ISO/IEC JTC 1/SC 27/WG 5 "Identity management and privacy technologies"
Convenorship: **DIN**
Convenor: **Rannenberg Kai Mr Prof. Dr.**

ISO/IEC JTC 1/SC27/WG5 N2877 WG5 SD 2 Draft

Document type	Related content	Document date	Expected action
Ballot / Reference document	Ballot: N 2979 - ISO/IEC JTC 1/SC27/WG5 N2877 WG5 SD 2 Draft (restricted access)	2021-11-16	**COMMENT/REPLY** by 2021-12-31

Reference number of working document: **ISO/IEC JTC 1/SC 27 WG 5 NXXXX**

Date: 2021-10-18

Reference number of document: **ISO/IEC WG 5 SD2 DRAFT**

Committee identification: ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

WG 5 Standing Document 2 – Privacy References List

Document type: International standard
Document subtype: -
Document stage: (20) Preparation
Document language: E

CONTENTS

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.

WG5 Standing Document 2 — Privacy References List

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

Privacy officer

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

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

If the preference is to use privacy officer, then the terms can be inverted in the entry and changed in the note to entry.

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.

4 Symbols and Abbreviated Terms

APEC	Asia Pacific Economic Co-operation
APPA	Asia Pacific Privacy Authorities
DPA	Data Protection Act
EPIC	Electronic Privacy Information Center
IAPP	International Association of Privacy Professionals
JPIPA	Japan enacted the Personal Information Protection Act
NADPO	National Association of Data Privacy Officers
PII	Personally Identifiable Information
PRIME	Privacy and Identity Management for Europe

5 Law and regulation

5.1 National and regional laws and regulations

5.1.1 Argentina

Data privacy commissioner

Protección de Datos Personales
https://www.argentina.gob.ar/aaip/datospersonales

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Argentina's Personal Data Protection Act of 2000
  http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=64790

  Full text of law: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

  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
  http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm

5.1.2 Australia

Data privacy commissioner

Office of the Privacy Commissioner
http://www.privacy.gov.au/

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 and regarding 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.

5.1.3 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- ➢ Amended Data Protection Law
  http://www.privacycommission.be/fr/static/pdf/wetgeving/loi_vie_privee.pdf
  http://www.law.kuleuven.be/icri/publications/
  499Consolidated_Belgian_Privacylaw_v200310.pdf (English translation)

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

5.1.4 Brazil

Data privacy commissioner

National Data Protection Authority – ANPD
https://www.gov.br/anpd/pt-br

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Brazil's Civil Law of the Internet, Law # 12.695, of April 2,3 of 2014.
  Full text of law: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm

  This law establishes principles, guarantees, rights and duties for the use of the Internet in Brazil and, among other aspects, this law considers that access to the Internet is essential to the exercise of citizenship, and establishes the rights guaranteed to the user, many of them relating to privacy and protection of personal data.

- Brazil's General Personal Data Protection Law (LGPD), Law # 13.709, of August 14, 2018.
  Full text of law: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

  This law specifies when the processing of personal data may occur and its hypotheses (legal bases). It also establishes the rights of the personal data principals and the duties of those involved in the processing of these data.
  Technical and administrative security measures capable of protecting personal data are considered in Article 46.
  It establishes the National Data Protection Authority and defines the administrative sanctions due to non-compliance by data processing agents

- Brazil's National Data Protection Authority – Guide for definitions of personal data processing agents and commissioner (DPO)
  Full text o Guide: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf

"This guide seeks to establish guidelines that are not binding on treatment agents and explain who can exercise the role of controller, operator and supervisor; the legal definitions; the respective liability regimes; concrete cases that exemplify ANPD's explanations and frequently asked questions on the subject." § 3.

5.1.5 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Privacy Act (R.S., 1985, c. P-21)
  http://laws.justice.gc.ca/en/P-21/index.html

  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)
  http://laws.justice.gc.ca/en/P-8.6/258031.html

  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;
- ✓ expect the personal information an organization holds about them to be accurate, complete and up-to-date;
- ✓ 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.

5.1.6 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.

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Assessment Measure of Personal Information Export Security (Draft for Comments)
  http://www.cac.gov.cn/2019-06/13/c_1124613618.htm

- Regulation on Network Protection of Children's Personal Information, promulgated on 23 August 2019, has come into effect as of 1 October 2019.
  http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

- The Cyber Security Law of the People's Republic of China, promulgated on 7 November 2016, has come into effect as of 1 June 2017.
  http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

- Provisions on Protection of Personal Information of Telecommunications and Internet Users, promulgated on 16 July 2013, has come into effect as of 1 September 2013.
  http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c4700145/content.html

- Civil Code of the People's Republic of China (promulgated on 28 May 2020, effective on 1 January 2021)
  http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591bd07917e1d25cc8.shtml

5.1.7 Europe

European Data Protection Board

Tasks and duties

The EDPB was set up to achieve the following tasks and duties:

- To provide **general guidance** to clarify the European data protection laws;
- To **advise** the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union;
- To adopt **consistency findings** in cross-border data protection cases;
- To promote **cooperation** and the effective exchange of information and best practice between national supervisory authorities. If needed, the EDPB is empowered by the GDPR to make binding decisions towards national supervisory authorities to ensure a consistent application; and
- To **issue guidelines, recommendations and best practices** on the use and the application of the GDPR.

The EDPB has been established by the EU General Data Protection Regulation (GDPR), adopted on 27 April 2016 and published in the EU Official Journal on 4 May 2016.
https://edpb.europa.eu/"

European regulations

- EU General Data Protection Regulation (GDPR)
  https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504
  This regulation 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 or a processor is established within the EU, but whenever also to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services (irrespective of whether a payment of the data subject is required) or where it is related to the monitoring of their behavior as far as their behavior takes place within the Union. Finally, it also applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

European directives

- Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
  EUR-Lex - 32016L0680 - EN - EUR-Lex (europa.eu)

  The Police Directive was adopted in order to set the rules on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes. It ensures that police forces can efficiently do their work using technological means while preserving the fundamental rights of citizens. The Directive is designed to be consistent with the General Data Protection Regulation.

- Directive 2002/58/EC on privacy and electronic communications
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

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).
  http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=consil:ST_5419_2016_INIT

Convention 108 from the Council of Europe

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

  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

5.1.8 France

Data privacy commissioner

Commission Nationale de l'Informatique et des Libertés
http://www.cnil.fr/

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

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

  The principles that are addressed in it are the following:

  - ✓ respect of the formalities and the procedure:
    any processing of personal data, even in negligence, without respecting the procedure laid down by either French law or the GDPR, is punished by 5 years imprisonment and a 300 000 € fine. (Articles 226-16, 226-16-1, 226-17 and 226-17-1 of the Penal Code)

  - ✓ 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.

- ➢ Décret n° 2019-536 (published in May, 29th 2019) for the application of Loi Informatique et Liberté (Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties)
  https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038528420?r=tOwdeEKG2b

5.1.9 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) – Published September 1st 2009
  http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG_idFv01092009.pdf

  The BDSG implements the European Directive 95/46/EC and transfers it into a national law.

- Telecommunications Act (Telekommunikationsgesetz - TKG) – Published December 25th 2008
  http://www.bfdi.bund.de/cae/servlet/contentblob/411286/publicationFile/25386/TelecommunicationsAct-TKG.pdf

  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:
  - ✓ directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33);
  - ✓ directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108 page 21);
  - ✓ directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108 page 7);
  - ✓ directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51); and
  - ✓ directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 108 page 37).

  Privacy aspects are covered in the following clauses:
  - ✓ chapter 2 - Access Regulation - § 17 - Confidentiality of Information
    - ✓ PART 3 - CUSTOMER PROTECTION
      - o 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
      - o 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

➢ Telemedia Act (Telemediengesetz - TMG) – Published February 26th 2007
http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf

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).

5.1.10 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 and regarding 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)
http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf

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).

5.1.11 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 and regarding 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

  - ✓ 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.

5.1.12 Indonesia

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Regulation on personal data protection in electronic system, related to privacy protection.
  https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016

5.1.13 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Data Protection Act of 1988
  http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html

  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
  http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html

  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

5.1.14 Israel

Data privacy commissioner

The Privacy Protection Authority (Previously ILITA)
https://www.gov.il/en/Departments/the_privacy_protection_authority

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Basic Law: Human Dignity and Liberty of 1992
  http://www.knesset.gov.il/laws/speciaL/eng/basic3_eng.htm

- Protection of Privacy Law, 5741-1981
  https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf

- Privacy Protection (Data Security) Regulations, 5777 – 2017
  https://www.gov.il/en/Departments/legalInfo/data_security_regulation

- Protection of Privacy Regulations (Transfer of Data Abroad)
  https://www.gov.il/BlobFolder/legalinfo/legislation/en/PrivacyProtectionTransferofDataabroadRegulationsun.pdf

- Privacy Protection Regulations (Terms of Holding Data and iIts Maintenance and Procedures for Transfer of Data between Public Entities), 5746 – 1986

The provided laws and regulations include main privacy protection principals such as consent and notice requirements, purpose limitation, right of access and rectification, direct marketing, data security obligations, trans border data transfers, data breach notification obligation and more.

There are also numerous laws on various sector specific matters, such as Taxation, Genetics, Biometrics, Financial Data and more that include specific provisions and mechanisms to enhance data protection.

Furthermore, Israel has a regulatory authority (the PPA) empowered to enforce the law, in both criminal investigations and administrative inspections, accompanied by computer investigations and forensics. The authority also conducts audits and publishes binding guidelines and best practices.

For an English summary of the PPA guidelines please click on the link down below:

https://www.gov.il/en/Departments/General/guidelines_ppa

Sanctions may include monitory fines, orders to perform mitigation measures and report on them, and orders to cease from data processing.

Adequacy Decision:

The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection.

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

On January 31st, 2011, the European Union Commission published its decision according to which Israel maintains an adequate protection of personal data with regard to automated processing of personal data. For the decision, please click on the link down below:

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415701992276&uri=CELEX:32011D0061

5.1.15 Japan

Data privacy commissioner

Personal Information Protection Commission
https://www.ppc.go.jp/en/.

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Act on the Protection of Personal Information
  https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

- Cabinet Order
  https://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf

- Commission Rules
  https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

- 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_dt03.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_syohi/m_mail.html (Japanese only)

  This act relates on anti-spam mail.

- Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of May 30, 2003)
  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
  https://www.tele.soumu.go.jp/horei/reiki_honbun/72001000001.html
  (Japanese only)
  http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=04&id=3205

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

- Telecommunications Business Act (Act No. 86 of December 25, 1984 – updated on June 24, 2011 under Act No. 74)
  https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=359AC0000000086
  (Japanese only)
  http://www.japaneselawtranslation.go.jp/law/detail/?id=2859&vm=&re=02

  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=□□&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 compenesation 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.”

- 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)
  https://www.cao.go.jp/bangouseido/pdf/en3.pdf
  (English)

- Act Regarding Anonymized Medical Data to Contribute to R&D in the Medical Field
  https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=429AC0000000028 (Japanese only)

- Act on the Protection of Personal Information Held by Incorporated Administrative Agencies
  https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000058
  (Japanese only)

  http://www.cas.go.jp/jp/seisaku/hourei/data/APPIHAO.pdf

Guidelines

- Guidelines for the online notice and consent from consumers

- Guidelines for the Act on the Protection of Personal Information (Volume on General Rules)
  https://www.ppc.go.jp/files/pdf/guidelines01.pdf
  (Japanese only)

  These Guidelines stipulate a specific guidance under Article 4, Article 8 and Article 60 of the Act on the Protection of Personal Information (Act No.57, 2003, hereinafter referred to as the “Act”), for the purpose of supporting activities carried out by business operators regarding securing proper handling of personal information and for the purpose of appropriate and effective implementation of measures to be taken by business operators through the said support.

- Guidelines for the Act on the Protection of Personal Information (Volume on Provision to a Third Party in a Foreign Country)
  https://www.ppc.go.jp/files/pdf/guidelines02.pdf
  (Japanese only)

- Guidelines on the Act on the Protection of Personal Information (Volume on confirmation and record-keeping obligation at the time of third party provision)
  https://www.ppc.go.jp/files/pdf/guidelines03.pdf
  (Japanese only)

- Guidelines for the Act on the Protection of Personal Information (Volume on Anonymously Processed Information)

https://www.ppc.go.jp/files/pdf/guidelines04.pdf
(Japanese only)

5.1.16 Korea (Republic of)

Data privacy commissioner

The Korean Government Personal Information Protection Commission
http://www.pipc.go.kr/cmt/main/english.do

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Information Protection Act for public organizations – Promulgated on January 7th, 1994, Effective on January 8th, 1995 until March 2011. It was incorporated into the law on Personal Information Protection Act in March 29th, 2011 below.

- Personal Information Protection Act ("PIPA") – Promulgated on March 29th, 2011, Effective on September 30th, 2011 and recently revised on Feb 4, 2020.
  http://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95&x=0&y=0#liBgcolor17
  (provided by national lay information centre in Korea Government)

  http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf (provided by the Korean Law via the Internet - http://koreanlii.or.kr/)

  The purpose of this Act is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information.

  On January 09th, 2020, the Korean National Assembly passed amendments (collectively, the 'Amendments') to three major data privacy laws: the Personal Information Protection Act ("PIPA"), the Act on the Promotion of Information and Communications Network Utilization and Information Protection ("Network Act") and the Act on the Use and Protection of Credit Information ("Credit Information Act").

  The adoped amendments largely aim to:

  - Minimize the burden of redundant regulatory activities and avoid confusion among regulated persons stemming from previously overlapping data privacy regulations and multiple supervisory bodies; and

  - Introduce the concept of 'pseudonymized data' and a legal basis upon which data may be utilized more flexibly (to an extent reasonably related to the original purpose of collection).

  The key changes to PIPA are the following:

  - Clarified concept of 'personal information': Distinguished concepts of personal information, pseudonymised information and anonymised information (excluded anonymised information from the scope of personal information).

  - Defined permissible scope of pseudonymised information processing:
    - Permitted processing of pseudonymised information for statistical, scientific research, or public interest record-keeping purposes.

- Permitted combination of pseudonymised information of personal data controllers through specialised agencies.

- Imposed restrictions upon pseudonymised data processing.
- Permitted use and release of personal data without obtaining data subjects' consent to an extent reasonably related to the original purpose of data collection.
- Elevated and strengthened the Personal Information Protection Commission's status and powers.
- Added special provisions related to the deleted provisions of the previous Network Act.
- Effective date: six months after promulgation.

.

The content of PIPA is the following:

CHAPTER I GENERAL PROVISIONS
- Article 1 (Purpose)
- Article 2 (Definitions)
- Article 3 (Principles for Protecting Personal Information)
- Article 4 (Rights of Data Subjects)
- Article 5 (Obligations of State, etc.)
- Article 6 (Relationship to other Acts)

CHAPTER II ESTABLISHMENT OF PERSONAL INFORMATION P
- Article 7 (Personal Information Protection Commission)
- Article 7-2 (Composition of the Protection Commission)
- Article 7-3 (Chairperson)
- Article 7-4 (Term of Office of Commissioners)
- Article 7-5 (Status Guarantee for Commissioners)
- Article 7-6 (Prohibition on Dual Office Holding)
- Article 7-7 (Grounds for Disqualification)
- Article 7-8 (Affairs under Jurisdiction of the Protection Commission)
- Article 7-9 (Matters to be Deliberated and Resolved on by the Protection Commission)
- Article 7-10 (Meetings)
- Article 7-11 (Disqualification of, Challenge to, and Refrainment by, Commissioners)
- Article 7-12 (Subcommission)
- Article 7-13 (Secretariat)
- Article 7-14 (Operation)
- Article 8 Deleted.
- Article 8-2 (Assessment of Data Breach Incident Factors)
- Article 9 (Master Plan)
- Article 10 (Implementation Plan)
- Article 11 (Request for Materials, etc.)
- Article 12 (Personal Information Protection Guidelines)
- Article 13 (Promotion and Support of Self-Regulation)
- Article 14 (International Cooperation)

CHAPTER III PROCESSING OF PERSONAL INFORMATION
SECTION 1 Collection, Use, Provision, etc. of Personal information
- Article 15 (Collection and Use of Personal Information)
- Article 16 (Limitation to Collection of Personal Information)
- Article 17 (Provision of Personal Information)
- Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information)
- Article 19 (Limitation to Use and Provision of Personal Information on Part of Its Recipients)

- Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties)
- Article 21 (Destruction of Personal Information)
- Article 22 (Methods of Obtaining Consent)

SECTION 2 Limitation to Processing of Personal Inf

- Article 23 (Limitation to Processing of Sensitive Information)
- Article 24 (Limitation to Processing of Personally Identifiable Information)
- Article 24-2 (Limitation to Processing of Resident Registration Numbers)
- Article 25 (Limitation to Installation and Operation of Visual Data Processing Devices)
- Article 26 (Limitation to Personal Information Processing Subsequent to Outsourcing of Work)
- Article 27 (Limitation to Transfer of Personal Information following Business Transfer, etc.)
- Article 28 (Supervision of Personal Information Handlers)

SECTION 3 Special Cases concerning Pseudonymous Data

- Article 28-2 (Processing of Pseudonymous Data)
- Article 28-3 (Restriction on Combination of Pseudonymous Data)
- Article 28-4 (Obligation to Take Safety Measures for Pseudonymous Data)
- Article 28-5 (Prohibited Acts for the Processing of the Pseudonymized Information)
- Article 28-6 (Imposition of Administrative Surcharges for the Processing of the Pseudonymized Information)
- Article 28-7 (Scope of Application)

CHAPTER IV SAFEGUARD OF PERSONAL INFORMATION

- Article 29 (Duty of Safeguards)
- Article 30 (Establishment and Disclosure of Privacy Policy)
- Article 31 (Designation of Privacy Officers)
- Article 32 (Registration and Disclosure of Personal Information Files)
- Article 32-2 (Certification of Personal Information Protection)
- Article 33 (Privacy Impact Assessment)
- Article 34 (Data Breach Notification)
- Article 34-2 (Imposition, etc. of Penalty Surcharges)

CHAPTER V GUARANTEE OF RIGHTS OF DATA SUBJECTS

- Article 35 (Access to Personal Information)
- Article 36 (Rectification or Erasure of Personal Information)
- Article 37 (Suspension of Processing of Personal Information)
- Article 38 (Methods and Procedures for Exercise of Rights)
- Article 39 (Responsibility for Compensation)
- Article 39-2 (Claims for Statutory Compensation)

CHAPTER VI SPECIAL CASES CONCERNING PROCESSING OF

- Article 39-3 (Special Provisions on Consent to the Collection and Use of Personal Information)
- Article 39-4 (Special Cases on the Notification and Reporting on the Divulgence of Personal Information)
- Article 39-5 (Special Cases on Safeguards for Personal Information)
- Article 39-6 (Special Cases on the Destruction of Personal Information)
- Article 39-7 (Special Cases on Users' Rights)
- Article 39-8 (Notification of the Use History of Personal Information)
- Article 39-9 (Indemnity for Losses)
- Article 39-10 (Deletion and Blocking of Exposed Personal Information)
- Article 39-11 (Designation of Domestic Agents)
- Article 39-12 (Protection of Information Transferred Overseas)
- Article 39-13 (Reciprocity)
- Article 39-14 (Special Cases for Broadcasting Service Providers)
- Article 39-15 (Special Cases for the Imposition of Administrative Surcharges)

CHAPTER VII PERSONAL INFORMATION DISPUTE MEDIATION
- Article 40 (Establishment and Composition)
- Article 41 (Guarantee of Members' Status)
- Article 42 (Exclusion, Recusal, and Refrainment of Members)
- Article 43 (Application for Mediation)
- Article 44 (Time Limitation of Mediation Proceedings)
- Article 45 (Request for Materials)
- Article 46 (Settlement Advice before Mediation)
- Article 47 (Dispute Mediation)
- Article 48 (Rejection and Suspension of Mediation)
- Article 49 (Collective Dispute Mediation)
- Article 50 (Mediation Procedures)

CHAPTER VIII CLASS-ACTION LAWSUIT OVER DATA INFRIN
- Article 51 (Parties to Class Action Lawsuit)
- Article 52 (Exclusive Jurisdictions)
- Article 53 (Retention of Litigation Attorney)
- Article 54 (Application for Permission of Lawsuit)
- Article 55 (Requirements for Permission of Lawsuit)
- Article 56 (Effect of Conclusive Judgment)
- Article 57 (Application of Civil Procedure Act)

CHAPTER IX SUPPLEMENTARY PROVISIONS
- Article 58 (Partial Exclusion of Application)
- Article 58-2 (Exemption from Application)
- Article 59 (Prohibited Activities)
- Article 60 (Confidentiality)
- Article 61 (Suggestions and Recommendations for Improvements)
- Article 62 (Reporting on Infringements)
- Article 63 (Requests for Materials and Inspections)
- Article 64 (Corrective Measures)
- Article 65 (Accusation and Recommendation for Disciplinary Action)
- Article 66 (Disclosure of Results)
- Article 67 (Annual Reports)
- Article 68 (Delegation and Entrustment of Authority)
- Article 69 (Persons Deemed to be Public Officials for Purposes of Penalty Provisions)

CHAPTER X PENALTY PROVISIONS
- Article 70 (Penalty Provisions)
- Article 71 (Penalty Provisions)
- Article 72 (Penalty Provisions)
- Article 73 (Penalty Provisions)
- Article 74 (Joint Penalty Provisions)
- Article 74-2 (Confiscation and Collection)
- Article 75 (Administrative Fines)
- Article 76 (Special Exemption to Application of Provisions on Administrative Fines)

ADDENDA

- 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.

The content of this act is the following:

- Article 1 (Purpose)
- Article 2 (Definition)
- Article 3 (Devising policies to protect and use location information)
- Article 4(Relationship to other laws)
- Article 5 (Permission of the location information business, etc.
- Article 6 (Reasons for disqualification of executives)
- Article 7 (Transfer of location information business and merger of corporations)
- Article 8 (Suspension, discontinuation, etc. of the location information business)
- Article 9 (Reporting of the location-based service business)
- Article 10 (Transfer of the location-based service business, merger of corporations, etc.)
- Article 12 (Reporting of service agreements, etc.)
- Article 13 (Cancellation of permission and discontinuation, suspension, etc. of business)
- Article 14 (Imposition of surcharges, etc.)
- Article 15 (Prohibition of collection of location information, etc.)
- Article 16 (Protection of location information, etc.)
- Article 17 (Prohibition of leaking of location information, etc.)
- Article 18 (Collection of personal location information)
- Article 19 (Use or provision of personal location information)
- Article 20 (Location information provider's provision of personal location information, etc.)
- Article 21 (Restriction of the use and provision of personal location
- information, etc.)
- Article 22 (Notification of transfer of business, etc.)
- Article 23 (Destruction of personal location information, etc.)
- Article 24 (Rights of personal location information subjects, etc.)
- Article 25 (Rights of legal representatives)
- Article 26 (Use of location information for protection of children under 8 years of age)
- Article 27 (Compensation for damages)
- Article 28 (Mediation of disputes, etc.)
- Article 29 (Use of personal location information for emergency relief
- Article 30 (Request for and personal location information and method thereof)
- Article 31 (Reduction and exemption of costs)
- Article 32 (Submission of statistical data, etc.)
- Article 33 (Technology development, etc.)
- Article 34 (Standardization)
- Article 35 (Promotion of use of location information)
- Article 36 (Location information deliberation committee)
- Article 37 (Public hearing)
- Article 38 (Delegation of authorities)
- Article 39 (Penal provisions)
- Article 40 (Penal provisions)
- Article 41 (Penal provisions)
- Article 42 (Dual punishment)

- Act on Use and Protection of Credit Information Act established on July 6, 1995 and lastly revised on July 26th, 2017
  http://www.pipc.go.kr/cmt/english/functions/creditInfo.do

  The purpose of this act is to foster a sound credit information business, promoting an efficient utilization and systematic management of credit information, and protecting privacy, etc. from the misuse and abuse of credit information properly, thereby contributing to the establishment of order in credit.

The content of this act is the following:

- Article 1 (Purpose)
- Article 2 (Definitions)
- Article 15 (Principles of Collection, Investigation and Processing)
- Article 16 (Restrictions on Collection, Investigation and Processing)
- Article 17 (Outsourcing of Collection, Investigation and Processing)
- Article 18 (Keeping Credit Information Accurate and Up-to-Date)
- Article 19 (Security Protection of Credit Information Computer System)
- Article 20 (Clarification of Accountability of Credit Information Management and Archiving
- of Business Processing Records)
- Article 20-2 (Retention Period, etc. for Personal Credit Information)
- Article 21 (Disposition of Archived Information upon Closure of Business)
- Article 31 (Public Notification of Credit Information Utilization Status)
- Article 32 (Consent to Provision and Use of Personal Credit Information)
- Article 33 (Use of Personal Credit Information)
- Article 34 (Provision and Use of Personal Identification Information)
- Article 35 (Fact-finding Inquiries into Use and Provision of Credit Information)
- Article 36 (Notification, etc. of Credit Information Giving Rise to Refusal of Commercial
- Transaction)
- Article 37 (Rights, etc. to Revoke Consent to Provide and Use Personal Credit
- Information)
- Article 38 (Demand for Perusal and Correction of Credit Information, etc.)
- Article 38-2 (Requests for Notification of Credit Inquiry)
- Article 38-3 (Request for Deletion of Personal Credit Information)
- Article 39 (Right to Free Perusal)
- Article 39-2 (Notification, etc. of Divulgence of Credit Information)
- Article 40 (Prohibited Matters for Credit Information Company, etc.)
- Article 41 (Prohibited Matters for Claims Collection Agency)
- Article 41-2 (Verification, etc. of Recruitment Channels of Agents of Recruitment
- Business)
- Article 42 (Prohibition of Divulgence, etc. for Non-Business Purposes)
- Article 42-2 (Imposition, etc. of Penalty Surcharges)
- Article 43 (Liability to Compensate for Damages)
- Article 43-2 (Claim for Statutory Damages)
- Article 43-3 (Guarantee of Compensation for Damage)
- Article 44 (Credit Information Companies Association)

5.1.17 Lithuania

Data privacy commissioner

State Data Protection Inspectorate
https://vdai.lrv.lt/

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Law of the Republic of Lithuania on Legal Protection of Personal Data
  https://www.e-tar.lt/portal/legalAct.html?documentId=43cddd8084cc11e8ae2bfd1913d66d57

EN
https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae?jfwid=-td2hew3hb

- Law of the Republic of Lithuania on Legal Protection of Personal Data Processed in the Framework of Police and Judicial Co-Operation in Criminal Matters
https://www.e-tar.lt/portal/legalAct.html?documentId=f0327c5084ce11e8ae2bfd1913d66d57

- Law of the Republic of Lithuania on Cyber Security
  https://www.e-tar.lt/portal/legalAct.html?documentId=67b9e0b07eb711e8ae2bfd1913d66d57
  EN
  https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ceb0e7b291ad11e8aa33fe8f0fea665f?jfwid=-td2hew3bq

- The list of the mandatory DPIA
  https://www.e-tar.lt/portal/lt/legalAct/abb01940465511e9a221b04854b985af

- Other recommendations, guidelines, local laws
  https://vdai.lrv.lt/lt/teisine-informacija/teises-aktai

5.1.18 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Amended Act of August 2nd, 2002 ("Data Protection Act")
  http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf#pagemode=none
  http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf (English version)

  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.legilux.public.lu/leg/a/archives/2005/0073/a073.pdf#page=26 (Original version unmodified by the Act of July 27th, 2007)
  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.

- Act of July 27th, 2007
  http://www.legilux.public.lu/leg/a/archives/2007/0131/a131.pdf

5.1.19 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Data Protection Act 2010 (Act 709)
  http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf

  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.

5.1.20 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 and regarding 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

  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)
  http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf

- Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties
  http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf

  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
  http://inicio.ifai.org.mx/DocumentosdeInteres/
  Guia_para_instrumentar_medidas_compensatorias.pdf

- Recommendations for appointment of the person or department of personal data
  http://inicio.ifai.org.mx/Publicaciones/Recomendaciones%20designacion%20Perona%20o%20Departamento%20%20Datos%20Personales.pdf

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

- Information security recommendations
  http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

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 followign 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
  http://www.economia.gob.mx/files/marco_normativo/PAR1.pdf

- Manual on security of personal data for small and medium organizations
  http://inicio.inai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf

- Guide to implement a Personal Data Security Management System
  http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementaci%C3%B3n_SGSDP_ene2014.pdf

5.1.21 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Personal Data Protection Act
  http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml

  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.

5.1.22 New Zealand

Data privacy commissioner

Office of the Privacy Commissioner/Te Mana Mātāpono Matapu
https://www.privacy.org.nz/

The Office of the Privacy Commissioner (OPC) is an Independent Crown Entity. It is funded by the state but is independent of Government or Ministerial control. OPC has a wide range of functions, which are listed in section 17 of the Privacy Act 2020.

Some key areas of work include:

- monitoring and enforcing compliance with the Privacy Act
- investigating complaints about breaches of privacy
- receiving reports of notifiable privacy breaches
- monitoring and examining the impact that technology has on privacy
- developing codes of practice for specific industries or sectors
- inquiring into any matter where it appears that individual privacy may be affected.

The OPC's website has up to date information about the Privacy Act and codes of practice as well as helpful providing guidance and resources.

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Privacy Act 2020
  https://legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23322

  The purpose of this Act is to promote and protect individual privacy by:

  a) Providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and
  b) Giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

  This act is the primary law regarding privacy in New Zealand. This is supplemented by six codes of practice:

  a) Civil Defence National Emergencies (Information Sharing) Code 2020
  b) Credit Reporting Privacy Code 2020
  c) Health Information Privacy Code 2020
  d) Justice Sector Unique Identifier Code 2020
  e) Superannuation Schemes Unique Identifier Code 2020
  f) Telecommunications Information Privacy Code 2020

  Section 24 of the Act clarifies the relationship between the application of the Act's Information Privacy Principles (IPPs) and other New Zealand law.

Public Sector

The Government Chief Privacy Officer (GCPO) supports government agencies to meet their privacy responsibilities and improve their privacy practices. Advice, guidance and tools to improve privacy capability and maturity are available at
https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/.

5.1.23 Peru

Data privacy commissioner

Autoridad Nacional de Protección de Datos Personales
https://www.minjus.gob.pe/dgtaipd/

NOTE: The "Autoridad Nacional de Protección de Datos Personales" is included in the "Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales" (Ministry of Justice - "MINJUS")

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Ley 29733 – Protection to Personal Data ACT
  http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

- Regulation for the law
  http://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf

- 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

- Video surveillance directive
  https://www.minjus.gob.pe/wp-content/uploads/2020/01/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf

- Model for privacy notice in compliance to Article 18 from Ley 29733
  https://www.minjus.gob.pe/wp-content/uploads/2018/07/ANEXO-I_Condiciones-de-Tratamiento-de-Datos-Personales.pdf

- Legislative Decree N°1353 : Creation of a National Authority of Transparency and Access to Public Information, and modification to Ley N°29733 – Protection to Personal Data ACT
  https://www.minjus.gob.pe/wp-content/uploads/2017/02/Decreto-Legislativo-1353.pdf

- Regulation of the Legislative Decree N°1353
  https://www.minjus.gob.pe/wp-content/uploads/2018/01/Reglamento-del-decreto-legislativo-n-1353-.pdf

5.1.24 Philippines

Privacy commissioner

National Privacy Commission
https://privacy.gov.ph

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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- R.A 10173: Data Privacy Act of 2012
  https://privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf

- Implementing Rules and Regulations of DPA of 2012
  https://privacy.gov.ph/wp-content/uploads/IRR-of-the-DPA.pdf
  The NPC exists to ensure compliance of the country with international standards set for data protection. It is the Philippine government's arm to make sure the data subject remains in full control of his/her personal information in this digital age. As digital evolution progresses and the need for data arise, the NPC safeguards the rights of a data subject while ensuring the free flow of information for innovation, growth, and national development.

- NPC Memorandum Circular 16-01 - Security of Personal Data in the Government
  https://privacy.gov.ph/memorandum-circulars/npc-circular-16-01-security-of-personal-data-in-government-agencies/
  These rules are issued to assist government agencies in the Philippines, as well as a guide for private entities engaged in the processing of personal data to meet their legal obligations under R.A. 10173.

- NPC Memorandum Circular 16-02 – Data Sharing Agreements Involving Government Agencies
  https://privacy.gov.ph/memorandum-circulars/npc-circular-16-02-data-sharing-agreements-involving-government-agencies/
  The provisions of this Circular apply to government agencies that share or transfer personal information for the purpose of performing a public function or providing of a public service. These provisions also cover personal data under the control or custody of a private entity that are being shared with or transferred to a government agency.

- NPC Memorandum Circular No. 16-03 – Personal Data Breach Management
  https://privacy.gov.ph/memorandum-circulars/npc-circular-16-03-personal-data-breach-management/
  The rules under this circular apply to any natural and juridical person in the government or private sector processing personal data in or outside of the Philippines regarding data breach management. These rules also provide the framework for personal data breach management and the procedure for personal data breach notification and other requirements.

- NPC Memorandum Circular No. 16-04 – Rules of Procedure of the National Privacy Commission
  https://privacy.gov.ph/memorandum-circulars/npc-circular-16-04-rules-of-procedure/
  This is a regulation issued by the National Privacy Commission regarding their procedure in receiving complaints, grievances, requests for assistance or advisory opinions, and other matters cognizable by the Commission

- NPC Memorandum Circular No. 17-01 – Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making
  https://privacy.gov.ph/npc-circular-17-01-registration-data-processing-notifications-regarding-automated-decision-making/

This Circular establishes the framework for registration of data processing systems in the Philippines. The provisions of this Circular shall apply to any natural or juridical person in the government or private sector processing personal data and operating in the Philippines, subject to the relevant provisions of the DPA, its IRR, and other applicable issuances of the NPC.

- NPC Advisory No. 17-01 Designation of Data Protection Officers
  https://privacy.gov.ph/wp-content/uploads/NPC-Advisory-2017-01-sgd.pdf
  These Guidelines shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and issuances by the NPC.

- NPC Advisory No. 17-02 - Access to Personal Data Sheets of Government Personnel
  https://privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.2017-02.pdf
  These are guidelines on how government agencies would handle requests for information on government personnel.

- NPC Advisory No. 17-03 – Guidelines on Privacy Impact Assessments
  https://privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.2017-03.pdf
  This advisory provides guidelines in conducting a privacy impact assessment for both government and private entities that process personal information.

- NPC Circular No. 18-01 – Rules of Procedure on Requests for Advisory Opinions
  https://www.privacy.gov.ph/npc-circular-no-18-01-rules-of-procedure-on-requests-for-advisory-opinions/
  These rules shall apply to all requests for advisory opinions cognizable by the NPC. An advisory opinion refers to a determination of the NPC on matters relating to data privacy or data protection, at the request of any party, or on a complaint endorsed by the Complaints and Investigations Division (CID) under Sections 4 and 10 of Rule II of NPC Circular No. 2016-04.

- NPC Circular No. 18-02 – Guidelines on Compliance Checks
  https://www.privacy.gov.ph/npc-circular-no-18-02-guidelines-on-compliance-checks/
  These rules shall apply to any Personal Information Controller (PIC) or Personal Information Processor (PIP) in the government or private sector processing personal data in the Philippines, subject to the relevant provisions of the Act and its Implementing Rules and Regulations. These rules provide the guidelines for the conduct of Compliance Checks by personnel of the Commission, whichever mode it may be.

- NPC Circular No. 18-03 – Rules on Mediation before the National Privacy Commission
  https://www.privacy.gov.ph/npc-circular-no-18-03-rules-on-mediation-before-the-national-privacy-commission/
  These rules shall apply to all complaints filed before the Commission. Mediation refers to the voluntary process in which a mediation officer facilitates communication and negotiation and assists the parties in reaching a voluntary agreement regarding a dispute.

- NPC Advisory No. 18-02 – Updated Templates on Security Incident and Personal Data Breach Reportorial Requirements
  https://privacy.gov.ph/wp-content/files/attachments/nwsltr/Final_Advisory18-02_6.26.18.pdf
  These templates can be used by the Personal Information Controllers (PICs) or Personal Information Processors (PIPs) for the reportorial requirements on security incidents and personal data breaches

- NPC Advisory Opinions
  https://www.privacy.gov.ph/advisory-opinions/
  These refers to issuances of the Commission on matters relating to data privacy or data protection, at the requests of any party, or on a complaint.

- The DPO Journal
  https://dpojournal.privacy.gov.ph
  This is the official monthly newsletter of the Philippine's National Privacy Commission where articles about issues and topics about data privacy and data protection.

- NPC Privacy Toolkit
  https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/3rdToolkit_0618.pdf
  The NPC Privacy Toolkit equips and guides PICs, PIPs, and Data Protection Officers (DPOs) through the process of complying with the law and building an organizational culture protective of individuals' data privacy rights.

- Data Privacy and Security Advisory (DPSA)
  https://www.privacy.gov.ph/2020/02/managing-mobile-app-permissions/
  A series of issuances of the National Privacy Commission (NPC) with regards to the relevant privacy issues that may cause privacy panic.

- NPC PrivacyWall
  https://privacywall.privacy.gov.ph/
  This forum site is the official platform of the NPC in disseminating information and hosting dialogues relevant to data privacy in all sectors. It establishes the digital community for Data Protection Officers (DPOs).

- NPC COVID-19 Bulletins
  https://www.privacy.gov.ph/list-of-npc-issuances-related-to-covid-19/
  A series of issuances released by the National Privacy Commission (NPC) with regards to relevant privacy issues in this COVID-19 pandemic.

- DOH-NPC Joint Memorandum Circular No. 2020-0001 – Guidelines on the Use of Telemedicine in COVID-19 Response
  https://www.privacy.gov.ph/wp-content/uploads/2020/10/DOH-mc2020-0016.pdf
  The overall aim of this Joint Memorandum Circular is to enable patients to receive health services even while staying at home except for serious conditions, emergencies, or to avail of COVID-19-related health services as per standing protocols.

- DOH-NPC Joint Memorandum Circular No. 2020-0002 – Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response
  https://www.privacy.gov.ph/wp-content/uploads/2020/10/jmc2020-0002v1.pdf
  This Joint Memorandum Circular implements the guidelines for the collection, processing and disclosure of COVID-19-related data in pursuit of disease surveillance and response, while protecting the data privacy rights f patients and individuals and ensuring the confidentiality, integrity, and availability of their personal data.

- NPC Circular No. 20-01 – Guidelines on the Processing of Personal Data for Loan-Related Transactions
  https://www.privacy.gov.ph/wp-content/uploads/2020/10/NPC-Circular-No.-20-01.pdf
  This Circular shall apply to, among others, the processing of personal data for purposes of loan processing activities, 1 through any modality, by lending or financing companies, as defined under the Lending Company Regulation Act of 2007 and Financing Company Act of 1998, respectively, or by any natural or juridical person who acts as such, whether or not granted with the requisite authority from the Securities and Exchange Commission (SEC). It shall likewise apply to personal information processors (PIP) or third-party service providers engaged by the lending or financing company, or any natural or juridical person who acts as such, whenever such PIPs or third-party service providers are engaged in the processing of the personal information of the latter's clients.

- NPC Circular No. 20-02 – Rules on the Issuance of Cease and Desist Order
  - https://www.privacy.gov.ph/wp-content/uploads/2020/10/NPC-Circular-20-02_Circular-Rules-on-CDO.pdf
  - FAQs:https://www.privacy.gov.ph/wp-content/uploads/2020/10/FAQs-for-Publication_NPC-Circular-20-02_Circular-Rules-on-CDO.pdf

These Rules shall apply to all applications for a Cease and Desist Order on the processing of personal data and other matters cognizable by the National Privacy Commission.

- NPC Circular No. 2020-03 – Data Sharing Agreements
  https://www.privacy.gov.ph/wp-content/uploads/2021/01/Circular-Data-Sharing-Agreement-amending-16-02-21-Dec-2020-clean-copy-FINAL-LYA-and-JDN-signed-minor-edit.pdf
  The provisions of this Circular apply to personal data under the control or custody of a personal information controller (PIC) that is being shared, disclosed, or transferred to another PIC. The Circular likewise applies to personal data that is consolidated by several PICs and shared or made available to each other and/or to one or more PICs.

- NPC Advisory No. 2020-01 - Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website
  - https://www.privacy.gov.ph/wp-content/uploads/2020/11/NPC-Advisory-2020-01-FINAL.pdf
  - Amendments: https://www.privacy.gov.ph/wp-content/uploads/2020/11/Amendment-to-Advisory-2020-01-Final.pdf

  These guidelines shall cover all Commission Decisions, Resolutions and Orders issued by the Commission En Banc.

- NPC Advisory No. 2020-02 – Guidelines in the Use of Videoconferencing Technology for the Remotes Appearance and Testimony of Parties Before the National Privacy Commission
  https://www.privacy.gov.ph/wp-content/uploads/2020/10/FINAL-VERSION-Guidelines-on-the-Use-of-Videoconferencing-Technology-for-Remote-Appearance-before-the-NPC-OPC.pdf
  The advisory provides parties the option to attend the proceedings remotely, in the relative safety of their chosen premises, in accordance with the Rules of Procedure, before the National Privacy Commission.

- NPC Advisory No. 2020-03 –Guidelines for Workplaces and Establishments Processing Personal Data for COVID-19 Response
  - https://www.privacy.gov.ph/wp-content/uploads/2020/11/NPC-Advisory-No.-2020-03-FINAL.pdf
  - Amendments: https://www.privacy.gov.ph/wp-content/uploads/2020/11/Advisory-2020-03-A-FINAL.pdf

  This Advisory aim to provide additional guidance to supplement the Joint Memorandum Circular (JMC) No. 20-04-A Series of 20201 issued by the Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE) which requires workplaces and various establishments to collect employee health declaration forms and client/visitor contact tracing forms and implement measures to manage asymptomatic and symptomatic employees in the workplace**.**

- NPC Advisory No. 2020-04 – Guidelines on the Use of Closed-circuit Television (CCTV) Systems
  https://www.privacy.gov.ph/wp-content/uploads/2020/11/Advisory-on-CCTV-16NOV2020-FINAL.pdf
  This Advisory shall apply to all PICs and PIPs engaged in the processing of personal data through the use of CCTV systems operating in public and semi-public areas. These include CCTV systems that record videos, as well as those systems with both video and audio capabilities.

- NPC Privacy Safety Security & Trust Online (PSST!) Campaign
  https://www.privacy.gov.ph/psst/
  The PSST! is an advocacy campaign that emphasizes the central role of data subjects in creating a digital democratic space conducive to privacy, safety, security, and trust. This campaign aims to empower digital citizens by increasing their awareness on their data privacy rights and responsibilities.

- NPC Kabataang Digital
  https://www.privacy.gov.ph/kd/
  The Kabataang Digital (KD) is a campaign under PSST! that encourages data protection for children by enjoining school officials and parents in educating their children on appropriate digital citizenship, promoting safe choices, and elaborating the implications of the digital environment for children's privacy rights.

- PNS Advisory Adoptions
  https://www.privacy.gov.ph/pns-advisory-adoptions/
  List of Advisory Adoptions of the NPC to ISO/IEC standards on data privacy and protection. The advisory describes the standards, its benefits to the organizations and guide for adopting.

5.1.25 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 and regarding 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

- Law 103/2015 - adds article 45-A - The insertion of false data - to Law 67/98
  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
  https://www.cnpd.pt/bin/cnpd/Lei_43_2004.pdf

Health

- Law 12/2005 - Personal health genetic information
  https://www.cnpd.pt/bin/legis/nacional/Lei12-2005.pdf

Electronic Communications

- Decree-Law 7/2004 - E-Commerce

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

- Law 46/2012 - Amends Law 41/2004 and Decree-Law 7/2004
https://www.cnpd.pt/bin/legis/nacional/Lei_46_2012.pdf

- Regulation (EU) No 611/2013 - Measures applicable to the notification of breaches of personal data in accordance with Directive 2002/58 / EC of the European Parliament and of the Council on privacy and electronic communications
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:PT: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 vídeo 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

- Law 1/2005 – Regulates vídeo surveillance systems in use by the law enforcement forces in public places.
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
https://www.cnpd.pt/bin/legis/nacional/DL207-2005-RADARES.pdf

- 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
https://www.cnpd.pt/bin/legis/nacional/PORTARIA1164-A-2007-vvgTAXIS.pdf

Work

- Law 7/2009 - Approves the Labor Code
http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=1047&tabela=leis

Citizen's card

- Law 7/2007 - Creates citizen's card and governs its issuance and use
https://www.cnpd.pt/bin/legis/nacional/Lei7-2007-cartao-cidadao.pdf

Cyibercrime

- Law 109/2009 - Cybercrime Law
  http://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf

5.1.26 Slovenia

Data privacy commissioner

Information Commissioner of Slovenia
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 and regarding 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)
  https://www.ip-rs.si/fileadmin/user_upload/doc/ZVOP-1_in_ZVOP-1a__English_/30.10.07-Personal_Data_Protection_Act_of_Slovenia_status_2007_final_eng.doc

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

5.1.27 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Organic Law 15/1999
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/Ley_Orgaica_15-99_ingles.pdf

  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
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/reglamentolopd_en.pdf

  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
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/Ley_34-2002_LSSI_ingles.pdf

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
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/LEY_DE_AUTON_DEL_PACIENTE.pdf

  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
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/Ley_32-2003_LGT.pdf

- Act 62/2003 on fiscal measures, administrative measures and measures of a social nature
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/ACT_62_2003.pdf

- Instruccion 1/2006 on processing personal data for surveillance purposes through camera or video-camera systems
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/instruccion_1-2000_ingles_pdf.pdf

- Instruccion 1/2000 on the rules governing international data movements
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/instruccion_1-2000_ingles_pdf.pdf

- Instruccion 1/1995 regarding the rendering of information services on creditworthiness and credit
  https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/ACT_62_2003.pdf

5.1.28 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Data Protection Act 2018
  http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

  The Act comprises 215 Clauses and 20 Schedules

The Act makes provision about the processing of personal data
Most processing of personal data is subject to the GDPR
Part 2 supplements the GDPR (see Chapter 2) and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply (see Chapter 3)
Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive
Part 4 makes provision about the processing of personal data by the intelligence services
Part 5 makes provision about the Information Commissioner
Part 6 makes provision about the enforcement of the data protection legislation
Part 7 makes supplementary provision, including provision about the application of this Act to the Crown and to Parliament

5.1.29 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 and regarding data privacy, please contact the local Data Privacy Commissioner or any relevant public administrations.

- Gramm-Leach-Bliley Act (GLBA)
  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

  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)
  http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR02622:|TOM:/bss/d108query.html

  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

  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
  http://www.fcc.gov/Reports/1934new.pdf

  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)
  http://www.fcc.gov/cgb/consumerfacts/tcpa.html

  This act regulates telemarketing and establishes a national Do-Not-Call list.

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

  This act applies to telephone carriers' use of "customer proprietary network information".

- Electronic Communications Privacy Act (ECPA)
  http://it.ojp.gov/default.aspx?area=privacy&page=1285

  This act protects wire, oral, and electronic communications while in transit.

It defines requirements for search warrants.

- Family Educational and Privacy Rights Act (FERPA)
  - http://www2.ed.gov/policy/gen/guid/fpco/index.html
  - http://www2.ed.gov/policy/gen/reg/ferpa/index.html

  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

  This act prohibits unauthorized access to protected computers.

- Video Privacy Protection Act (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
  http://www.justice.gov/opcl/privacyact1974.htm

  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.

5.2 Data retention periods

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

5.2.1 Argentina

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.

Type of documents	Mandatory retention period(s)	Recommended period(s) (optional)	Legislative reference	Type (optional)
Personal data	Once the contractual relationship has been completed, if there is authorization from the data owner to use it in subsequent operations, the personal data may be stored for a period of up to two years.		Article 25, Law 25.326	
Significant personal data to evaluate the economic-financial solvency	For five years. If the debtor cancels or terminates the obligation, this retention period is reduced to two years.		Article 26, Law 25.326	

5.2.2 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.

Type of documents	Mandatory retention period(s)	Recommended period(s) (optional)	Legislative reference	Type (optional)
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

5.2.3 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.

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

5.2.4 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.

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

5.2.5 Lithuania

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.

The Office of the Chief Archivist of Lithuania is a government agency, which participates in the shaping of national policy in the field of management and use of documents and archives, as well as implements this policy, supports the Chief Archivist of Lithuania in the carrying-out of state administration of the field of documents and archives.

The Office of the Chief Archivist of Lithuania establishes document retention period

LAW ON DOCUMENTS AND ARCHIVES

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.436564?jfwid=-lrklxcxem

Data controller decides other data retention periods

other related laws:

http://www.archyvai.lt/en/legislation.html

5.2.6 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.

Type of documents	Mandatory retention period(s)	Recommended period(s) (optional)	Legislative reference	Type (optional)
Accounting documents	10 years			Original / Reproduction
Pension fund	+ 30 years after (prescription)		Applicable Law- Complimentary Pension Regime 8 June 1999	Original / Reproduction
Personnel files	3 years if remuneration	Wages and personal documents can also be considered as related to accounting documents. They shall consequently be kept for 10 years	Applicable Law- Civil Code Art. 2277	Original / Reproduction
Payroll	3 years (see personnel)		Applicable Law- Civil Code Art. 2277	Original / Reproduction
Physical access control	3 months	3 years if physical access control system used for working hours control	Deliberation 64/2007 from June 22nd 2007	Original / Reproduction
Video monitoring	1 month	7 days	-	Original / Reproduction
Working hours control	3 years		Deliberation 63/2007 from June 22nd 2007	Original / Reproduction

5.2.7 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.

Type of documents	Mandatory retention period(s)	Recommended period(s) (optional)	Legislative reference	Type (optional)
Commercial document	No legal period	-	-	-
Tax document including job contracts	7 years	-	Articles 2:10 and 3:15i of the Civil Code and Article 52 of AWR	-
Salary administration	2 years	-	Article 8 of the Personal Data Protection Act	-
Staff administration	2 years	-	Article 7 of the Personal Data Protection Act	-
Employees income tax form	5 years	-	Article 65 of the law of 2001related to salary tax	-
Copies of employees proof	5 years	-	Article 66 of the law of 2001related to salary tax	-

of identity				
Data about applicant	4 weeks without applicant approval 1 year max with approval	-	Article 5 of the Personal Data Protection Act	-
Work and rest time records	52 weeks	-	Article 3.2.1 of the Working Hours Decree	-
Work medical examination about dangerous material	40 years	-	Article 4.10.d of the Working Conditions Decree	-
Work medical examination about biological agents	10 years	-	Article 4.91 of the Working Conditions Decree	-
List of employees dealing with task which are dangerous for their safety and health	40 years	-	Article 4.15 jo and article 4.10.d of the Working Conditions Decree	-
List of employees exposed to asbestos	40 years	-	Article 4.53 jo article 4.10.d of the Working Conditions Decree	-
Register of employees dealing with categories 3 and 4 biological agent	10 years	-	Article 4.90 of the Working Conditions Decree	-
Mechanical vibration measure	10 years	-	Article 6.11b of the Working Conditions Decree	-

5.2.8 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).

Documents/Records to Retain	Retention Period	Observations
Payments and other documents relating to the provision of services by third parties	5 years - Art. 36.º Decree-Law 17/2009	

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

Documents/Records to Retain	Retention Period	Observations
		contract.
Data base	Until the date of authorization to hold the database, if applicable, or 10 years, otherwise	
Registration of legal actions in labor matters	10 years	

5.2.9 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.

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

5.2.10 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.

Type of documents	Mandatory retention period(s)	Recommended period(s) (optional)	Legislative reference	Type (optional)
Accounting document	10 years from the end of the fiscal year	-	Articles from the 32nd title of the « Code des Obligations »	Original or electronic
Commercial document	No legal period	30 years	-	Original
Tax document	10 years from the end of the fiscal year		Articles from the 32nd title of the « Code des Obligations »	Original
Human resources document	40 years for staff health files No legal period for others	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	Article 16 of the « Ordonnance concernant la tenue et la conservation des livres de comptes » (Olico)	Original

6 Standards and guidelines

6.1 Standards

6.1.1 Information security and PII protection

- ISO/IEC 27018 International Standard
  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
  Information technology - Security techniques - Privacy framework

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

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

- ISO/IEC 29151 International Standard
  Information technology -- Security techniques -- Code of practice for personally identifiable information protection

- ISO Guide 73
  Risk management - Vocabular

- ISO/IEC 27001:2013 International Standard
  Information technology - Security techniques - Information security management systems - Requirements

- ISO/IEC 27002:2013 International Standard
  Information technology - Security techniques - Code of practice for information security management

- ISO/IEC 31000:2009 International Standard
  Risk management - Principles and guidelines

- ISO/IEC 27701:2019 International Standard
  Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines

- ISO/IEC 29184:2020 International Standard

- ISO/IEC 29184:2020 International Standard
  Information technology — Online privacy notices and consent

- GB/Z 28828-2012 Information Security Technique: Personal Information Protection Guide in Public and Commercial Service Information System(CN)
  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.

- GB/T 35273 - 2017 Information security technology—Personal information security specification (CN)

  This standard stipulates the principles and safety requirements for the collection, preservation, use, sharing, transfer, public disclosure and other personal information processing activities. This standard is applicable to the regulation of personal information processing activities of various organizations. It is also applicable to the supervision, management and evaluation of personal information processing activities by organizations such as competent regulatory authorities and third-party evaluation agencies.

- GB/T 37964 - 2019 Information security technology—Guide for de-identifying personal information (CN)

  This standard describes the goals and principles of personal information de-identification and proposes the process of de-identification and management measures.

- GB/T 35273-2020 Information security technology - Personal information security specification

  The Standard specifies the principles and security requirements for the collection, storage, use, sharing, transfer, public disclosure and deletion of personal information.
  The Standard is applicable to personal information processing activities carried out by all kinds of organizations. It can also be used by competent authorities, third party assessment agencies and other organizations to supervise, manage and evaluate personal information processing activities.

- GB/T 34978—2017 Information Security Technology—Technology Requirements for Personal Information Protection of Smart Mobile Terminal

  The standard specifies the personal information classification of smart mobile terminals, as well as the protection principles and technical requirements of personal information
  The standard applies to guide public and commercial smart terminal to process personal information, other related parties may refer it for use as well.

6.1.2 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.

6.2 Guidelines

6.2.1 Financial services

- Credit Reporting Code of Conduct
  http://www.privacy.gov.au/materials/types/codesofconduct/view/6787

  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:

  a) Deal promptly with individual requests for access and amendment of personal credit information
  b) Ensure that only permitted and accurate information is included in an individual's credit information file
  c) Keep adequate records in regard to any disclosure of personal credit information
  d) Adopt specific procedures in settling credit reporting disputes
  e) 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.

- Report on the Review of the Credit Provider Determinations
  http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=reports&fullsummary=6031&Itemid=1021

- **Code of Practice on Consumer Credit Data**
  http://www.pcpd.org.hk/english/files/ordinance/CCDCode_eng.pdf

  This code of practice habe 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 references agencies and debt collection agencies.

- **Credit Reporting Privacy Code**
  http://www.privacy.org.nz/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.

- Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes (18 September 2002)
  https://wcd.coe.int/ViewDoc.jsp?id=306221&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990)
  https://wcd.coe.int/ViewDoc.jsp?id=603199&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR
  Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR | European Data Protection Board (europa.eu)

6.2.2 Health Sector

- Guidelines on Privacy in the Private Health Sector
  http://www.privacy.gov.au/materials/types/guidelines/view/6517
  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.

- The Medical and Health Sector: The Data Protection Rules in Practice
  http://www.dataprotection.ie/viewdoc.asp?DocID=245
  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.

- Standards for Privacy of Individually Identifiable Health Information
  http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm
  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.

- HHS Fact Sheet on Protecting the Privacy of Patient's Health Information
  http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm

- Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs
  http://www.privacy.gov.au/law/other/medical/review
  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.

- Health Information Privacy Code
  http://www.privacy.org.nz/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.

- Office of the Privacy Commissioner (New Zealand) Health Brochure
  http://www.privacy.org.nz/brochure-for-health-consumers
  Provides information for health consumers about their rights under the Health Information Privacy Code.

- Guidelines for Agreements Between Trustees and Information Management Service Providers
  http://www.health.gov.sk.ca/adx/aspx/adxGetMedia.aspx?DocID=292,94,88,Documents&MediaID=134&Filename=health-agreement-guideline-final.pdf
  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.

- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
  Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak | European Data Protection Board (europa.eu)

- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
  Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak | European Data Protection Board (europa.eu)

- 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)
  https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Recommendation No.R(97) 5 on the protection of medical data (13 February 1997)
  https://wcd.coe.int/ViewDoc.jsp?id=571075&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)
  https://wcd.coe.int/ViewDoc.jsp?id=589341&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

6.2.3 Human Resources

- Code of Practice on Human Resource Management
  http://www.pcpd.org.hk/english/ordinance/files/hrdesp.pdf

  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 prosprective, current and former employees.

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

- Code of Practice on Human Resource Management: Compliance Guide for Employers and HRM Practitioners
  http://www.pcpd.org.hk/english/ordinance/code_hrm.html
  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.

- Guidelines for personal data protection in employment relationships
  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_Employment.pdf
  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.

- 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)
  https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989)
  https://wcd.coe.int/ViewDoc.jsp?id=710373&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)
  https://wcd.coe.int/ViewDoc.jsp?id=699153&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

6.2.4 Marketing

- Data Protection Good Practice Note - Charities and marketing
  http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/charities_and_marketing_good_practice_note.pdf
  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.

- New Tool Will Help Online Advertisers Develop Stronger Privacy Practices
  http://www.cdt.org/privacy/20090128threshold.pdf
  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.

- Guidelines for the Private Sector - Code of conduct for personal data processing
  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice__kodeks_obnasanja_pri_zbiranju_OP-eng_06.02.2012.pdf
  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).

- 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)
  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)
  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)
  https://wcd.coe.int/ViewDoc.jsp?id=698775&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

6.2.5 Industry non-specific - Privacy policy establishment

- Data protection and privacy guidelines
  http://www.bba.net/bbaarchive/pdf/DataProtectionPrivacyGuidelinesJune2005.pdf
  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.

- 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
  http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec(2012)4_En_Social%20networking%20services.pdf

- Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines
  http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec(2012)3%20E%20-%20Search%20engins.pdf

- Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999)
  https://wcd.coe.int/ViewDoc.jsp?id=407311&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Report of the Group of Experts on Privacy
  http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

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.

6.2.6 Industry non-specific - Trans-border personal data flow

- OECD Privacy Framework
  http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
  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.

- The use of authentication across borders in OECD countries
  http://www.oecd.org/dataoecd/1/10/35809749.pdf
  The purpose of this survey was to:
  - Identify examples of current offerings and actual implementation of authentication across borders.
  - 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).
  - 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.

- APEC Privacy Framework
  http://www.apec.org/en/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx
  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.

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also named as Convention 108)
  http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
  https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

6.2.7 Technology

- Technology-induced challenges in privacy and data protection in Europe
  http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-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.

- Code of Practice on the Identity Card Number and other Personal Identifiers
  http://www.pcpd.org.hk/english/ordinance/code_id.html

- Privacy Features of European eID Card Specifications
  http://www.enisa.europa.eu/pages/02_01_press_2009_02_3_privacy_features_eID.html

  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.

- Privacy and Security Risks when Authenticating on the Internet with European eID Cards
  http://www.enisa.europa.eu/act/it/eid/eid-online-banking/at_download/fullReport

  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.

- Smartphones: Information security risks, opportunities and recommendations for users
  http://www.enisa.europa.eu/act/it/oar/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.

- Guidelines - Cloud computing and data protection
  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf
  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.

- Guidelines - Guidelines for developing information solutions
  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_razvoj_informacijski_resitev_ENG.pdf
  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.

- Guidelines for De-identification of Personal Data
  https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjopfLw9dTjAhXRyosBHQcBDogQFjAAegQIAhAC&url=https%3A%2F%2Fwww.privacy.go.kr%2Fcmm%2Ffms%2FFileDown.do%3FatchFileId%3DFILE_000000000827254%26fileSn%3D0&usg=AOvVaw2TwDsWt5IPNAJQdUcNLseK
  The guidelines for De-identification of personal data was published under the joint leadership of the Korean government including the Office for Government Policy Coordination, the Ministry of Interior, the Korea Communications Commission, the Financial Services Commission, the Ministry of Science, ICT and Future Planning, and the Ministry of Health and Welfare to provide clear standards on de-identification of personal data and scopes on utilizing de-identified data for the safe use of big data within the current legal boundary of personal data protection. By doing so, we aim to reduce uncertainties that businesses have in order to encourage corporate investment and industry

- CNIL : Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »
  https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf

- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation
  Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation | European Data Protection Board (europa.eu)

- Guidelines 08/2020 on the targeting of social media users
  Guidelines 08/2020 on the targeting of social media users | European Data Protection Board (europa.eu)

- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
  Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications | European Data Protection Board (europa.eu)

- Guidelines 02/2021 on Virtual Voice Assistants
  Guidelines 02/2021 on Virtual Voice Assistants | European Data Protection Board (europa.eu)

6.2.8 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 l998 (the "l998 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):

- http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx

- **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
Resource cost: Free
***Resource type(s)**:* Document(s)
Resource URL(s):

- http://www.ipc.on.ca/images/Resources/video-e.pdf

- **Guidelines for Using Video Surveillance Cameras in Schools**

These *Guidelines* recognize that modified expectations ofprivacy exist in schools. In contrast to public places, schools are considered to be a supervisedenvironment where a reasonable degree of monitoring by school staff is both desirable andexpected. A comprehensive surveillance system in a school, however, has the potential ofbeing privacy-invasive. These *Guidelines* were created to assist school boards intending touse video surveillance to introduce these programs in a manner that ensures stringent privacycontrols.

***Author(s)**:* Information and Privacy Commissioner Ontario
***Keyword(s)**:* CCTV, Surveillance, Schools
Resource cost: Free
***Resource type(s)**:* Document(s)
Resource URL(s):

- https://ozone.scholarsportal.info/bitstream/1873/6065/1/10317630.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):

- http://www.oipc.bc.ca/advice/VID-SURV(2006).pdf

- **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):

- https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_videosurveillance_eng.pdf

- Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation
  Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation | European Data Protection Board (europa.eu)

6.2.9 Public privacy awareness

- OnGuard Online
  http://www.onguardonline.gov/
  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.

- Privacy Today
  http://www.privacyrights.org/ar/Privacy-IssuesList.htm
  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.

- Secure your computer to protect your privacy
  http://www.privacyprotection.ca.gov/res/docs/pdf/Secure_Computer_Protect_Privacy_Speaker_Notes.pdf
  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.

- Privacy Breach Guidelines (New Zealand)
  http://privacy.org.nz/privacy-breach-guidelines-2/
  Provides guidance from the New Zealand Privacy Commissioner about steps agencies should take when a privacy breach occurs. The guidelines are voluntary.

- 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)
  https://wcd.coe.int/ViewDoc.jsp?id=529167&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

- Teen privacy online
  - http://issuu.com/mdwcollins/docs/teenprivacyonline_slides
  - http://dataprivacyday2010.org/wp-content/uploads/2009/07/Teen-Privacy-Online-09.ppt

  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.

- Guidelines - Being an informed consumer – who is allowed to handle my personal data and why?
  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Informed_consumers_eng_05.02.2012_.pdf
  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.

- 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

- Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987)
  https://wcd.coe.int/ViewDoc.jsp?id=704881&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

6.2.10 Privacy accreditation

- PrivacyMark System
  http://privacymark.org/
  The PrivacyMark System which is a system set up to accredidate private organisations that take appropriat 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]).

- DSCI Privacy Framework (DPF©)
  http://www.dsci.in
  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.

- ISMS-P(Personal Information & Information Security Management System)
  https://isms.kisa.or.kr/main/ispims/notice/?boardId=bbs_0000000000000014&mode=view&cntId=9

  ISMS-P is a certification system put in force in Korea, which awards a company who achieves a certain degree of performance in the systematic and persistent activities in terms of information security and personal information protection.

  The certification for the personal information management system (PIMS) was initially started in 2010 based on the "Act on Promotion of Information and Communications Network Utilization and Data Protection, etc". It was incorporated into the ISMS-P in 2018 based on both the "Act on Promotion of Information and Communications Network Utilization and Data Protection, etc" and "Personal information Protection Act". The ISMS-P is to address two certification schemes: Information security management system and Personal information management system.

  Korea Internet/ Security Agency, https://www.kisa.or.kr/eng/main.jsp

  Legal ground: Personal Information Protection Law, Article 32-2 (Certification of Personal Information Protection) below:

  (1) The Protection Commission may certify whether the data processing and other data protection-related action of a personal information controller abide by this Act, etc.

  (2) The certification provided for in paragraph (1) shall be effective for three years.

(3) In any of the following cases, the Protection Commission may revoke the certification granted under paragraph (1), as prescribed by Presidential Decree: Provided, That it shall be revoked in cases falling under subparagraph 1:

1. Where personal information protection has been certified by fraud or other unjust means;
2. Where follow-up management provided for in paragraph (4) has been denied or obstructed;
3. Where the certification criteria provided for in paragraph (8) have not been satisfied;
4. Where personal information protection-related statutes are breached seriously.

(4) The Protection Commission shall conduct follow-up management at least once annually to maintain the effectiveness of the certification of personal information protection.

(5) The Protection Commission may authorize the specialized institutions prescribed by Presidential Decree to perform the duties related to certification under paragraph (1), revocation of certification under paragraph (3), follow-up management under paragraph (4), management of certification examiners under paragraph (7).

(6) Any person who has obtained certification subject to paragraph (1) may indicate or promote the certification, as prescribed by Presidential Decree.

(7) Qualifications of certification examiners who conduct the certification examination subject to paragraph (1), criteria for disqualification, and other related matters shall be prescribed by Presidential Decree, taking into account specialty, career, and other necessary matters.

(8) Other necessary matters for the certification criteria, method, procedure, etc. subject to paragraph (1), including whether the personal information management system, guarantee of data subjects' rights, and measures to ensure safety are based on this Act, shall be prescribed by Presidential Decree.

- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
  Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board (europa.eu)

6.2.11 Identification for development

- Identification for Development (ID4D) Global Dataset
  https://datacatalog.worldbank.org/sites/default/files/dataset_resources/ddhfiles/public/WB_ID4D_Dataset_2018_0.xlsx
  The ID4D Global Database, compiled by the World Bank Group's Identification for Development (ID4D) initiative, provides a global estimate for the number of individuals without proof of legal identity.

  This document presents:
  1. Quantitative data on the number of individuals without access to proof of legal identity split by country, region, and income level;
  2. Qualitative data on the entities charged with identification & civil registration (CR); the status of enabling legal and regulatory frameworks; and ICT, e-government, and poverty indices to allow for additional analysis.

7. Relationships between laws, standards and guidelines

7.1 Terminology

7.1.1 General

The relationships between terminology used in specific privacy-related standards produced by ISO/IEC JTC 1/SC 27 and terminology used more generally are explained. This is intended to assist in understanding both the ISO/IEC standards themselves and the wider subject areas, and how they relate.

7.1.2 Data de-identification terminology

General

Clarification is provided on how the terminology used in ISO/IEC 20889:2018 (*Privacy enhancing data de-identification terminology and classification of techniques*) relates to terms being used in prior art. ISO/IEC 20889 reuses prior terminology wherever it has been defined and used consistently. However, in some cases the definitions in ISO/IEC 20889 are not always identical to earlier definitions because the prior art sometimes uses terminology inconsistently and not in accordance with the state of the art; the terms used in ISO/IEC 20889 have been formulated to capture the latest understanding in the field of data de-identification, and avoids using terms that have been used inconsistently in prior art as discussed below.

The prior art tends to entangle technical de-identification techniques with technical and other organizational measures implemented to enhance the effectiveness of de-identification. The terminology defined in ISO/IEC 20889 has been designed to allow the discussion of de-identification to be distinguished from technical and other organizational measures, and as a result permits ISO/IEC 20889 to focus on de-identification techniques.

ISO/IEC 20889 does not use the term “reversible” or its derivatives (i.e. irreversible, reversibility, etc.) because this term has been used to denote organizational measures being taken to allow or disallow controlled re-identification (as shown in Table 1 below) as well as to describe mathematical properties of transformation functions (e.g. of cryptographic hash-functions).

ISO/IEC 20889 also does not use the term “anonymize” or its derivatives (i.e. anonymisation, anonymization, anonymised, anonymized, anonymous, anonymity, etc.) because the term has been used in the past to convey a range of different meanings, as shown in Table 1 below.

Table 1: Mapping of de-identification terminology to the prior art

Term used in this document	ISO 25237[27]	ISO 29100[29]	ICO 2012[20],	Article 29 2014[1],
De-identification	De-identification, Anonymization	Anonymization	Anonymisation	N/A
Masking	N/A	N/A	Anonymisation	N/A
Pseudonymization with controlled re-identification	Pseudonymization reversible	Pseudonymization	Anonymisation	Pseudonymisation
Pseudonymization without controlled re-identification	Pseudonymization irreversible	Anonymization	Anonymisation	Pseudonymisation
Randomization	N/A	N/A	Anonymisation	Anonymisation
Generalization	N/A	N/A	Anonymisation	Anonymisation
Differential Privacy	N/A	N/A	N/A	Anonymisation

N/A Not applicable.

ISO/IEC 19944 versus ISO/IEC 20889

Table 2 shows how the privacy enhancing de-identification techniques described in ISO/IEC 20889, when used to process data containing PII, can result in a state of data characterized by one or more of the data identification qualifiers listed in ISO/IEC 19944.
NOTE Use of the techniques listed in this table are not the only way of achieving the data identification states described by the qualifiers.

Table 2: Mapping between ISO/IEC 19944 and ISO/IEC 20889 terminology

ISO/IEC 19944 data identification qualifiers describing state of data	ISO/IEC 20889 Privacy enhancing data de-identification techniques whose application leads to the corresponding state of data
Identified data	original, unprocessed data containing identifiers; in other words, no de-identification techniques are applied yet; for the other qualifiers, the identifiers are removed (masked)
Pseudonymized data	data processed using pseudonymization techniques with controlled re-identification possible/implemented
Unlinked pseudonymized data	data processed using pseudonymization techniques with no controlled re-identification allowed
Anonymized data	data processed using generalization and/or randomization techniques
Aggregated data	data processed using aggregation techniques

Relationship to Statistical disclosure control terminology

Statistical Disclosure Control (SDC) [also known as Statistical Disclosure Limitation (SDL)] is a discipline that was originally developed for controlling the disclosure risk when publishing census and survey data. Subsequently, SDC has been applied to other, similar, use cases, such as the publication of health records and medical statistics. As such, SDC significantly contributed to the broader practice of data de-identification, which is the focus of ISO/IEC 20889. Many SDC techniques are, in fact, de-identification techniques and are included in ISO/IEC 20889.
Since the establishment of SDC, both refinements to known de-identification techniques and new de-identification models have been developed to address additional use cases for data de-identification. As a result, new terms, rooted in additional disciplines, have been introduced to the field of data de-identification. ISO/IEC 20889 normalizes the resulting general-purpose terminology, which has become the predominantly used terminology across a range of industries and academia.
In some cases, the terminology used in ISO/IEC 20889 overlaps with SDC terminology. Table 3 below lists cases where a simple mapping is possible.

Table 3: Mapping to SDC terminology

Terminology in ISO/IEC 20889	SDC terminology
Attribute	Variable
Attacker	(Data) Intruder
Data usefulness	Data utility
Generalization	Global recoding
Indirect identifier	Key variable

In addition, in some cases similar terminology is used to refer to different concepts as described below.

In SDC, the term “tabular data” (also known as “aggregate tabular data” or “aggregate data”) refers to the practice of creating (and subsequently publishing) tables solely containing statistics about the original values of the attributes, such as frequency count table. In this document, the terms “aggregation” and “aggregated data” refer to statistical computations on the original data, neither implying the format nor specifying the means to access the resultant computations.
The term “tabular” is not used in ISO/IEC 20889 to avoid confusion between its specific meaning in the field of statistical disclosure control and its English meaning of “in a structured form”.
[Sections 7.1.3, 7.1.4, etc. should be added as and when suitable text becomes available.]

7.2 Privacy information management

7.2.1 General

Privacy regulations have seen a remarkable growth over the last decade; many jurisdictions now regulate the gathering, storage and use of personal data to try to protect the privacy of citizens. However, this plethora of law and regulation poses businesses operating internationally with a major problem. Such organizations will clearly need to ensure compliance with the laws and regulations governing the handling of personal data in all the countries in which they operate. However, each jurisdiction imposes slightly different requirements, so ensuring and demonstrating compliance can become extremely complex.
Similar problems arise when establishing contractual relationships between businesses, if the contracts cover services involve the processing of personal data. For example, if a cloud service provider undertakes to process data which include personal data on behalf of a client, then this client must take steps to ensure that this third-party processing of personal data meets its legal obligations. That is, the contract must be drafted to reflect the laws and regulations applying to the client. Moreover, the client must also take due diligence to ensure that the cloud provider will perform its processing with appropriate care; in principle this could, for example, require the client to conduct an audit of the security and other provisions put in place by the cloud service provider.
It is thus clear that the multiplicity of regulatory requirements applying to personal data imposes a number of serious problems for business. In particular organizations using third party services will need to ensure that the contracts for these services ensure the client's legal obligations are met, and assurance in the security of the service provider is obtained. Also, organizations operating in multiple regulatory regimes will need to ensure that they are compliant with the rules applying in every jurisdiction in which they operate, and that they can demonstrate to clients that they are compliant with the appropriate set of rules.
Of course, international standards have a somewhat different role to regulations as they are voluntary. To quote the ISO website[1], “Standards are voluntary agreements, developed within an open process that gives all stakeholders, including consumers, the opportunity to express their views and have those views considered. This contributes to their fairness and market relevance, and promotes confidence in their use.”
One way in which these standards can help address the privacy regulation challenges are through detailed mappings from individual pieces of legislation and regulation to the provisions of standards. These mappings will need to explain, for any particular piece of legislation or regulation, exactly which requirements are met by conformance to a standard, and which remain to be addressed. This is, of course, only the first step in realising the benefits of standardisation --- mapping is not enough in and of itself, and there is also a key role for the regulators.
Here mappings are provided from ISO/IEC 27552 to specific piece of legislation worldwide.

7.2.2 Mapping ISO/IEC 27701 to GDPR

This annex gives an indicative mapping between provisions of this document and Articles 5 to 49 except 43 of the General Data Protection Regulation of the European Union. It shows how compliance to requirements and controls of this document can be relevant to fulfil obligations of GDPR.

However, it is purely indicative and as per this document, it is the organizations responsibility to assess its legal obligations and decide how to comply with them.

[1] https://www.iso.org/sites/ConsumersStandards/1_standards.html

Table 4 — Mapping of ISO/IEC 27701 structure to GDPR articles

Subclause of this document	GDPR article
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)
6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)
6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)

6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)
7.3.3	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c), (5)(1)(e)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)
7.4.8	(5)(1)(f)
7.4.9	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)

8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)
8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)
8.5.8	(28)(2)

[Sections 7.2.3, 7.2.4, etc. should be added as and when text mapping ISO/IEC 27552 to other privacy regulations becomes available.]

8 Privacy-related bodies

8.1 Newsletters and forums

- Daily Dashboard
  https://www.privacyassociation.org/publications/daily_dashboard/
  The Daily Dashboard summarizes the day's top stories with links to the full articles…sent direct to your desktop each weekday.

- Center for Democracy and Technology
  http://www.cdt.org
  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.

- Privacy Law & Business International Newsletter
  http://www.privacylaws.com/templates/Enews.aspx?id=307
  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.

- E-commerce Law Week by Steptoe and Johnson
  - http://www.steptoe.com/publications.html
  - http://www.steptoe.com/publications.html

  This global law firm publishes a free weekly newsletter that discusses electronic commerce issues and new law developments including privacy.

- Privacy Exchange
  http://www.privacyexchange.org/
  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.

- BNA Privacy Law Watch and Privacy and Security Report
  http://www.bna.com/products/corplaw/pvln.htm
  Produced daily or weekly, these reports provide notification of current events and articles analyzing those events by attorneys and reporters on primarily US issues.

- Alston & Bird International Privacy Library
  http://resource.alston.com/abResourceCenter/resource_overview.aspx?s=3
  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.

- Tech Law Journal
  http://www.techlawjournal.com
  News, records, and analysis of legislation in USA, litigation, and regulation affecting the computer, internet, communications and information technology sectors.

- Private Word
  http://www.privacy.org.nz/private-word
  A quarterly newsletter which provides information on relevant local privacy issues and also brief casenotes of recent investigations by the Office.

- International Journal of Information Security and Privacy
  http://www.igi-global.com/journal/international-journal-information-security-privacy/1096

- Journal of Privacy and Confidentiality
  http://repository.cmu.edu/jpc/

8.2 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
    - ✓ http://www.privacy.gov.au/aboutus/international/appa

- 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

- 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/

- 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

- 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
    - ✓ http://www.ponemon.org/

- 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/

- 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
    - ✓ Articles
    - ✓ Comprehensive Data Breach Tracking
  - Website
    - ✓ http://www.privacyrights.org/

- 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/

- 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

- **Global Privacy Assembly (GPA)**
  The Global Privacy Assembly first met in 1979 as the International Conference of Data Protection and Privacy Commissioners. The Assembly has been the premier global forum for data protection and privacy authorities for more than four decades. The Assembly seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe.

  - *Deliverables*
    - ✓ Resolutions and declarations
    - ✓ Statements
    - ✓ Report
    - ✓ Communiqués and newsletters

- ✓ Annual conference

- o *Website*
  - ✓ https://globalprivacyassembly.org/

8.3 Privacy related research 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.

  - o Deliverables
    - ✓ PRIME Framework V2

  - o Website
    - ✓ https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.b_ec_wp14.1_V1_final.pdf