerning the matters set forth by the Act, are formulated as practical guidelines to support the activities performed by entities and others to ensure the proper handling of personal information in sectors, over which the Ministry of Economy, Trade and Industry holds jurisdiction, and specific sectors (hereinafter referred to as “economic and industrial sectors”), in which the Minister of Economy, Trade and Industry is designated as a competent minister pursuant to Paragraph 1 of Article 36 of the Act.
5.13 Korea (Republic of)

Data privacy commissioner

The Korean Government Personal Information Protection Commission

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Information Protection Act – Promulgated on March 29th, 2011, Effective on September 30th, 2011.
  http://www.pipc.go.kr/cmt/english/functions/pipact.do (provided by the Korean government personal information commission)
  http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf (provided by the Korean Law via the Internet - http://koreanlii.or.kr/)

7. Objective
   - To increase the people’s rights and to ensure the protection of the people’s dignity and values.

8. Principles of personal information protection
   - Goal specification, minimum collection, accuracy of information, safe management etc.

9. The establishment of the Personal Information Protection Commission
   - Independently performs affairs under the direct jurisdiction of the President; and
   - Deliberates on and resolves matters concerning the protection of personal information.

10. Protection guideline in each step of processing personal information
    - Minimum collection based on consent of information;
    - Prohibition of personal information management for other purposes;
    - Careful protection of sensitive information and unique identifying information;
    - Guarantee of access to individual information; and
    - Prompt destruction of information that has met its initial objective and/or exceeded its holding period.

11. Regulation of image data processing equipment
    - Guideline of installation and operation of data processing equipment like CCTV etc.

12. Introduction of the Personal Information Impact Assessment
    - Analyze risk factors and discover improvements in managing personal information files.

13. Remedies for violations of personal information
    - Liability for compensation for damage;
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

- Establishment of Personal Information Dispute Mediation Committee; and
- Introduction of collective dispute mediation and Class Actions.

- Act on promotion of information and communications network utilization and information protection, etc, established on May 12, 1986 and lastly revised March 23, 2013

  The purpose of this act is to contribute to the improvement of citizens' lives and the enhancement of public welfare by facilitating utilization of information and communications networks, protecting personal information of people using information and communications services, and developing an environment in which people can utilize information and communications networks in a sounder and safer way.

- Act on the protection and use of location information, established on January 27, 2005 and lastly revised February 29, 2008
  http://eng.kcc.go.kr/user.do?page=E02090000&dc=E02040000

  Main purposes of this act are to protect privacy against the leak, abuse and misuse of location information, to promote a safe environment for using location information and reinvigorate the use of location information, and thus to contribute to the improvement of national life and the promotion of public welfare.
5.14 Luxembourg

Data privacy commissioner

Commission Nationale pour la Protection des Données
http://www.cnpd.lu

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Amended Act of August 2nd, 2002 ("Data Protection Act")

  This act is a transposition from the European Directive 95/46/EC. This act has been amended by the Act of July 27th, 2007.

- Grand-Ducal Regulation of November 27th, 2004 (data protection officers)
  http://www.legilux.public.lu/leg/a/archives/2004/2002012/2002012.pdf#page=2&zoom=125,0,0

  It is a regulation explaining the scope and responsibilities of the “Data Protection Officer”.

- Amended Act of May 30th, 2005 (data protection and electronic communications)
  http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi30052005_en.pdf (English version of the original one)

  It is the data protection act for the telecommunications industry. This act has been amended by the Act of July 27th, 2007.

5.15 Malaysia

Data privacy commissioner

Office of Personal Data Protection Commissioner
http://www.pdp.gov.my

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Data Protection Act 2010 (Act 709)

The Personal Data Protection Act 2010 (Act 709), an Act to regulate the processing of personal data in commercial transactions requires a person who either jointly or in common with other persons process any personal data or has control or authorizes the processing of any personal data to be registered according to the class of data user sets out in the Order.

5.15 Mexico

Data privacy commissioner

“Instituto Nacional de Acceso a la Información y Protección de Datos” (INAI)
National Institute for Access to Public Information and Data Protection
http://inicio.ifai.org.mx/

The objectives of this Institute are:

a) To facilitate and ensure the access of people to public information, access to and protection of personal data, and to contribute to the organization of the national archives.

b) To promote a culture of transparency in governance and government accountability to society, and the exercise of the rights of citizens regarding access to information and protection of personal data.

c) To contribute to the processes of analysis, deliberation, design and issuance of necessary legal norms concerning archives and personal data, as well as in legislative procedures to improve and strengthen the regulatory and institutional framework for transparency and access to public information.
Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

In Mexico there are the following two laws on personal data protection:

- “Federal Law of Transparency and Access to Public Government Information” (2002) responsible for ensuring the protection of personal data and access for everyone to information held by the branches of government, autonomous constitutional bodies or those with legal autonomy, and any other federal entity; and
- “Federal Law on Protection of Personal data Held by Private Parties” (2010) establishing the protection of personal data held by private parties, in order to regulate their legitimate treatment, controlled and informed, in order to ensure privacy and the right to personal data self-determination.

Public sector

- Federal Law of Transparency and Access to Public Government Information
  [http://www.diputados.gob.mx/LeyesBiblio/ref/lftaipg/LFTAIPG_orig_11jun02.pdf](http://www.diputados.gob.mx/LeyesBiblio/ref/lftaipg/LFTAIPG_orig_11jun02.pdf)
  This law establishes the obligation of the parties for the protection of personal data, hence they must adopt adequate procedures for receiving requests for access and correction of data, training public servants on the policy of protection of personal data, perform an adequate treatment, relevant and not excessive and in compliance with the purposes for which they collected personal data, make available to individuals the document where the aims of treatment are established and take the necessary measures to ensure the security of data reducing at all times personal alteration, loss, transmission and unauthorized access.

Private sector

- Federal Law on Protection of Personal Data held by Private Parties (LFDPPP)
- Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties
  To fulfill the LFPDPPP arises in the year 2011, the Regulations states that the data controllers or data processors of personal data must comply with the principles of legality, consent, information, quality, purpose, loyalty, proportionality and responsibility and the duties of security and confidentiality in the processing of personal data by specific measures such as developing an inventory of personal data, defining the roles and responsibilities of those involved in the treatment, conducting a risk analysis to identify events that may compromise the security of personal data, establishing security measures, conducting reviews and audits to ensure compliance with established controls and training the staff involved in the treatment.
In support for these measures, INAI has created guidelines and recommendations to help managers and organizations in meeting LFPDPPP.

- Guidance to comply with the principles and duties of the LFPDPPP
  http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf

- Privacy notice guidelines
  http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Lineamientos_DOF.pdf

- Guide to implement compensatory measures privacy notices

- Recommendations for appointment of the person or department of personal data

- Risk Analysis Methodology BAA
  http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Analisis_de_Riesgo_BAA_nuevo_aviso.pdf

- Information security recommendations

INAI has encouraged the adoption by data controllers and data processors of self-regulation schemes consisting in a set of principles, standards and the voluntary adoption of procedures in order to respect to personal data treatments. The following document establishes parameters of self-regulation for the Protection of Personal Data (2014) and defines the implementation of a Personal Data Management System. México is the first country that developed an autoregulation scheme that can be certified thorough an accredited third party recognized by the authority, certifying compliance with the principles, duties and obligations stated in the law.

http://www.rea.ifai.org.mx/_catalogs/masterpage/Sec6_1.aspx

Documentation related to self-regulation schemes and management systems:

- Parameters of self-regulation on the protection of personal data

- Manual on security of personal data for small and medium organizations

- Guide to implement a Personal Data Security Management System
5.16 Netherlands

Data privacy commissioner

Dutch Data Protection Authority
http://www.dutchdpa.nl

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Data Protection Act

  The most important rules for recording and using personal data have been set forth in the Wet bescherming persoonsgegevens (Wbp; Personal Data Protection Act). This act was unanimously adopted by the Dutch House of Representatives on 23 November 1999 and accepted by the Dutch Senat on 3 July 2000. The act came into force on 1 September 2001.
  The Wbp relates to every use - ‘processing’ - of personal data, from the collection of these data up to and including the destruction of personal data.

  The Ministry of Justice has published guidelines for personal data processors:
  ✓ http://english.justitie.nl/images/handleidingwbpuk_tcm75-28677_tcm35-15485.pdf?refer=true&theme=purple

  Notification obligation and exemption from the notification obligation
  The supervisory authority, the Dutch DPA must be notified of all processing of personal data. The Dutch DPA keeps a public register of these notifications. However, a large number of socially well known and accepted processing operations have been exempted from the notification obligation. On this web site, the Dutch DPA offers a checklist for the use of the exemption decree.

  Technology
  The Wbp has a separate section (Section 13) on the use of technology in the protection of personal data.

  Supervision of compliance with the Wbp and enforcement of the Wbp
  The Wbp also governs the tasks and powers of the supervisor of the act, the Dutch DPA. As a national supervisory authority, the Dutch DPA is the successor of the former Registratiekamer. The Dutch DPA is authorised to impose sanctions.

  Data protection officer
  Organisations can also appoint their own internal supervisor, the data protection officer.
5.17 New Zealand

Data privacy commissioner
Office of the Privacy Commissioner
http://www.privacy.org.nz

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Privacy Act 1993

This act is the primary law regarding privacy in New Zealand. This is supplemented by codes of practice for key sectors (such as health). Elements of the Privacy Act are overridden by other pieces of legislation for specific purposes (such as taxation information).

The Office of the Privacy Commissioner website has up to date information about the Privacy Act, and copies of codes of practice.

Please note that it is stated in this act that its objective is to promote and to protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

5.18 Peru

Data privacy commissioner
Autoridad Nacional de Protección de Datos Personales
http://www.minjus.gob.pe/proteccion-de-datos-personales/
Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Ley 29733 – Protection to Personal Data ACT

- Regulation for the law

- Security directive
  http://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

- Directorial resolutions
  http://www.minjus.gob.pe/resoluciones-directorales-dgpdp

5.19 Portugal

Data privacy commissioner

CNPD
http://www.cnpd.pt/
Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

Protection of Personal Data

- Article 35 of the Constitution of the Portuguese Republic - use of information technology
  https://www.cnpd.pt/bin/legis/nacional/ARTIGO_35_CRP.pdf

- Law 67/98 - Personal Data Protection Act
  https://www.cnpd.pt/bin/legis/nacional/LPD.pdf

  https://www.cnpd.pt/bin/legis/nacional/Lei103_2015.pdf

- Law 2/94 - Establishes the control and monitoring mechanisms of the Schengen Information System
  https://www.cnpd.pt/bin/legis/nacional/Lei2-94-Schengen.pdf

- Law 68/98 - National entity in the Joint Supervisory Body of EUROPOL
  https://www.cnpd.pt/bin/legis/nacional/Lei68-98.pdf

- Law 36/2003 - Regulates the status and powers of the national member of EUROJUST
  https://www.cnpd.pt/bin/legis/nacional/lei36-03.pdf

- Law 43/2004 - Law on the organization and operation of CNPD

Health

- Law 12/2005 - Personal health genetic information

Electronic Communications

- Decree-Law 7/2004 - E-Commerce
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

- Law 41/2004 - Regulates the protection of personal data in the electronic communications sector - (amended and republished)

  [https://www.cnpd.pt/bin/legis/nacional/Lei_46_2012.pdf]


- Law 32/2008 - Transposes the Data Retention Directive on the retention of electronic communications data
  [https://www.cnpd.pt/bin/legis/nacional/Lei32-2008_retencao_dados.pdf]

- Law 5/2004 - Provides for the creation of a database of debtor subscribers of electronic communications services (altered and republished)
  [https://www.cnpd.pt/bin/legis/nacional/Lei_5_2004.pdf]

**Video surveillance**

- Law 34/2013 – Use of video surveillance systems by private security and autoprotection services
  [https://www.cnpd.pt/bin/legis/nacional/Lei_34_2013_Seguranca_privada.pdf]

- Ordinance 273/2013 - Regulates Law 34/2013
  [https://www.cnpd.pt/bin/legis/nacional/Portaria_273_2013_Seguranca_privada.pdf]

  [https://www.cnpd.pt/bin/legis/nacional/LEI_9_2012.pdf]

- Decree-Law 207/2005 – Regulates the means of roads electronic surveillance used by the security forces

- Law 51/2006 – Regulates the use of road surveillance systems by the EP and the road concessionaires
  [https://www.cnpd.pt/bin/legis/nacional/LEI51-2006-VVG-AUTOESTRADAS.pdf]

- Law 33/2007 - Regulates the installation and use of video surveillance systems in taxis
  [https://www.cnpd.pt/bin/legis/nacional/Lei33-2007-vvg-taxis.pdf]

- Ordinance 1164-A / 2007 - Approves the model of video surveillance notice in taxis
**ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2**

**Work**

- Law 7/2009 - Approves the Labor Code
  

**Citizen’s card**

- Law 7/2007 - Creates citizen’s card and governs its issuance and use
  

**Cybercrime**

- Law 109/2009 - Cybercrime Law
  

**5.20 Slovenia**

**Data privacy commissioner**

Information Commissioner of Slovenia

[http://www.ip-rs.si](http://www.ip-rs.si)

**Laws and regulations**

*Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.*

- Personal Data Protection Act of Slovenia (Official Gazette of Slovenia, No. 94/2007; ZVOP-1-UPB1)
  

  This act is a transposition from the European Directive 95/46/EC.
5.21 Spain

Data privacy commissioner
Spanish Data Protection Agency
http://www.agpd.es

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Organic Law 15/1999
  This law guarantees and protects the public liberties and fundamental rights of natural persons, and in particular their personal and family privacy, with regards to the processing of personal data.

- ROYAL DECREE 1720/2007
  This decree approves the regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data.

- Act 34/2002 on Information Society Services and Electronic Commerce
  This act relates to the sending of commercial communications by electronic mail or another equivalent means of electronic communication.

  It shall be the task of the Spanish Data Protection Agency to impose sanctions for the commission of the infractions listed in articles 38.3 c), d) and i) and 38.4 d), g) and h) hereof.

- Act 41/2002 on Health
  It is a basic regulating act on the autonomy of the patient and on the rights and obligations in matters of clinical information and documentation.

- Act 32/2003 State Telecommunications Act
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

- Act 62/2003 on fiscal measures, administrative measures and measures of a social nature

- Instrucción 1/2006 on processing personal data for surveillance purposes through camera or video-camera systems

- Instrucción 1/2000 on the rules governing international data movements

- Instrucción 1/1995 regarding the rendering of information services on creditworthiness and credit

5.22 United Kingdom

Data privacy commissioner

Information Commissioner’s Office
https://ico.org.uk/

There is a wide range of Codes of Practice, Guidance and other documentation available from the Information Commissioner's web site. These relate to both organizations implementing the UK legislation and to individuals whose personal data is protected by the legislation.

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Data Protection Act 1998, 1998 Chapter 29, Part II (7)
  http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

  This act defines rights of access to personal data.

  The Data Protection Act (DPA) is a United Kingdom Act of Parliament. It defines a legal basis for the handling in the UK of information relating to living people. It is the main piece of legislation that governs protection of personal data in the UK. Although this act does not mention privacy, in practice it provides a way in which individuals can enforce the control of information about them. Most of this act does not apply to domestic use, for example keeping a personal address book. This act is used by many companies & organizations in the United Kingdom.
Compliance with this act is overseen by an independent government authority, the Office of the Information Commissioner (OIC). The OIC maintains Guidance relating to this act.

This act defines eight principles of information-handling practice.

The UK Data Protection Act is a large act, and has a reputation for complexity. Whilst the basic principles are honored for protecting privacy, interpreting the act is not always simple. Many companies, organizations and individuals seem very unsure of the aims, content and principles of the DPA. Some hide behind this act and refuse to provide even very basic, publicly available material quoting this act as a restriction.

Data may only be used for the specific purposes for which it was collected.

Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (for example, the prevention or detection of crime). It is an offence for other parties to obtain these personal data without authorization.

Individuals have a right of access to the information held about them, subject to certain exceptions (for example, information held for the prevention or detection of crime).

Personal data may be kept for no longer than is necessary.

Personal data may not be transmitted outside the EEA unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.

Subject to some exceptions for organizations that only do very simple processing, and for domestic use, all entities that process personal information must register with the Information Commissioner.

Entities holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organizational measures (such as staff training).
5.23 United States

Data privacy regulatory authorities

The Federal Trade Commission
www.ftc.gov

The Federal Communications Commission (FCC)
www.fcc.gov

Laws and regulations

Please note that following references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy regulatory authorities or any relevant public administrations.

- **Gramm-Leach-Bliley Act (GLBA)**
  [http://www.ftc.gov/privacy/privacyinitiatives/glbact.html](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html)
  This act applies to the collection and disclosure of customers' personal financial information by financial institutions and companies that receive such information.

- **The Fair Credit Reporting Act (FCRA)**
  [http://www.ftc.gov/privacy/privacyinitiatives/credit.html](http://www.ftc.gov/privacy/privacyinitiatives/credit.html)
  This act promotes accuracy in consumer reports and is meant to ensure the privacy of the information in them.

  It has been amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

- **Fair and Accurate Credit Transactions Act of 2003 (FACTA)**
  This act amends the Fair Credit Reporting Act to improve the accuracy of consumer records, improve resolution of consumer disputes, make improvements in the use of credit information, and improve consumer access to credit information.

  It also aims to prevent identity theft.

- **The Children's Online Privacy Protection Act (COPPA)**
  [http://www.ftc.gov/privacy/privacyinitiatives/childrens.html](http://www.ftc.gov/privacy/privacyinitiatives/childrens.html)
This act gives parents control over what information is collected from their children online and how the information may be used.

It applies to children under the age of 13.

- The Federal Trade Commission Act (FTC Act)  
  http://www.ftc.gov/ogc/ftcact.shtm
  This act gives the FTC the power to prevent unfair competition and unfair or deceptive acts in commerce.

- The Driver’s Privacy Protection Act of 1994 (DPPA)  
  http://epic.org/privacy/drivers/  
  This act restricts the disclosure of personal information associated with motor vehicle records.

- Health Insurance Portability and Accountability Act (HIPAA)  
  http://www.hhs.gov/ocr/privacy/index.html  
  This act applies to health plans, health care clearinghouses, health care providers, and business associates of covered entities.

  It includes privacy provisions that give consumers rights over their health information and sets rules and limits on who can look at and receive health information.

- Communications Act of 1934  
  This act has been defined for the regulation of interstate and foreign communication by wire or radio.

  It has been amended by the Cable Communications Policy Act of 1984 (CCPA) and the Telecommunications Act of 1996.

- Cable Communications Policy Act of 1984 (CCPA)  
  http://privacy.med.miami.edu/glossary/xd_ccpa.htm

- Telecommunications Act of 1996  
  http://www.fcc.gov/telecom.html

- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)  
  http://www.ftc.gov/bcp/edu/microsites/spam/rules.htm  
  http://www.fcc.gov/cgb/consumerfacts/canspam.html
This act requires the Federal Trade Commission (FTC) to adopt detailed rules restricting the sending of unwanted commercial e-mail messages to computers.

It requires the Federal Communications Commission (FCC) to adopt rules that prohibit sending unwanted commercial e-mail messages to wireless devices without prior permission.

- The Telephone Consumer Protection Act (TCPA)
  This act regulates telemarketing and establishes a national Do-Not-Call list.

- The Telecommunications Act of 1996
  This act applies to telephone carriers’ use of “customer proprietary network information”.

- Electronic Communications Privacy Act (ECPA)
  This act protects wire, oral, and electronic communications while in transit. It defines requirements for search warrants.

- Family Educational and Privacy Rights Act (FERPA)
  This act protects the privacy of student education records. It applies to all schools that receive funds under a program of the U.S. Department of Education.

- Computer Fraud and Abuse Act (CFAA)
  [http://www.law.cornell.edu/uscode/18/1030.html](http://www.law.cornell.edu/uscode/18/1030.html)
  This act prohibits unauthorized access to protected computers.

- Video Privacy Protection Act (VPPA)
  [http://epic.org/privacy/vppa/](http://epic.org/privacy/vppa/)
  This act prevents disclosure of personally identifiable rental records of prerecorded video cassette tapes or similar audio visual material.
FCC Freedom of Information Act (FOIA)
http://www.fcc.gov/foia/
This act gives the American public greater access to the Federal Government's records.
It has been amended by the Electronic Freedom of Information Act Amendments of 1996.

The Electronic Freedom of Information Act Amendments of 1996
http://www.fcc.gov/foia/
This act expands the scope of the FOIA to encompass electronic records.
It also requires the creation of "electronic reading rooms" to make records more easily and widely available to the public.

Federal Privacy Act of 1974
This act applies to the records of federal government executive and regulatory agencies.

Numerous state security breach notification laws, including California SB 1386
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
This act requires state agencies and business that conduct business in California to disclose any security breach pertaining to the personal data of any resident of California.
6 Standards

6.1 Information security and PII protection

- **ISO/IEC 27018 International Standard**
  ISO/IEC 27018, *Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

- **ISO/IEC 29100 International Standard**
  ISO/IEC 29100, *Information technology - Security techniques - Privacy framework*

- **ISO/IEC 29101 International Standard**
  ISO/IEC 29101, *Information technology - Security techniques - Privacy reference architecture*

- **ISO/IEC 29134 International Standard**
  ISO/IEC 29134, *Information technology -- Privacy impact assessment -- Guidelines*

- **ISO/IEC 29151 International Standard**

- **ISO Guide 73**
  ISO Guide 73, *Risk management - Vocabular*
This standard defines the terms and basic concepts on personal information protection in the information system, clarifies the roles concerned and their functions in the personal information protection, puts forward the basic principles for personal information treatment in the information system, describes the norms and requirements for personal information treatment in the information system. The personal information treatment includes the four links of information collection, processing, transfer and deletion. It is applicable to various organizations and agencies like telecommunication, finance and medical care services.
6.2 Financial services

ISO 22307:2008 International Standard

ISO 22307:2008 International Standard Financial services -- Privacy impact assessment recognizes that a privacy impact assessment (PIA) is an important financial services and banking management tool to be used within an organisation, or by "contracted" third parties, to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems.

ISO 22307:2008 International Standard:
- describes the privacy impact assessment activity in general,
- defines the common and required components of a privacy impact assessment, regardless of business systems affecting financial institutions, and
- provides informative guidance to educate the reader on privacy impact assessments.

A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution's current level of compliance with the law and identifies steps to avoid future non-compliance with the law. While there are similarities between privacy impact assessments and privacy compliance audits in that they use some of the same skills and that they are tools used to avoid breaches of privacy, the primary concern of a compliance audit is simply to meet the requirements of the law, whereas a privacy impact assessment is intended to investigate further in order to identify ways to safeguard privacy optimally.

ISO 22307:2008 International Standard recognizes that the choices of financial and banking system development and risk management procedures are business decisions and, as such, the business decision makers need to be informed in order to be able to make informed decisions for their financial institutions. ISO 22307:2008 International Standard provides a privacy impact assessment structure (common PIA components, definitions and informative annexes) for institutions handling financial information that wish to use a privacy impact assessment as a tool to plan for, and manage, privacy issues within business systems that they consider to be vulnerable.

Author(s): ISO/IEC TC 68/SC 7
Keyword(s): Privacy impact assessment
Resource cost: Commercial
Resource type(s): International Standard
Resource URL(s):
7 Guidelines

7.1 Financial services

- Credit Reporting Code of Conduct

The Code of Conduct supplements Part IIIA of the Privacy Act 1988 on matters of detail not addressed by the Act. Among other things, it requires credit providers and credit reporting agencies to:

- deal promptly with individual requests for access and amendment of personal credit information
- ensure that only permitted and accurate information is included in an individual’s credit information file
- keep adequate records in regard to any disclosure of personal credit information
- adopt specific procedures in settling credit reporting disputes
- provide staff training on the requirements of the Privacy Act.

Part IIIA and the Code of Conduct generally only apply to consumer credit. As such, commercial credit is generally unaffected other than in limited exceptional circumstances. Exceptions include where consumer credit information relating to an individual is disclosed in the context of a commercial credit application.

The Code of Conduct, like Part IIIA of the Act, is legally binding. The Code is accompanied by Explanatory Notes which seek to explain, in a systematic way, how Part IIIA and the Code interact.

**Author(s):** Australia – The Office of the privacy commissioner  
**Keyword(s):** Credit Reporting, Consumer  
**Resource cost:** Free  
**Resource type(s):** Document(s)  
**Resource URL(s):**


- Report on the Review of the Credit Provider Determinations

**Author(s):** Australia – The Office of the privacy commissioner  
**Keyword(s):** Credit Provider  
**Resource cost:** Free  
**Resource type(s):** Document(s)  
**Resource URL(s):**

Code of Practice on Consumer Credit Data

This code of practice has been issued by the Privacy Commissioner for Personal Data in the exercise of the powers conferred on him by PART III of the Personal Data (Privacy) ordinance (Cap. 486) (“the Ordinance”).

The Code is designed to provide practical guidance to data users in Hong Kong in the handling of consumer credit data. It deals with the collection, accuracy, use, security and access and correction issues as they relate to personal data of individuals who are, or have been, applicants to consumer credits. The Code covers, on one hand, credit reference agencies, and on the other hand, credit providers in their dealing with credit reference agencies and debt collection agencies.

Author(s): Office of the privacy commissioner for Personal Data, Hong Kong
Keyword(s): Consumer credit, reference agencies
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Credit Reporting Privacy Code

This code applies specific rules to credit reporters to better ensure the protection of individual privacy. The code addresses the credit information collected, held, used, and disclosed by credit reporters. For credit reporters the code takes the place of the information privacy principles.

Author(s): Office of the Privacy Commissioner, New Zealand
Keyword(s): Privacy, credit reporting
Resource cost: Free
Resource type(s): Document
Resource URL(s):
7.2 Health Sector

Guidelines on Privacy in the Private Health Sector

The guidelines acknowledge that the health service provider’s principal concern is the health care of the patient. The Privacy Act realises individuals’ wishes to have their privacy protected. Therefore, the guidelines aim to assist health service providers to meet their obligations under the National Privacy Principles while providing treatment and care.

Author(s): Australia – The Office of the privacy commissioner
Keyword(s): Health care
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
The Medical and Health Sector: The Data Protection Rules in Practice

The confidentiality of patient records forms part of the ancient Hippocratic oath, and is central to the ethical tradition of medicine and health care. This tradition of confidentiality is in line with the requirements of the Data Protection Acts 1988 & 2003, under which personal data must be obtained for a specified purpose, and must not be disclosed to any third party except in a manner compatible with that purpose.

Author(s): Ireland – Data Protection Commissioner
Keyword(s): Medical, Health
Resource cost: Free
Resource type(s): Web Page(s), Document(s)
Resource URL(s):
  • http://www.dataprotection.ie/viewdoc.asp?DocID=245

Standards for Privacy of Individually Identifiable Health Information

The guideline is an overview that provides answers to general questions regarding the regulation entitled, Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), promulgated by the U.S. Department of Health and Human Services (HHS), and process for modifications to that rule.

Author(s): Office for Civil Rights
Keyword(s): Medical, Health
Resource cost: Free
Resource type(s): Web Page
Resource URL(s):
  • http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm

HHS Fact Sheet on Protecting the Privacy of Patient’s Health Information

Author(s): US Department of Health and Human Services
Keyword(s): Medical, Health
Resource cost: Free
Resource type(s): Web Page
Resource URL(s):
  • http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm
Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs

The Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs are legally binding guidelines for the management of personal information collected from claims on the Medicare Benefits and Pharmaceutical Benefits Programs. They chiefly apply to Medicare Australia and the Department of Health and Ageing but bind all Australian Government agencies in relation to their handling of this data.

In brief, the Guidelines:
- require the separate storage of Medicare Benefits and Pharmaceutical Benefits Programs claims information;
- specify the circumstances in which data from the two programs may be linked;
- require the de-identification of claims information over five years old; and
- specify the circumstances when old information may be re-identified.

Author(s): Australia – The Office of the privacy commissioner
Keyword(s): Health care
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Health Information Privacy Code

The Health Information Privacy Code sets specific rules for agencies in the health sector to better ensure the protection of individual privacy. The code addresses the health information collected, used, held and disclosed by health agencies. For the health sector the code takes the place of the information privacy principles in the Privacy Act. The Code is accompanied by detailed commentary.

Author(s): Office of the Privacy Commissioner, New Zealand
Keyword(s): Privacy, health information
Resource cost: Free
Resource type(s): Document
Resource URL(s):
Office of the Privacy Commissioner (New Zealand) Health Brochure

Provides information for health consumers about their rights under the Health Information Privacy Code.

Author(s): Office of the Privacy Commissioner, New Zealand
Keyword(s): Privacy, health
Resource cost: Free
Resource type(s): Document
Resource URL(s):

Guidelines for Agreements Between Trustees and Information Management Service Providers

Section 18 of the Health Information Protection Act (HIPA) requires that trustees enter into written agreements with information management service providers (IMSP) before providing personal health information to the IMSP. This guideline can be used by trustees and ISMPSs to review existing agreements or to draft new agreements.

Author(s): Saskatchewan
Keyword(s): Health, Trustees, Service Providers
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010)

Author(s): Council of Europe
Keyword(s): Personal data processing, profiling
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  - https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383
7.3 Human Resources

- **Code of Practice on Human Resource Management**

The Code is designed to give practical guidance to data users who handle personal data in performing human resource management functions and activities. It deals with the collection, accuracy, use, security, access and correction in relation to the personal data of prospective, current and former employees.

The provisions of the code apply to data users who are employers of individuals relating to their prospective, current or former employment with the employers concerned.

**Author(s):** Office of the privacy commissioner for Personal Data, Hong Kong  
**Keyword(s):** Human Resources Management, Prospective, Employees, Employers  
**Resource cost:** Free  
**Resource type(s):** Document(s)  
**Resource URL(s):**

Code of Practice on Human Resource Management: Compliance Guide for Employers and HRM Practitioners

The Code of Practice on Human Resource Management ("the Code") came into effect on 1st April 2001. It provides employers and HRM practitioners with a practical guide to the application of the provisions of the Personal Data (Privacy) Ordinance ("the PD(P)O") to employment-related personal data privacy.

The Code draws on the Data Protection Principles ("DPPs") that appear in Schedule 1 of the PD(P)O and applies them to the management of personal data in three important areas: recruitment, current employment, and former employees' matters. The Code also illustrates good personal data practices applied to HRM activities.

Author(s): Office of the privacy commissioner for Personal Data, Hong Kong
Keyword(s): Human Resources Management, Employees, HRM Practitioners
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Guidelines for personal data protection in employment relationships

The guidelines provide answers to frequently asked questions of employees and employers regarding the provisions of the Personal Data Protection Act and at the same time harmonize the requirements and practices of the inspection supervision.

Author(s): Information Commissioner of Slovenia
Keyword(s): Employment relationships, personal data
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010)

Author(s): Council of Europe
Keyword(s): Personal data processing, profiling
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989)

Author(s): Council of Europe
Keyword(s): Personal data protection, employment
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  o https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Recommendation No.R(86) 1 on the protection of personal data for social security purposes (23 January 1986)

Author(s): Council of Europe
Keyword(s): Personal data protection, social security
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  o https://wcd.coe.int/ViewDoc.jsp?id=699153&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

7.4 Marketing

Data Protection Good Practice Note - Charities and marketing

This guidance explains what charities and voluntary organisations need to do to comply with the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 when carrying out their marketing activities.

Author(s): Information Commissioner’s Office
Keyword(s): Charities and marketing
Resource cost: Free
Resource type(s): Web Page(s)
Resource URL(s):
New Tool Will Help Online Advertisers Develop Stronger Privacy Practices

The Center for Democracy and Technology released a new assessment tool to help online advertising companies develop strong, appropriate privacy protections for the users they serve. Released to coincide with Data Privacy Day 2009, the "Threshold Analysis for Online Advertising Practices," is the result of extensive consultation among CDT, Internet companies and public interest advocates. It notes a series of simple tests companies can use to determine whether online advertising activities may trigger the need for additional privacy protections. The document also provides suggestions on how companies can begin putting those protections in place.

Author(s): Center for Democracy and Technology
Keyword(s): Privacy protection, Advertising companies, Assessment tool
Resource cost: Free
Resource type(s): Document(s) / Tool(s)
Resource URL(s):

Guidelines for the Private Sector - Code of conduct for personal data processing

These guidelines provide answers to frequently asked questions by the providers of goods and services on how to deal with consumers' personal data. By examples of good and bad practice, the guidelines explain how personal data should be treated and processed in a lawful manner, and suggest recommendations for formulating the information notice on personal data processing (privacy policy).

Author(s): Information Commissioner of Slovenia
Keyword(s): Providers of goods and services, marketers, personal data, consent, business practice, marketing, notice on personal data processing, proportionality
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010)

Author(s): Council of Europe
Keyword(s): Personal data processing, profiling
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
- https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997)

Author(s): Council of Europe
Keyword(s): Personal data processing, statistics
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
- https://wcd.coe.int/ViewDoc.jsp?id=589341&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Recommendation No.R(85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985)

Author(s): Council of Europe
Keyword(s): Personal data protection, direct marketing
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
- https://wcd.coe.int/ViewDoc.jsp?id=698775&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383
7.5 Industry non-specific - Privacy policy establishment

- **Data protection and privacy guidelines**

  The purpose of these data protection and privacy guidelines is to alert the management of Group companies to the importance of data protection and privacy, the need to have a policy in place to cover privacy and data protection. These guidelines aim to serve as a checklist of issues to consider when drawing up such a policy.

  **Author(s):** BBA Group  
  **Keyword(s):** Privacy issues, Companies  
  **Resource cost:** Free  
  **Resource type(s):** Document(s)  
  **Resource URL(s):**  

- **Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services**

  **Author(s):** Council of Europe  
  **Keyword(s):** Human rights, social networks  
  **Resource cost:** Free  
  **Resource type(s):** Document(s)  
  **Resource URL(s):**  

- **Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines**

  **Author(s):** Council of Europe  
  **Keyword(s):** Human rights, search engines  
  **Resource cost:** Free  
  **Resource type(s):** Document(s)  
  **Resource URL(s):**  
Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999)

Author(s): Council of Europe
Keyword(s): Privacy protection, Internet
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  - https://wcd.coe.int/ViewDoc.jsp?id=407311&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Report of the Group of Experts on Privacy

A comprehensive privacy law is under development in India. To help lay down the framework for developing the law, an expert group on privacy was setup by Planning Commission, Govt. of India, under chairmanship of Justice A. P. Shah, retired Chief Justice of High Court of India, to come up with a framework that can be considered for developing a privacy law in India. The group consists of members from the government, industry, civil society, academia and media community. The framework takes into account privacy concerns and challenges, while drawing best practices from global privacy principles and practices, and proposes a multi-dimensional framework to formulate the law. It also recommends a horizontal privacy law applicable to government and private sector, recommends national privacy principles and an enforcement regime based on co-regulation model.

Author(s): Government of India, Planning Commission
Keyword(s): Indian privacy law, privacy concerns and challenges, privacy best practices, privacy framework
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  - http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf
7.6 Industry non-specific - Trans-border personal data flow

➢ OECD Privacy Framework

The chapter 1 of this document provides an update of the Guidelines governing the Protection of Privacy and Transborder Flows of personal data, and which were originally issued in year 1980. The chapter 2 is the explanatory text of these Guidelines.

Author(s): Organization for Economic Cooperation and Development (OECD)
Keyword(s): Transborder flow, privacy principles
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

➢ The use of authentication across borders in OECD countries

The purpose of this survey was to:
  o Identify examples of current offerings and actual implementation of authentication across borders.
  o Identify actual or potential barriers to the current cross-border use of digital signatures from the supplier/user perspective (taking into account input from other stakeholders as well).
  o Explore the extent to which the cross-border offerings of authentication meet (or do not meet) transaction needs.

While the focus of this survey was on the current cross-border use of authentication methods/methodologies, it was also viewed as a good opportunity to collect information on factors that have been identified as fostering or impeding the national use of authentication technologies and digital signatures. On the basis that such information on national use of authentication would assist in understanding cross-border use, it was also collected.

Author(s): Organization for Economic Cooperation and Development (OECD)
Keyword(s): Cross-border Authentication
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  o http://www.oecd.org/dataoecd/1/10/35809749.pdf
APEC Privacy Framework

The APEC Privacy Framework aims to promote a consistent approach to information privacy protection, avoid the creation of unnecessary barriers to information flows and prevent impediments to trade across APEC member economies. The Framework provides technical assistance to those APEC economies that have not addressed privacy from a regulatory or policy perspective.

Author(s): Asia Pacific Economic Cooperation APEC
Keyword(s): Information privacy protection, APEC members
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
(also named as Convention 108)

Author(s): Council of Europe
Keyword(s): Personal data processing, transborder flow
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
7.7 Technology

➢ Technology-induced challenges in privacy and data protection in Europe

This report identifies the main technology-induced gaps between data protection regulation and the realities of the developing socio-economic environment. It highlights the potential threats and opportunities presented by state-of-the-art technologies and it suggests priorities for tackling the most pressing gaps. The principles of data protection are robustly formulated in technology-neutral terms, but understanding how these principles can be applied effectively to innovations supporting the Lisbon goal of making the EU “the most competitive and dynamic knowledge-driven economy” is a critical task. If citizens are to retain confidence that their fundamental rights are protected, and that the EU framework is relevant to their daily experience, they must be able to exercise privacy rights in practical and useful ways.

In addition, the report provides a preliminary description of each problem identified, gives a list of its specific characteristics, and offers a set of recommendations. The analysis takes into account the role of relevant public and private sector bodies on a European and Member State level, where applicable.

Author(s): European Network and Information Security Agency (ENISA)
Keyword(s): Technology-induced Gaps, Data Protection Principles, Public Sector, Private Sector
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

➢ Code of Practice on the Identity Card Number and other Personal Identifiers

The Code is designed to give practical guidance to identity card number privacy-related specifications.

Author(s): Office of the privacy commissioner for Personal Data, Hong Kong
Keyword(s): Identity Card Number, Personal Indentifiers
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  o http://www.pcpd.org.hk/english/ordinance/code_id.html
Privacy Features of European eID Card Specifications

The aim of this paper is to allow easy comparison between privacy features offered by European eID card specifications and thereby to facilitate identification of best practice. The target audience is corporate and political decision-makers and the paper seeks to raise awareness of the legal and social implications of new developments in eID card technologies. In particular, the findings should have important implications for data protection and security policies.

The main part of the paper is then dedicated to a survey of how these available privacy enhancing technologies are implemented in existing and planned European eID card specifications, the European Citizen Card and ICAO electronic passport specifications.

The information is based on the latest publicly available specifications with a complete set of references provided and is presented in a series of tables for easy comparison. The table entries show how diverse the European eID card landscape is. Although this paper only compares privacy features, other aspects of the cards are similarly diverse.

Author(s): European Network and Information Security Agency (ENISA)
Keyword(s): Citizen Privacy Protection, eID cards, Electronic Identity Card, ICAO Passport, European Citizen Card
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
  o http://www.enisa.europa.eu/pages/02_01_press_2009_02_3_privacy_features_eID.html

Privacy and Security Risks when Authenticating on the Internet with European eID Cards

The main purpose of this paper is to help define a comprehensive list of requirements for national ID cards in order to ensure that they are as flexible and as multi-purpose as possible.

The main conclusions of the discussion are:
- Electronic identity cards offer secure, reliable electronic authentication to internet services
- A privacy-protecting universally applicable eID card is technologically feasible.

Author(s): European Network and Information Security Agency (ENISA)
Keyword(s): Privacy, risk assessment, electronic identity cards, smart-card chip, PIN
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
Smartphones: Information security risks, opportunities and recommendations for users

The objective of this report is to allow an informed assessment of the information security and privacy risks of using smartphones. This report analyses 10 information security risks for smartphone users and 7 information security opportunities. It makes 20 recommendations to address the risks.

Author(s): European Network and Information Security Agency (ENISA)
Keyword(s): Privacy, risk assessment, smartphones
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Guidelines - Cloud computing and data protection

The purpose of the document is to establish common control points, by which users as well as supervisory authorities will be able to come to informed decisions regarding the use and oversight of the cloud computing services in part where processing of personal data is concerned.

The initiatives for safer use and certifications of cloud services on the other hand are offered guidelines for future development with the goal of compliance with personal data protection legislation.

Author(s): Information Commissioner of Slovenia
Keyword(s): Cloud computing, personal data protection, security, privacy, transfer of data to third countries, contractual data processing, risk assessment, information security.
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
Guidelines - Guidelines for developing information solutions

These guidelines address the most important requirements to be followed in the development of information solutions encompassing personal data processing. The guidelines are intended for all those involved in the development of solutions in the field of information and communications technologies or the commissioning of such, irrespective of whether new products, services, and systems, or individual solutions and applications are at issue.

Author(s): Information Commissioner of Slovenia
Keyword(s): Information system, application, personal data protection, traceability, proportionality, privacy by design.
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

7.8 Video surveillance

CCTV Code of practice

This is a code of practice issued by the Data Protection Commissioner in accordance with her powers under Section 51 (3)(b) of the Data Protection Act 1998 (the "1998 Act"). It is intended to provide guidance as to good practice for users of CCTV (closed circuit television) and similar surveillance equipment.

Author(s): Information Commissioner’s Office
Keyword(s): CCTV, Surveillance
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

Guidelines for Using Video Surveillance Cameras in Public Places

These Guidelines are intended to assist institutions in deciding whether the collection of personal information by means of a video surveillance system is lawful and justifiable as a policy choice, and if so, how privacy protective measures can be built into the system.

Author(s): Information and Privacy Commissioner Ontario
Keyword(s): CCTV, Surveillance, Public Places
Guidelines for Using Video Surveillance Cameras in Schools

These Guidelines recognize that modified expectations of privacy exist in schools. In contrast to public places, schools are considered to be a supervised environment where a reasonable degree of monitoring by school staff is both desirable and expected. A comprehensive surveillance system in a school, however, has the potential of being privacy-invasive. These Guidelines were created to assist school boards intending to use video surveillance to introduce these programs in a manner that ensures stringent privacy controls.

Author(s): Information and Privacy Commissioner Ontario
Keyword(s): CCTV, Surveillance, Schools
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
- http://www.ipc.on.ca/images/Resources/video-e.pdf

Public Surveillance System Privacy Guidelines

These guidelines are designed to assist public bodies in deciding whether collection of personal information by means of a video, audio or other mechanical or electronic surveillance system is both lawful and justifiable as a policy choice and, if so, how privacy protection measures should be built into the system. The Office of the Information and Privacy Commissioner (“OIPC”) strongly encourages all public bodies that use, or are considering the use of, surveillance systems to comply with these guidelines.

Author(s): Office of the Information and Privacy Commissioner for British Columbia
Keyword(s): CCTV, Surveillance, Public
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):
Guidelines on Video Surveillance

The guidelines provide assistance to those who already perform video surveillance and have questions regarding compliance with the law. They provide an overview of legal requirements, best practice examples, information on supervision and sanctions and provide answers to frequently asked questions.

Author(s): Information Commissioner of Slovenia
Keyword(s): Video surveillance
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

7.9 Public privacy awareness

OnGuard Online

Provides practical tips from the US federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Author(s): Federal Trade Commission
Keyword(s): Internet fraud prevention, FTC
Resource cost: Free
Resource type(s): Document(s) / Video(s) / Tool(s)
Resource URL(s):
  - http://www.onguardonline.gov/

Privacy Today

The purpose of the presentation is to highlight and summarize key privacy issues affecting consumers today and tomorrow. Presentation written by: Professor Peter P. Swire Ohio State University Center for American Progress www.peterswire.net On behalf of the International Association of Privacy.

Author(s): International association of privacy professionals / Intel
Keyword(s): Privacy issues, Consumers, Data Privacy Day
Resource cost: Free
Secure your computer to protect your privacy

The presentation on securing home computers was developed by the California Office of Privacy Protection for use by community organisations and businesses to train individuals on securing their home computers.

Author(s): California Office of Privacy Protection
Keyword(s): Privacy training, Individual
Resource cost: Free
Resource type(s): Document(s)
Resource URL(s):

- [http://www.privacyrights.org/ar/Privacy-IssuesList.htm](http://www.privacyrights.org/ar/Privacy-IssuesList.htm)

Privacy Breach Guidelines (New Zealand)

Provides guidance from the New Zealand Privacy Commissioner about steps agencies should take when a privacy breach occurs. The guidelines are voluntary.

Author(s): Office of the Privacy Commissioner, New Zealand
Keyword(s): Privacy breach, data breach
Resource cost: Free
Resource type(s): Document
Resource URL(s):

ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

- Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995)

  Author(s): Council of Europe
  Keyword(s): Personal data protection, telephone services
  Resource cost: Free
  Resource type(s): Document(s)
  Resource URL(s):
    - https://wcd.coe.int/ViewDoc.jsp?id=529167&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Teen privacy online

  Over 55 percent of online American teens between 12 and 17 use social networks, and older teens are even more likely to have profiles. The vast majority of American teens use the Internet. Choose a prepared presentation or group of materials and use them to help educate teens about how to protect the privacy of their personal information online. Alternatively, search the useful links and resources below to find a video or website that speaks to your particular audience. The important thing is to get teens talking and thinking critically about privacy. As innovative and creative users of technology, teens can be the first and best protectors of their privacy online.

  Author(s): International association of privacy professionals / Intel
  Keyword(s): Privacy online, Data Privacy Day
  Resource cost: Free
  Resource type(s): Document(s)
  Resource URL(s):
    - http://issuu.com/mdwcollins/docs/teenprivacyonline_slides

- Guidelines - Being an informed consumer – who is allowed to handle my personal data and why?

  These guidelines provide answers to frequently asked questions by the consumers on how to protect their personal data when engaging in business or other activities over the Internet, mobile marketing, participating in prize winning games, answering questionnaires on preferences, joining clubs and applying for loyalty cards.

  Author(s): Information Commissioner of Slovenia
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

**Keyword(s):** Personal data, consumers, internet, online shopping, mobile marketing, prize winning games, clubs and loyalty cards, viral marketing.

**Resource cost:** Free

**Resource type(s):** Document(s)

**Resource URL(s):**
- [https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Informed_consumers_eng_05.02.2012_.pdf](https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Informed_consumers_eng_05.02.2012_.pdf)

- [Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991)](https://wcd.coe.int/ViewDoc.jsp?id=608451&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383)

  **Author(s):** Council of Europe

  **Keyword(s):** Personal data disclosure to third parties, public sector

  **Resource cost:** Free

  **Resource type(s):** Document(s)

- [https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383)

  **Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987)**

  **Author(s):** Council of Europe

  **Keyword(s):** Personal data processing, police

  **Resource cost:** Free

  **Resource type(s):** Document(s)

- [https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383)
7.10 Privacy accreditation

- **US Safe Harbor**

  Bridge between USA and EU privacy approaches and requirements

  Due to the differing regulations between the EU and the US, and EU concerns that data about its residents be properly protected, USA and EU have concluded a legal arrangement mentioned Safe Harbor

  Companies, which would like to be compliant with “Safe Harbor” status, shall follow its principles to provide an adequate security and privacy level, required to process EU personal data without undue risk of improper use or disclosure.

  Safe Harbor is available only to legal entities that are regulated by the FTC or Department of Transportation (DOT), not to financial institutions, as they are regulated by the FTB.

  **Author(s):** Federal Trade Commission (FTC)
  **Keyword(s):** Privacy accreditation
  **Resource cost:** -
  **Resource type(s):** Document(s)
  **Resource URL(s):**

    - [http://www.export.gov/safeharbor](http://www.export.gov/safeharbor)

- **PrivacyMark System**

  The PrivacyMark System which is a system set up to accreditate private organisations that take appropriate measures to protect personal information. Such private organisations are granted the right to display the PrivacyMark in the course of their business activities. The PrivacyMark System is in compliance with Japan Industrial Standards (JIS Q 15001:2006 [Personal Information Protection Management System - Requirements]).

  **Author(s):** JIPDEC (Japan Information Processing Development Corporation, [http://www.jipdec.or.jp/eng/](http://www.jipdec.or.jp/eng/))
  **Keyword(s):** Privacy accreditation
  **Resource cost:** -
  **Resource type(s):** Document(s)
  **Resource URL(s):**

    - [http://privacymark.org/](http://privacymark.org/)
DSCI Privacy Framework (DPF®)

Launched in 2010, DSCI Privacy Framework (DPF®) compiles practices in 9 practice areas that help organizations design, implement, monitor and review a privacy program. DSCI Assessment Framework-Privacy, (DAF-P®) followed in 2012. It essentially translates DPF® practices, and emphasises on what to do, how to assess implementation of privacy policies, processes, procedures and practices within an organization. Based on DPF® and DAF-P®, DSCI launched the DSCI privacy Certification scheme to provide assurance to relevant stakeholders on the robustness of organization’s privacy program. Seven Assessment Organizations (AOs) have been engaged for this initiative until now, which conduct independent third party assessment leading to DSCI certification. DSCI Certified Privacy Lead Assessor (DCPLA®) training and certification program is being operated to train the assessors for conducting privacy assessments.

Author(s): Data Security Council of India (DSCI), A NASSCOM® Initiative
Keyword(s): Privacy accreditation, Privacy Certification, Privacy Assessment, DPF®, DAF-P®, DPC, DCPLA®, AO
Resource cost: Free of charge
Resource type(s): Document(s)
Resource URL(s):
  o http://www.dsci.in

Personal Information Management System (PIMS)

The certification scheme is to ensure if an organization’s personal information management system complies with the Notification No. 17 (2013) of the Korea Communications Commission (http://eng.kcc.go.kr/user/ehpMain.do) and allows KISA (Korea Internet/Security Agency) to grant a certificate to an organization with a certain level of PII protection. It was started in 2011 and grounded on the Act on Promotion of Information and Communication Network Utilization and Information Protection.

Author(s): KISA (Korea Internet/Security Agency), http://www.kisa.or.kr/eng/main.jsp
Keyword(s): Personal information management system accreditation
Resource cost: Free of charge
Resource type(s): Document(s)
Resource URL(s):
  o Notification No. 17 (2013) of the Korea Communications Commission (in Korean)
    http://isms.kisa.or.kr/kor/notice/dataList.jsp?p_No=132&b_No=132/
8 Newsletters and forums

- **Daily Dashboard**
  The Daily Dashboard summarizes the day's top stories with links to the full articles...sent direct to your desktop each weekday

  - **Author(s):** International association of privacy professionals
  - **Keyword(s):** Newsletter, Articles, IAPP
  - **Resource cost:** Free
  - **Resource type(s):** Document(s)
  - **Resource URL(s):**
    - [https://www.privacyassociation.org/publications/daily_dashboard/](https://www.privacyassociation.org/publications/daily_dashboard/)

- **Center for Democracy and Technology**
  This organisation's Web site tracks US consumer privacy legislation within the current congress and has historical information about previous sessions. It also offers subscriptions to a newsletter on civil liberty issues and Web site updates.

  - **Author(s):** Center for Democracy and Technology
  - **Keyword(s):** Newsletter, US consumer privacy legislation, Articles
  - **Resource cost:** Free
  - **Resource type(s):** Document(s)
  - **Resource URL(s):**
    - [http://www.cdt.org](http://www.cdt.org)

- **Privacy Law & Business International Newsletter**
  The PL&B newsletter covers international legislation updates, case studies, and legal analysis in the areas of privacy principles, workplace privacy, marketing, and international data transfers. PL&B's Web site includes pointers to a vast number of privacy commissioners around the world.

  - **Author(s):** Privacy Laws & Business
  - **Keyword(s):** Newsletter, Consulting, Training, Laws, Articles
  - **Resource cost:** Free / Commercial
  - **Resource type(s):** Document(s)
  - **Resource URL(s):**
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

- **E-commerce Law Week by Steptoe and Johnson**
  
  This global law firm publishes a free weekly newsletter that discusses electronic commerce issues and new law developments including privacy.

  *Author(s):* Steptoe & Johnson LLP  
  *Keyword(s):* Newsletter, Laws, Articles  
  *Resource cost:* Free  
  *Resource type(s):* Document(s)  
  *Resource URL(s):*  
  - [http://www.steptoe.com/publications.html](http://www.steptoe.com/publications.html)  
  - [http://www.steptoe.com/publications.html](http://www.steptoe.com/publications.html)

- **Privacy Exchange**

  Resources including a news service and a legal library offering information on national data protection laws, regulations, standards and practices for businesses around the world concerned about handling trans-border communication. Features an exchange forum for international dialogue on consumer services and privacy protection.

  *Author(s):* Center for Social and Legal Research  
  *Keyword(s):* International Standards, Laws, Articles  
  *Resource cost:* Free / Commercial  
  *Resource type(s):* Document(s)  
  *Resource URL(s):*  
  - [http://www.privacyexchange.org/](http://www.privacyexchange.org/)

- **BNA Privacy Law Watch and Privacy and Security Report**

  Produced daily or weekly, these reports provide notification of current events and articles analyzing those events by attorneys and reporters on primarily US issues.

  *Author(s):* BNA  
  *Keyword(s):* Newsletter, Laws, Articles  
  *Resource cost:* Free / Commercial  
  *Resource type(s):* Document(s)  
  *Resource URL(s):*  
Alston & Bird International Privacy Library

Alston & Bird maintains an extensive collection of provisions from governments worldwide on the topic of privacy as well as privacy-related articles and analysis. It also maintains English translations of some foreign laws such as JPIPA.

**Author(s):** Alston & Bird International  
**Keyword(s):** Laws, Articles  
**Resource cost:** Free  
**Resource type(s):** Document(s)  
**Resource URL(s):**  

Tech Law Journal

News, records, and analysis of legislation in USA, litigation, and regulation affecting the computer, internet, communications and information technology sectors.

**Author(s):** Tech Law Journal  
**Keyword(s):** Laws, Articles, Analysis  
**Resource cost:** Free  
**Resource type(s):** Document(s)  
**Resource URL(s):**  
  o [http://www.techlawjournal.com](http://www.techlawjournal.com)

Private Word

A quarterly newsletter which provides information on relevant local privacy issues and also brief casenotes of recent investigations by the Office.

**Author(s):** Office of the Privacy Commissioner, New Zealand  
**Keyword(s):** Privacy  
**Resource cost:** Free  
**Resource type(s):** Document(s)  
**Resource URL(s):**  
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

- **International Journal of Information Security and Privacy**
  
  **Author(s):** Information Resources Management Association  
  **Keyword(s):** Security, privacy  
  **Resource cost:** $595/year  
  **Resource type(s):** Magazine  
  **Resource URL(s):**  
  - [http://www.igi-global.com/journal/international-journal-information-security-privacy/1096](http://www.igi-global.com/journal/international-journal-information-security-privacy/1096)

- **Journal of Privacy and Confidentiality**
  
  **Author(s):** Carnegie Mellon University  
  **Keyword(s):** Confidentiality, privacy  
  **Resource cost:** Free  
  **Resource type(s):** Magazine  
  **Resource URL(s):**  
  - [http://repository.cmu.edu/jpc/](http://repository.cmu.edu/jpc/)
9 Organisations and associations

- Asia Pacific Privacy Authorities
c/o The Australian Privacy Commissioner

  The Statement of Objectives includes common administrative practice e.g. the citation and dissemination of case notes. The webpage includes the APPA member list, APPA Forums, and Privacy Awareness Week.

  - **Deliverables**
    - Case notes
    - APPA Forums
    - Privacy Awareness Week

  - **Website**

- Consumer Data Industry Association
  1090 Vermont Avenue, N.W., Suite 200
  Washington, D.C. 20005
  USA

  Tracks Privacy laws related to consumer data industry such as but not limited to: data screening, check verification, employment verification, housing verification, credit reporting bureaus, and collection agencies.

  - **Deliverables**
    - Legislative tracking
    - White papers and guidance documents

  - **Website**
    - [http://www.cdiaonline.org](http://www.cdiaonline.org)
International Association of Privacy Professionals (IAPP)
170 Cider Hill Road
York, Maine 03909
USA

The mission of the IAPP is to define, promote, and improve the privacy profession globally. Focused on Commercial and Government Privacy Topics. Offers Certification and a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals, and provide education and guidance on opportunities in the field of privacy.

○ **Deliverables**
  - The Privacy Advisor (newsletter)
  - The Daily Dashboard (free daily e-newsletter)
  - The Peppers & Rogers/IAPP (free daily e-newsletter)
  - Certification
  - Conferences

○ **Website**
  - [https://www.privacyassociation.org/](https://www.privacyassociation.org/)

National Association of Data Privacy Officers (NADPO)
Located in the U.K.

NADPO was created in 1993 to formally represent people working in data protection. NADPO is a nonprofit making organisation. Our objectives are to: Promote and share good practice in data protection and related topics. Promote training and education associated with legislation on Data Protection, Freedom of Information and Environmental Information Regulations.

○ **Deliverables**
  - Newsletters
  - Conferences

○ **Website**
  - [https://www.nadpo.co.uk](https://www.nadpo.co.uk)
Ponemon Institute

The RIM Council brings together information management professionals from privacy and data protection disciplines to develop solutions to challenges facing an organisation’s acquisition, use, storage, transfer and disposal of information assets and to define related measures of success.

- **Deliverables**
  - Privacy Trust Studies
  - Emerging Issue Research
  - Benchmark Studies

- **Website**

Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave. NW, Suite 200, Washington, DC 20009
USA

EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues. Its stated goal is to protect privacy, the First Amendment, and constitutional values.

- **Deliverables**
  - Books
  - Newsletters

- **Website**
  - [http://epic.org/](http://epic.org/)

Privacy Rights Clearinghouse (PRC)
3100 - 5th Ave., Suite B
San Diego, CA 92103
USA

The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organisation focused on consumer advocacy.

- **Deliverables**
  - Online resources focused on Consumer Privacy Rights
  - Documented Legislative Inquiries
  - Lists of Consumer Laws
ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2

✓ Articles
✓ Comprehensive Data Breach Tracking

- **Website**

**Center for Democracy and Technology**

According to their website, the Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

- **Deliverables**
  ✓ Policy briefs
  ✓ News
  ✓ Development of standards
  ✓ Public education
  ✓ Research
  ✓ Advocacy
  ✓ International activism

- **Website**
  ✓ [http://cdt.org/](http://cdt.org/)

**Data Security Council of India (DSCI)**

3rd floor, Niryat Bhawan, Rao Tula Ram Marg
New Delhi – 110057
India

DSCI is a not-for-profit organization and focal body on data protection in India, set-up as an independent Self Regulatory Organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same. It has 650+ corporate members across different industry verticals and 1300+ individual members.

- **Deliverables**
  ✓ Development of privacy framework
  ✓ Development of privacy assessment framework
  ✓ Development of privacy assessment ecosystem leading to privacy certification
  ✓ Capacity building in privacy - Advanced and entry level training in privacy
Enable implementation of privacy related legal requirements in organizations (section 43A of the IT (Amendment) Act, 2008)
Increase awareness on privacy among stakeholders
Contribute in the development of international standards on privacy
Work towards development of forward leaning and business friendly yet effective privacy law in India
Educate and influence policy makers
Work towards enhancing cross border data flows

Website
http://www.dsci.in
10 Projects

- **PRIME – Privacy and Identity Management for Europe**

  PRIME aims to develop a working prototype of a privacy-enhancing Identity Management System. To foster market adoption, novel solutions for managing identities will be demonstrated in challenging real-world scenarios, e.g., from Internet Communication, Airline and Airport Passenger Processes, Location-Based Services and Collaborative e-Learning.

  - **Deliverables**
    - PRIME Framework V2
  - **Website**
11 Data retention periods

Personal data should or shall be safely stored for a defined period of time in regards to applicable laws and regulations.

11.1 Belgium

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
</table>
| Accounting documents    | 10 years for the accounting book and documentary evidences from the 1st of January following the fiscal year in progress.  
3 years for documents which have no evidence value | -                                | Article 9 of Royal Decree relative to the execution of annual accounts law Article 6, paragraph 4 of the annual accounts law | Original for the accounting book, and original or copy for others |
| Human resources documents | 5 years  
15 years for staff health files                                                                            | -                                | Article 25 of Royal Decree of 8 August 1980, Article 167 of the “Loi-programme” of 22 December 1989, Article 9 of Royal Decree relative to workers health monitoring of 28 May 2003 and Article 333, paragraph 2, third indent of Royal Decree of 28 November 1969 Article 85 of Royal Decree relative to workers health monitoring of 28 May 2003 | Any, except for health files (Original) |
| Tax documents           | 5 years                                                                                         | -                                | Article 315 of the “Code des Impôts sur le Revenu”.                                   | Original                                             |
11.2 France

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll book</td>
<td>5 years</td>
<td>Social length or 120 years</td>
<td></td>
<td>Reproduction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>starting from concerned</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>employee birth date.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff's registers</td>
<td>5 years</td>
<td>Social length or 120 years</td>
<td></td>
<td>Reproduction</td>
</tr>
<tr>
<td>and profession</td>
<td></td>
<td>starting from concerned</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>employee birth date.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files about</td>
<td>Unlimited</td>
<td>Social length or 120 years</td>
<td></td>
<td>Original</td>
</tr>
<tr>
<td>accidents at work</td>
<td></td>
<td>starting from concerned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or profession</td>
<td></td>
<td>employee birth date.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>illness giving</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>right to</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>compensation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All accounting</td>
<td>5 years</td>
<td>10 years (30 years for</td>
<td></td>
<td>Reproduction</td>
</tr>
<tr>
<td>files related to</td>
<td></td>
<td>documents referring to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>treatment</td>
<td></td>
<td>treatments and salaries before</td>
<td></td>
<td></td>
</tr>
<tr>
<td>and salaries</td>
<td></td>
<td>17 July 1971 and 10 years after)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payrolls</td>
<td>5 years</td>
<td>10 years</td>
<td></td>
<td>Reproduction</td>
</tr>
<tr>
<td>Full statement</td>
<td>5 years</td>
<td>6 years</td>
<td></td>
<td>Reproduction</td>
</tr>
<tr>
<td>receipt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copies of Work</td>
<td>5 years</td>
<td>6 years</td>
<td></td>
<td>Reproduction</td>
</tr>
<tr>
<td>certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copies of social</td>
<td>5 years</td>
<td>6 years</td>
<td></td>
<td>Original</td>
</tr>
<tr>
<td>contribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>payment slip</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social costs books and recaps</td>
<td>5 years</td>
<td>6 years</td>
<td>Original</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>Fiscal files per employee</td>
<td>5 years</td>
<td>10 years (30 years for documents referring to treatments and salaries before 17 July 1971 and 10 years after)</td>
<td>Reproduction</td>
<td></td>
</tr>
</tbody>
</table>
11.3 Korea (Republic of)

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic transaction data</td>
<td>5 years</td>
<td></td>
<td>Electronic Financial Transaction Act</td>
<td></td>
</tr>
<tr>
<td>Health data</td>
<td>5 years for patient lists</td>
<td></td>
<td>Framework Act on Health Care</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 years for electronic medical records</td>
<td></td>
<td>Framework Act on Health Care</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 years for prescriptions</td>
<td></td>
<td>Framework Act on Health Care</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 years for operation records</td>
<td></td>
<td>Framework Act on Health Care</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 years for nurse's records</td>
<td></td>
<td>Framework Act on Health Care</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 years for copy of medical certificates</td>
<td></td>
<td>Framework Act on Health Care</td>
<td></td>
</tr>
<tr>
<td>User data</td>
<td>1 year after last login of user to that website</td>
<td></td>
<td>Act on promotion of information and communications network utilization and information protection, etc.</td>
<td></td>
</tr>
</tbody>
</table>
11.4 Luxembourg

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting documents</td>
<td>10 years</td>
<td></td>
<td></td>
<td>Original / Reproduction</td>
</tr>
<tr>
<td>Pension fund</td>
<td>+ 30 years after (prescription)</td>
<td></td>
<td>Applicable Law- Complimentary Pension Regime 8 June 1999</td>
<td>Original / Reproduction</td>
</tr>
<tr>
<td>Personnel files</td>
<td>3 years if remuneration</td>
<td>Wages and personal documents can also be considered as related to accounting documents. They shall consequently be kept for 10 years</td>
<td>Applicable Law- Civil Code Art. 2277</td>
<td>Original / Reproduction</td>
</tr>
<tr>
<td>Payroll</td>
<td>3 years (see personnel)</td>
<td></td>
<td>Applicable Law- Civil Code Art. 2277</td>
<td>Original / Reproduction</td>
</tr>
<tr>
<td>Physical access control</td>
<td>3 months</td>
<td>3 years if physical access control system used for working hours control</td>
<td>Deliberation 64/2007 from June 22nd 2007</td>
<td>Original / Reproduction</td>
</tr>
<tr>
<td>Video monitoring</td>
<td>1 month</td>
<td>7 days</td>
<td></td>
<td>Original / Reproduction</td>
</tr>
<tr>
<td>Working hours control</td>
<td>3 years</td>
<td></td>
<td></td>
<td>Original / Reproduction</td>
</tr>
</tbody>
</table>
11.5 Netherlands

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial document</td>
<td>No legal period</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Tax document including job contracts</td>
<td>7 years</td>
<td>-</td>
<td>Articles 2:10 and 3:15i of the Civil Code and Article 52 of AWR</td>
<td>-</td>
</tr>
<tr>
<td>Salary administration</td>
<td>2 years</td>
<td>-</td>
<td>Article 8 of the Personal Data Protection Act</td>
<td>-</td>
</tr>
<tr>
<td>Staff administration</td>
<td>2 years</td>
<td>-</td>
<td>Article 7 of the Personal Data Protection Act</td>
<td>-</td>
</tr>
<tr>
<td>Employees income tax form</td>
<td>5 years</td>
<td>-</td>
<td>Article 65 of the law of 2001 related to salary tax</td>
<td>-</td>
</tr>
<tr>
<td>Copies of employees proof of identity</td>
<td>5 years</td>
<td>-</td>
<td>Article 66 of the law of 2001 related to salary tax</td>
<td>-</td>
</tr>
<tr>
<td>Data about applicant</td>
<td>4 weeks without applicant approval, 1 year max with approval</td>
<td>-</td>
<td>Article 5 of the Personal Data Protection Act</td>
<td>-</td>
</tr>
<tr>
<td>Work and rest time records</td>
<td>52 weeks</td>
<td>-</td>
<td>Article 3.2.1 of the Working Hours Decree</td>
<td>-</td>
</tr>
<tr>
<td>Work medical examination about dangerous material</td>
<td>40 years</td>
<td>-</td>
<td>Article 4.10.d of the Working Conditions Decree</td>
<td>-</td>
</tr>
<tr>
<td>Work medical examination about biological agents</td>
<td>10 years</td>
<td>-</td>
<td>Article 4.91 of the Working Conditions Decree</td>
<td>-</td>
</tr>
<tr>
<td>List of employees dealing with task which are dangerous for their safety and health</td>
<td>40 years</td>
<td>-</td>
<td>Article 4.15 jo and article 4.10.d of the Working Conditions Decree</td>
<td>-</td>
</tr>
<tr>
<td>List of employees exposed to asbestos</td>
<td>40 years</td>
<td>-</td>
<td>Article 4.53 jo article 4.10.d of the Working Conditions Decree</td>
<td>-</td>
</tr>
<tr>
<td>Register of employees dealing with categories 3 and 4 biological agent</td>
<td>10 years</td>
<td>-</td>
<td>Article 4.90 of the Working Conditions Decree</td>
<td>-</td>
</tr>
<tr>
<td>Mechanical vibration measure</td>
<td>10 years</td>
<td>-</td>
<td>Article 6.11b of the Working Conditions Decree</td>
<td>-</td>
</tr>
</tbody>
</table>
11.6 Portugal

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

Retention of data in Electronic Communications is regulated by the Law 32/2008.

The general term of mandatory preservation of documents of commercial companies is 10 years, under the terms of the Commercial Code; Special deadlines are established for specific documents and data (e.g. Labor Code).

<table>
<thead>
<tr>
<th>Documents/Records to Retain</th>
<th>Retention Period</th>
<th>Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payments and other documents relating to the provision of services by third parties</td>
<td>5 years - Art. 36.º Decree-Law 17/2009</td>
<td></td>
</tr>
<tr>
<td>Social benefits (e.g., insurance policy and health insurance documents)</td>
<td>10 years - Art. 40.º Comercial code</td>
<td></td>
</tr>
<tr>
<td>Disability records (including registration of workers with disabilities and incapacities resulting from accidents at work and occupational diseases)</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Work Accident and Injury Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(i) Record of occurrences / accidents (without claim of compensation);</td>
<td>5 years - Art. 98.º Law 102/2009</td>
<td></td>
</tr>
<tr>
<td>(ii) History of claims for damages arising from accidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Records (Including individual training materials, plans and records)</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Personal Data of Workers</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Including:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(i) Name, address, date of birth gender, duties performed;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ii) Hours worked, rest days, map of working hours, night work and respective health examinations, supplementary work record;</td>
<td>5 years (Art. 202º, 225º e 231º Labor Code and Art 98º Lei. 102/2009)</td>
<td></td>
</tr>
<tr>
<td>(iii) Reason for termination;</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>(iv) Other clearances and registration of payments.</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Individual files:</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Documents/Records to Retain</td>
<td>Retention Period</td>
<td>Observations</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>(i) Requirements, contracts, additions;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ii) Absence documentation;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(iii) Disciplinary records;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(iv) Performance evaluations and tests / internships;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documents relating to other HR material</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>(Promotions, retrogradations, transfers, layoffs, bonuses, salary adjustments)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal procedures and regulations</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Foreigners (includes documentation regarding residence permit and visas)</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Documents related to international detachments</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Recruitment and selection records (includes announcements, applications received, interview notes, tests)</td>
<td>5 years (Art. 32.º Labor Code)</td>
<td>Workers can claim credits up to 1 year after termination of the contract.</td>
</tr>
<tr>
<td>Unique Social Map</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Social Security Documentation (including forms, payments, receipts and unemployment benefit)</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Disciplinary Inquiries (includes audits)</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Health and Safety Records</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>Wage processing records (includes deductions, compensation, bonus, expenses and attendance records)</td>
<td>10 years</td>
<td>Workers can claim credits up to 1 year after termination of the contract.</td>
</tr>
<tr>
<td>Data base</td>
<td>Until the date of authorization to hold the database, if applicable, or 10 years, otherwise</td>
<td></td>
</tr>
<tr>
<td>Registration of legal actions in labor matters</td>
<td>10 years</td>
<td></td>
</tr>
</tbody>
</table>
11.7 Slovenia

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic communications data</td>
<td>14 months (telephone related data)</td>
<td></td>
<td>Act on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 months (internet access, e-mail and VoIP related data)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health documentation</td>
<td>10 years after death (health records), 15 years after death (other medical documentation), dental records (permanently)</td>
<td></td>
<td>Health Care and Health Insurance Act</td>
<td></td>
</tr>
<tr>
<td>Social transfers</td>
<td>5 year after end of entitlement</td>
<td></td>
<td>Act on Entitlements from Public Funds</td>
<td></td>
</tr>
<tr>
<td>Tax documentation – natural persons</td>
<td>5 years</td>
<td></td>
<td>Act on Taxation Procedure</td>
<td></td>
</tr>
<tr>
<td>Video surveillance</td>
<td>Maximum 1 year (not mandatory)</td>
<td></td>
<td>Personal Data Protection Act</td>
<td></td>
</tr>
</tbody>
</table>
11.8 Switzerland

Please note that following data retention information, references to laws and regulations shall not be considered as exhaustive or even accurate. For further information on laws and regulations applicable within this country in regards to data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

<table>
<thead>
<tr>
<th>Type of documents</th>
<th>Mandatory retention period(s)</th>
<th>Recommended period(s) (optional)</th>
<th>Legislative reference</th>
<th>Type (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting document</td>
<td>10 years from the end of the fiscal year</td>
<td>-</td>
<td>Articles from the 32\textsuperscript{nd} title of the « Code des Obligations »</td>
<td>Original or electronic</td>
</tr>
<tr>
<td>Commercial document</td>
<td>No legal period</td>
<td>30 years</td>
<td>-</td>
<td>Original</td>
</tr>
<tr>
<td>Tax document</td>
<td>10 years from the end of the fiscal year</td>
<td></td>
<td>Articles from the 32\textsuperscript{nd} title of the « Code des Obligations »</td>
<td>Original</td>
</tr>
<tr>
<td>Human resources document</td>
<td>40 years for staff health files</td>
<td>10 years after the end of working relationship, then sent to federal archives for 40 years. If the company cannot send files to federal Archives, document should be withheld 80 years</td>
<td>Article 16 of the « Ordonnance concernant la tenue et la conservation des livres de comptes » (Olico)</td>
<td>Original</td>
</tr>
</tbody>
</table>