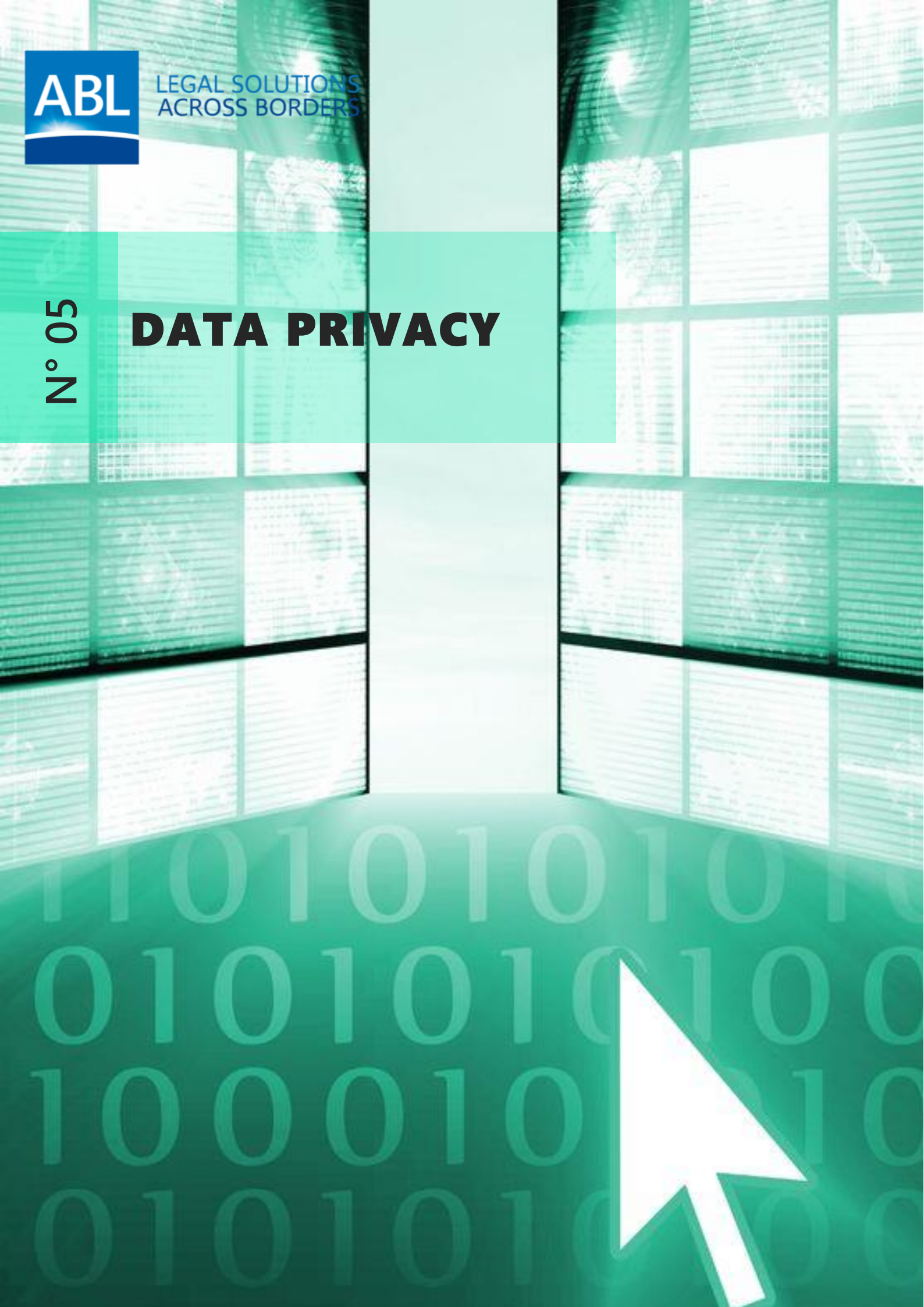
ABL

LEGAL SOLUTIONS
ACROSS BORDERS

N° 05

# DATA PRIVACY



# CONTENTS

## LIST OF CONTRIBUTORS

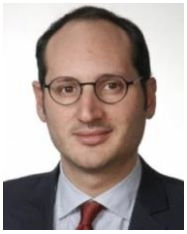
### INDIA

**Ryan Locke**

MMB Legal
Bangalore

Send Email

### ITALY



**Sala Tommaso**

Franzosi Dal Negro Setti
Milan

Send Email

### ITALY

**Chiara Brighenti**

Franzosi Dal Negro Setti
Milan

Send Email

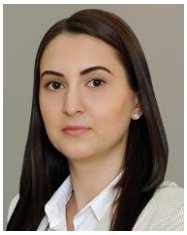
### ITALY

**Pasquale Di Mino**

Franzosi Dal Negro Setti
Milan

Send Email

### ROMANIA



**Roxana Constantin**

Ionescu si Sava
Bucharest

Send Email

### SPAIN

**Jorge Salvador Rebolleda**

MG Abogados
Madrid

Send Email

### SWEDEN

**Valerie Moshiri**

Salmi & Partners
Stockholm

Send Email

### SWITZERLAND

**Blaise Krähenbuhl**

DGM Avocates
Geneva

Send Email

## LIST OF CONTRIBUTORS Continued

### UNITED KINGDOM

**Claire Rigby**

Druces LLP
London

Send Email

## EXECUTIVE SUMMARY

Welcome to the fifth Report of the ABL's Young Lawyers Group ("the Group").

The Group was formed in 2015 to enable young lawyers in ABL member firms to develop and work alongside the senior members of ABL and to contribute towards the continued success of ABL. As such, the Group aims to enable young lawyers to build up their own network of contacts within ABL and to develop their own legal education through the publication of reports on topical issues chosen by the Group's members on ABL's website, members' own firm websites and the ABL Insider.

The topic of "Data Privacy" is of particular interest and was chosen as the Group's fifth Report given the international work that member firms are involved with.

The Report draws attention upon the distinctive trait of the Privacy legislation in each country mentioned in this Report.

The Report was prepared with contributions from seven members of the Group from India, Italy, Romania, Spain, Sweden, Switzerland and the UK. A link to the individuals' biographies can be found on the "List of Contributors" page.

**Claire Rigby**

Druces LLP, London

Member and Chair of the Young Lawyers Group

# India

**Introduction**

As of today, India does not have an exclusive data protection legislation and our courts have, over time, entwined the concept of privacy with the interpretation of right to life and personal liberty as provided under Article 21 of the Constitution of India. However, it is through the Information Technology (Amendment) Act of 2008 which was passed in the year 2009, that for the very first time, there was the provision for express inclusion of certain sections, primarily Sections 43A and 72A of the Information Technology Act, 2000 ("**Act**") that exclusively deal with matters of data privacy and penalties for breach therein. These provisions are complemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Rules**").

A press note[1] ("**Press Note**") was released by the Ministry of Communications and Information Technology, Government of India on August 24, 2011 in order to clarify the intention of the Rules. The Press Note clarified several provisions of the Rules, including the applicability of certain provisions of the Rules to players in the outsourcing industry. The clarification appears to confirm the general view that the Rules were unlikely to have extra-territorial application (i.e. application to data imported into India). Further, the clarification appears to limit the application of the Rules to body corporates in India.[2] The Press Note also clarifies that Section 5 (Collection of information) and Section 6 (Disclosure of information) of the Rules are not applicable to a body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under a contractual obligation with any legal entity located within or outside India.

**Provisions dealing with Data Privacy and Penalties within the Information Technology Act, 2000**

1) **Section 43A:** The primary focus of this section is providing compensation in cases where negligence is proved in relation to executing and preserving reasonable security practices and procedures in relation to sensitive personal data or information.

This section states that where a body corporate[3], possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable

[1] http://pib.nic.in/newsite/erelcontent.aspx?relid=74990.
[2] *Ibid*.
[3] The explanation to Section 43A of the Information Technology Act, 2000 states that a "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

The Rules have clearly identified certain information that qualifies as sensitive personal data or information. The Rules[4] state that "sensitive personal data or information of a person" means such personal information which consists of information relating to: (i) passwords; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to a body corporate for providing service; and (viii) any of the information received under the above clauses by a body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these Rules.

The implication of this section for entities doing business in India is that they will now have to review their contractual arrangements thoroughly in order to ensure that their data security practices and procedures are at par with those that are stipulated under the law.

Section 43-A of the Act mandates following of reasonable security practices and procedures in relation to sensitive personal data or information. There are stipulated standards that are mentioned under the Rules that may be implemented by a body corporate. However, industry associations and entities are permitted under Rule 8 of the Rules to follow other standards provided that such standards are notified and approved by the Government of India. Body corporates which have used such stipulated standards need to get the same certified or audited by an independent, government approved auditor, as mentioned under Rule 8 of the Rules. Further, there need to be yearly audits conducted when there is a significant upgradation of processes or computer resources. In addition to these practices and procedures, the Rules also contain express mandates on the collection and transfer of sensitive personal data or information, including in relation to disclosure to third parties, privacy policies and appointment of a grievance officer by every body corporate.

2) **Section 72A:** This section mandates punishment for disclosure of "personal information" in breach of lawful contract or without the information provider's consent. This section states that "save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence,

[4] Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

3) Apart from the aforementioned two sections which are directly aimed towards data privacy there are also certain sections of the Act that indirectly have data privacy implications; those sections being Sections 65, 66 and 66E of the Act which cumulatively state that the act of tampering and hacking computer systems with the knowledge or intention of the same is an offence which is subject to the prescribed punishment.

**Conclusion**

It is particularly encouraging that the judiciary in India has been pro-active in formulating stricter and more efficient standards when it comes to data privacy issues. The judiciary has opined that trustees of customer data must be judged on tough standards and has made clear that defaulting entities shall be held liable[5]. The involvement of the state in data protection ensures stricter policies and makes clear how seriously data protection is taken. Hopefully in the near future India will have detailed laws with respect to data protection.

[5] Internet and Mobile Association of India & Anr. v. Union of India & Anr., W.P. (C) No. 758/2014.

# Italy

## Introduction

Italy's consolidated data protection code (the "**Code**") came into force on January 1, 2004. The Code brings together all the various laws, codes and regulations relating to data protection since 1996, superseding the Data Protection Act 1996 (no. 675/1996) and implementing Directive 95/46/EC on data protection ("**Data Protection Directive**"). The three key guiding principles behind the Code are *simplification*, *harmonisation* and *effectiveness*.

The Code is divided into three parts:

- 1st sets out the general data protection principles that apply to all organisations;
- 2nd provides additional measures that will need to be undertaken by organisations in certain areas (eg. healthcare, telecommunications, banking and finance, or human resources;
- 3rd relates to sanctions and remedies.

## Personal Data

Any information concerning natural persons that are or can be identified also by way of other items of information – e.g., via a number or an ID code.

For instance, personal data is one's first or last name, address, Tax ID as well as a picture, the recording of one's voice or one's fingerprint, or medical, accounting or financial information relating to that person.

## Data Controller, Data Processor and Data Subject

The Code defines the different subjects entitled to manage the collected data in different ways:

a) "*Data subject*": the natural person a personal data relates to.

b) "*Data processor*": is the natural person, company, association or organization the Data Controller has entrusted with specific data processing management and control tasks on account of the relevant experience and/or skills.

c) "*Data Controller*": is the natural person, company, association or other entity that is factually in control of the processing of personal data and is empowered to take the essential decisions on the purposes and mechanisms of such processing including the applicable security measures. If personal data is processed by a company or a public administrative body, it is the entity as a whole that acts as the data controller rather than the individual or department/unit that manages or represents such entity (e.g. Chairperson, CEO, auditor, Minister, Director General, etc.). The cases where an individual is the data controller mostly concern processing operations performed by self-employed professionals or single-person corporations.

The Data Controller has to submit a notification to the enforcement authority before the commencement of certain kinds of personal data processing. A Data Controller must provide the fair processing information to data subjects and must also provide information about: (i) whether

the supply of data is mandatory or voluntary; (ii) the possible consequences of refusal to consent to the data processing; (iii) the (categories of) entities to whom the data may be communicated or which may have access to the data as data processors or persons in charge of the processing; (iv) their rights as data subjects; and (v) the name and address of the Data Controller and the Data Processor.

**The Code Principles**

Personal data must be processed with respect for the data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection.

Information systems and software must be configured by minimising the use of personal data and identification data. This must be done in a way that prohibits their processing if the purposes for processing can be achieved by using either anonymous data or providing suitable arrangements to allow the identification of data subjects only in necessary cases.

**Rights of Individuals**

Under the Code, every Data Subject has various rights in connection with the processing of their personal data (see Section 7 of the Code):

1. the right to obtain general information on processing operations performed in our country by accessing, free of charge, the online Register of Processing Operations kept by the Code;
2. the right to access their own personal data directly at the entity holding such data (the Data Controller), i.e. the right to obtain confirmation that such data exists and communication of the data as well as to know the source of the data and what criteria and purposes apply to its processing. In the latter case the Data Controller may charge a fee ("handling fee") if it is found that no data relating to the data subject is held;
3. the right to obtain erasure or blocking of any data that is processed in breach of the law, for instance because no consent was asked for. This right may also be exercised if there is no valid reason any longer for retaining data that had been collected lawfully;
4. the right to have inaccurate and/or incomplete data updated, rectified or supplemented;
5. in the cases mentioned under 3. and 4. above, the right to obtain confirmation from the Data Controller that the above operations have been also made known to the entities the data had been communicated to beforehand, unless this proves impossible or requires a disproportionate effort compared to the right to be protected;
6. the right to object to the processing of one's own data on legitimate grounds;
7. the right to object, in any and all cases, to the processing of one's own data for commercial information purposes and/or for sending advertising or direct selling materials and/or for market research purposes.
8. Data Subjects have a right to compensation which includes pecuniary and non-pecuniary damage that can be requested from the Civil Courts.

**Data Protection Authority**

The Italian Data Protection Authority ("***Garante***"), is an administrative independent authority, that ensures the protection of fundamental rights and freedoms as regards the processing of personal

data along with respect for individuals' dignity. The *Garante* handles citizens' claims and reports and supervises over compliance with the provisions protecting private life. It decides on complaints lodged by citizens and is empowered to prohibit, also of its own motion, any processing operation that is unlawful or unfair. It can perform inspections, impose administrative penalties, and issue opinions in the cases mentioned by the Code. It can also draw Parliament's and Government's attention to the desirability of regulatory measures concerning personal data protection.

**Future Developments**

On April 14, 2016 the European Parliament adopted:

1) General Data Protection Regulation - Regulation EU 2016/679 ("**GDPR**")

While the GDPR entered into force on May 24, 2016, it shall apply from **May 25, 2018**. The GDPR will replace the Data Protection Directive and will be directly applicable in all Member States without the need for implementing national legislation. The GDPR updates and modernises the principles enshrined in the Data Protection Directive to guarantee privacy rights, giving people more control over their personal data. It focuses on:

- reinforcing individuals' rights;
- strengthening the EU internal market;
- ensuring stronger enforcement of the rules;
- streamlining international transfers of personal data; and
- setting global data protection standards.

2) Directive EU 2016/680 ("**Directive**")

It entered into force on May 5, 2016 and EU Member States have to transpose it into their national law by **May 6, 2018**. The Directive rules 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.

# Romania

**Legal framework**

In Romania, processing of personal data is regulated by the following three important laws, which are transposing the European Union regulations into the national legislation:

1. Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which implements the provisions of Directive 95/46/EC;
2. Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, which implements the provisions of Directive 2002/58/EC; and
3. Law no. 305/2002 on electronic commerce, which implements Directive 2000/31/EC.

**General information**

The main objective of data privacy legislation is to guarantee and protect the fundamental rights and freedoms of individuals, in particular the right to intimate, family and private life.
Due to the digitalization of everyday life, protection of personal data became a globally hot topic. Whether an individual goes online for opening a bank account, purchasing any type of goods, applying for a job or giving its contact details for marketing purposes, his personal data is processed by public or private entities.

**Scope of data privacy legislation**

The Romanian data privacy legislation applies to any data processing operation performed by controllers established in Romania, by diplomatic missions or consular offices of Romania or by controllers who are not established in Romania, but they use means of any kind located on the territory of Romania, unless such means are used only for the purpose of transit through Romania of the personal data subject to such processing.
A controller is defined both by the European Union legislation and by the Romanian legislation as being any individual or legal person, either public or private entity (e.g. a bank, a foundation, a company), which determines the purpose (e.g. marketing, recruitment, financial evidence) and means of processing of personal data (e.g. a website, an application, a software).
The Romanian legislation stipulates that a controller which is not established in Romania must appoint a representative established on the Romanian territory in order to represent the foreign operator and to keep in touch with the national competent authority in respect to the processing of personal data in Romania.

**Rights of individuals**

Both the European Union legislation and the Romanian legislation provide that the individual whose personal data is processed must be informed at least of the following: the controller's identity, the scope of processing the personal data, the recipients of such information and the rights of the individual with regard to personal data processing.

In respect to the processing of his personal data, the law guarantees the individual the following rights:

- right of access, which in Romania can be exercised on request and free of charge, once a year, by transmitting a notice to the controller, which must respond to the individual if it is processing or not his personal data;
- right of intervention, under which the individual can request the controller to rectify, update, block, delete and transform into anonymous data its personal data;
- right to object, by which the individual can object to the processing of his personal data, in the vast majority of cases;
- right not to be subjected to an automated individual decision, under which the individual can request the withdrawal, cancellation or reassessment of any decision taken based on an automated processing of his personal data;
- right to appeal to justice, for the protection of any rights guaranteed by the law, which have been violated.

**Competent authority**

The Romanian competent authority with the supervision of processing of personal data is the National Supervisory Authority for Personal Data Processing. To this authority must be submitted, before any processing operation, the registration notification as personal data operator by any individual or legal entity who intends to process in Romania the personal data of individuals.

**Notification of the competent authority**

Before December 2015, any natural or legal person who intended to process the personal data of individuals in Romania had to notify the national competent authority in order to register as controller for the purposes set by the latter.

On December 14th, 2015, the President of the Romanian Supervisory Authority for Personal Data Processing issued Decision 200/2015, whereby the situations under which the notification of the national competent authority is required were limited, except for the following, per example:

- processing of personal data relating to racial or ethnic origin, political, religious, philosophical or similar beliefs, trade union membership or health and sexual life (e.g. in case of surveys and market research);
- processing of genetic and biometric data (e.g. in case of scientific research);
- processing of data which allow, directly or indirectly, the geographical location of individuals by means of electronic communications (e.g. in case of monitoring/security of people and/or public/private assets by using GPS);
- processing of personal data by video surveillance systems (except in case of processing by an individual for personal use through a surveillance system that captures images including public spaces);

- processing of personal data of minors in the framework of direct marketing activities;
- transfer of personal data to states located outside the European Union, the European Economic Area, as well as to states to which the European Commission has not recognized an appropriate level of protection by decision.

**Sanctions**

The omission by any controller to notify the national competent authority in respect to processing of personal data in Romanian represents contravention and it is sanctioned with fine in amount of 5,000,000 RON up to 100,000,000 RON.

Processing of personal data with the non-compliance of the Romanian legal provisions is sanctioned as well, with a fine in amount of 10,000,000 RON up to 250,000,000 RON.

Also, non-fulfillment of legal obligations regarding the implementation of the security measures and confidentiality of the processing represents contravention, if it is not committed in such a way as to be considered a crime, and it is sanctioned with a fine from 15,000,000 RON to 500,000,000 RON.

**Regulation (EU) 2016/679 - Implications in Romania**

The new European Union Regulation on General Data Protection (GDPR), which entered into force on May 25, 2016 and will be directly applicable in all Member States starting with May 25, 2018, will surely lead to some amendments of the national applicable legislation, particularly with regard to the competences of the national authority responsible for data processing supervision, new rights of the individual whose personal data is processed and new obligations of the controllers, especially in respect to appointing a data privacy officer.

# SPAIN

## Regulation

The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data.

The Regulation developing the Data Protection Act was approved by Royal Decree 1720/2007 of 21 December (Data Protection Regulations).

There are no sector-specific laws regulating the processing of personal data, but there are regulations that contain specific provisions on personal data processing (Law 26/2006 on insurance and reinsurance intermediation). The most relevant regulations are the:

- Spanish Information Society Services Act (Law 34/2002 on information society services and e-commerce).
- Spanish General Telecommunications Act (Law 9/2014).

In addition, specific legal provisions apply to the processing of:

- Files regulated under the electoral regime legislation.
- Files used exclusively for statistical purposes and protected by legislation on public statistical functions.
- Files for storing data contained in personal classification reports referred to in the armed forces personnel legislation.
- Files derived from the Civil Registry and the Central Registry of Convicts and Fugitives.
- Files from video and audio recordings obtained by law enforcement agencies using video cameras.

## Scope of legislation

The Data Protection Act and the Data Protection Regulations apply to data controllers and data processors.

A data controller is any natural or legal person, whether public or private, or administrative body that makes decisions on the purpose, content and use of personal data processing.

Data processors process data on behalf of data controllers as a result of a relationship that links them. A data processor's scope for action is limited by the service it provides to the data controller.

The Data Protection Act and the Data Protection Regulations apply to personal data recorded on physical media for its processing and subsequent use.

Personal data is any information relating to an identified or identifiable natural person (known as the data subject).

The Data Protection Act and the Data Protection Regulations apply to the processing of personal data.

Data processing means any operation or procedure (whether automated or not) for the collection, recording, storage, elaboration, modification, blocking or erasure of data. It also includes disclosure of data resulting from communications, queries, interconnections or transfers.

The Data Protection Act and the Data Protection Regulations apply to:

- Data processing carried out in the context of the activities of an establishment of the data controller in Spain. Where this is not the case, but the data controller uses a data processor established in Spain, the data processor must comply with the provisions on security measures established in the Data Protection Regulations.
- Data processing carried out by a data controller not established in Spain but in a place where Spanish law applies by virtue of international public law.
- Data processing carried out by a data controller not established in the European Union but using means located in Spain, unless such means are used only for transit purposes. In this case, the data controller must appoint a representative established in Spain.

**Main Data Protection Rules and Principles**

Under the Data Protection Act and the Data Protection Regulations, data controllers must comply with several obligations, including:

- Complying with the principles of data quality.
- Informing data subjects about data processing on collection.
- Obtaining data subjects' consent to process their data.
- Registering personal data files.
- Implementing security measures to protect personal data, including drafting a security document.
- Attending to data subjects' rights of access, rectification, cancellation and opposition.
- Entering into data processing agreements with data processors.
- Keeping personal data confidential.

As a rule, consent from data subjects is required. Consent must be informed. Depending on the circumstances, it can be implied, express (for example, for health data) or written (for example, for data revealing ideology).

Unless the law requires express consent, the Data Protection Regulations establish that data controllers can inform data subjects of the processing they intend to carry out and give them 30 days to oppose it. This way of obtaining consent is subject to limitations (for example, a data controller cannot request the same consent again until a year has passed).

Consent from a parent or guardian is needed for children under 14 years of age.

Data subjects' consent is not required when:

- Data is collected by a public administration when exercising its functions.
- Data refers to the parties to an administrative, employment or business contract or pre-contract, provided the data is necessary for its performance.
- The purpose of the data processing is to protect the data subject's vital interest.
- The data processing is necessary to satisfy a legitimate interest pursued by the data controller (or a third party to whom the data is disclosed), provided that the data subject's fundamental rights and freedoms are not overridden.

**International transfer of data**

International data transfers are transfers to countries whose level of protection has not been declared adequate by the relevant authorities (any country outside the European Economic Area (EEA) with some exceptions). Such transfers must be notified to the Data Protection Agency and authorized by its director, regardless of whether the data importer belongs to the same group as the data exporter.

Authorization can be obtained using the Model Contracts for the transfer of personal data to third countries approved by the European Commission.

The Data Protection Agency must receive the contract and confirm that the parties' representatives have sufficient power to sign it. The Agency has up to three months from the date it receives the request to issue and communicate its decision.

Data Protection Agency authorization is not necessary in the following cases (although it must still be notified of the international data transfer):

- When the transfer results from the application of an international treaty to which Spain is party.
- When the transfer is meant to provide or request international judicial aid.
- When the transfer is necessary for medical prevention or diagnosis, or providing healthcare or medical treatment or for managing healthcare services.
- When the transfer relates to money transfers made according to their specific legislation.
- When the data subject has unequivocally given consent to the data transfer (if the data subject has no real option to oppose the transfer (which is usually the case with employees) consent will not be valid).
- When the transfer is necessary for the performance of a contract between the data subject and the data controller or to adopt pre-contractual measures at the data subject's request.
- When the transfer is necessary to execute or perform a contract concluded or to be concluded, between the data controller and a third party in the interest of the data subject.
- When the transfer is necessary or legally required to protect the public interest.
- When the transfer is necessary for the recognition, exercise or defense of a right in a legal proceeding.

The Data Protection Agency has approved standard contractual clauses that regulate international data transfer from a data processor established in Spain to data sub-processors established in countries whose level of protection is not adequate. In this case, to obtain the Data Protection Agency's authorization, the data processor must also provide the Data Protection Agency with an agreement between the data processor and the data controller under which the latter authorizes the sub-contracting and the international data transfer.

**Enforcement and sanctions**

The Data Protection Agency is responsible for imposing sanctions for non-compliance and it is entitled to inspect data files and request any information necessary to perform its functions. The Data Protection Agency's inspectors can ask to see documents and data and examine them wherever they are located, as well as check out the physical equipment and software used to process data by accessing the premises where it is installed.

Data protection infringements can be classified as:

- **Minor infringements.** These are subject to fines ranging from EUR900 to EUR40,000.
- **Serious infringements.** These are subject to fines ranging from EUR40,001 to EUR300,000.
- **Very serious infringements.** These are subject to fines ranging from EUR300, 001 to EUR600,000.

**Regulator details**

**Spanish Data Protection Agency (Agencia Española de Protección de Datos).**

**Main areas of responsibility.** The Data Protection Agency is the national independent public authority responsible for ensuring compliance with data protection law. The Data Protection Agency's main functions are to interpret, apply and disseminate data protection law, maintain the General Data Protection Registry, safeguard citizens' data protection rights, and authorize international data transfers.

# SWEDEN

This report seeks to draw attention to the principles and regulations of Data Privacy in Sweden.

*"Developments within information technology are accelerating. Technology becomes increasingly powerful, simpler to use and less expensive. This means that it is available to increasing numbers of people. At the same time, it is becoming easier to receive and disseminate data stored on the computer. The facilities for storage and searching for information are becoming increasingly flexible… Developments have meant that technology can be used in a manner that involves an unacceptable intrusion into personal integrity. The individual is entitled to be protected by society against such violations of integrity. At the same time, the need of the individual for protection must be balanced against other fundamental democratic rights and values, for example, freedom of information and freedom of expression. Legitimate needs for using information related to people also exist, for example, for the purpose of social planning…".*[6]

The collection and use of personal data is regulated by the Swedish Personal Data Act (1998:204) (PDA), (*Personuppgiftslagen*)[7].[8] The PDA is based on Directive 95/46/EC[9] which aims to prevent the violation of personal integrity in the processing of personal data.[10]

The PDA act is subsidiary meaning that if another statute or other enactment contains provisions that deviate from this Act, those provisions shall apply.[11] The Freedom of the Press Act or Fundamental Law on Freedom of Expression are perfect examples of when the PDA may be deviated from. Thus, the provisions of the PDA are not to be applied in such way that they might limit the principle of public access to documents or to contravene the provisions concerning the freedom of the press or expression as contained in the Freedom of the Press Act or Fundamental Law on Freedom of Expression. With support of the principle of public access to official documents, it means that the public authorities are liable upon request to provide copies of public documents unless secrecy applies.

---

[6] Ministry of Justice, Personal Data Protection, *Information on the Personal Data Act,* 4th revised edition 2006, available at <http://www.regeringen.se/contentassets/87382a7887764e9995db186244b557e4/personal-data-protection>.

[7] *Amendments to the Act have been taken into account up to SFS 2010:1969. If you wish to learn more about the Act may read the Government Bills 1997/98:44, 1999/2000:11 and 2005/06:173 together with the Standing Committee on the Constitution Report 1997/98:KU18.*

[8] Personal Data Act (1998:204) available at <http://www.wipo.int/edocs/lexdocs/laws/en/se/se097en.pdf>.

[9] **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data., available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.**

[10] Personal Data Act (1998:204) section 1.

[11] Ibid. section 2.

Another law that the PDA partially gives way to is the Official Statistics Act (2001:99).

The Government of Sweden has issued supplementary regulations in conjunction with the PDA in the Personal Data Ordinance (1998:1191) (*Personuppgiftsförordningen*) and the statute book (DIFS) of the Data Protection Authority (DPA) (*Datainspektionen*).[12]

Jurisdictional scope and to whom PDA applies

The PDA applies to controllers[13] who are established in Sweden.[14]

As a main rule, Swedish law is also applicable when a controller from a third country (i.e. a country outside the EU and EEA) uses equipment, for example terminals and questionnaires, situated in Sweden for the processing of personal data. In such cases, the controller must appoint for himself an agent who is established in Sweden. The agent is equated with a controller when applying the PDA.

The PDA does not apply if equipment is only used to transfer information between two countries that are outside the EU and EEA.

It is important to note that when the controller engages an assistant[15] to conduct the processing of personal data, there shall be a written contract that specifically regulates the security aspects. The controller shall also be responsible to ensure that the assistant actually implements the necessary security measures.

If someone who works for the controller discloses personal data in contravention of that provided by the PDA, it is the controller who bears the legal responsibility in relation to the registered person.

Acts that are regulated by the PDA

The PDA applies to such processing of personal data as is wholly or partly performed with the aid of computers.

---

[12] For a full report of the Personal Data Ordinance (1998:1191), Data Protection Authority Statute Book (DIFS) (1998:3) and (2001:1) see following links; http://www.wipo.int/edocs/lexdocs/laws/en/se/se098en.pdf
http://www.datainspektionen.se/Documents/datainspektionen-foreskrifter-1998-3-english.pdf
http://www.datainspektionen.se/Documents/datainspektionen-foreskrifter-2001-1-english.pdf

[13] *Controller of personal data- A person who alone or together with others decides why and how personal data shall be processed. This is usually a legal person; a company, an association, a public authority or a local authority, or a natural person; a businessman.*

[14] Personal Data Act (1998:204), section 4.

[15] *Personal data assistant- A person who processes personal data on behalf of the controller. The assistant may be an independent service provider.*

It also applies to manual registers if these form part of or are intended to form part of a structured collection of personal data that is available to searches or compilations according to specific criteria.[16]

There is no requirement that the information processed as data should be structured in a register or the like. The Personal Data in structured material may only be processed for specific and explicitly stated purposes. It may not later be processed in a manner that is not compatible with that purpose.

Data that is regulated by the PDA

Personal data constitute all kinds of information that is directly or indirectly referable to a natural and physical living person. This may include data which is designated as *sensitive personal data* such as;[17]

- Revealing race or ethnic origin,
- Revealing political opinions,
- Revealing religious or philosophical convictions,
- Revealing membership of trade unions,
- Concerning health or sexual life.

It is prohibited to process personal data and it may only be processed if the registered person has consented *explicitly*. However exemptions from the prohibition of processing sensitive personal data is permitted in cases stated in sections 15-19 of the PDA.[18]

According to section 10 of the PDA, personal data may be processed only if the registered person has given his/her consent to the processing or if the processing is necessary in order

- To enable the performance of a contract with the registered person or to enable measures that the registered person has requested to be taken before a contract is entered into,
- That the controller of personal data should be able to comply with a legal obligation,
- That the vital interests of the registered person should be protected,
- That a work task of public interest should be performed,
- That the controller of personal data or a third party to whom the personal data is provided should be able to perform a work task in conjunction with the exercise of official authority, or
- That a purpose that concerns a legitimate interest of the controller of personal data or of such a third party to whom personal data is provided should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of personal integrity.

[16] Personal Data Act (1998:204), section 5.
[17] Ibid, section 13.
[18] Ibid, section 14.

Sensitive personal data may be processed with the consent of the registered person for research and statistics, provided that the treatment is necessary and provided the public interest in the project manifestly exceeds the risk of improper violation of personal integrity.

The registered person must receive the information necessary to enable him/her to assess the advantages and disadvantages of the processing of personal data concerned. So that the person concerned may exercise his/her rights under the Personal Data Act.

Consent must be voluntary, unambiguous and specific. It must apply to a particular processing concerning the registered person that is performed by a particular controller for a particular purpose.

Consent may be either verbal or in writing.

The registered person can withdraw his or her consent. When a processing is subject to consent, further personal data may not be processed after the registered person has withdrawn his/her consent.

There are various other laws that govern the use of personal data within the public sector as well as sectorial laws, some of which are;

- **Patient Data Act (2008:355) (***Patientdatalag***) and the Pharmacy Data Act (2009:367) (***Apoteksdatalag*
- **Marketing Act (2008:486) (***Marknadsföringslagen***) and the Act on Names and Pictures in Advertising (1978:800) (***Lag om namn och bild i reklam***).**
- **Electronic Communications Act (2003:389) (***Lag om elektronisk kommunikation***)**
- **Camera Surveillance Act (2013:460) (***Kameraövervakningslag***).**

In addition to the Personal Data Act, the Debt Recovery Act of 1974 and the Credit Information Act of 1973 also constitute important legislation, se following links for more information; http://www.datainspektionen.se/in-english/legislation/the-debt-recovery-act/ and http://www.datainspektionen.se/in-english/legislation/The-Credit-Information-Act/.

Summary of the main features of the PDA

• People shall be protected against the violation of their personal integrity by processing of personal data.

• In contrast with the Data Act, the Personal Data Act does not only apply to automated processing of personal data but, in certain cases, also to manual registers.

• The Personal Data Act does not apply to the processing of personal data that forms part of a course of operation of a purely private nature.

• The provisions of the Act are not applicable to the extent that they would contravene the constitutional provisions relating to freedom of the press and freedom of expression or limit the principle of access to public information.
• The Act does not apply, in principle, to journalistic, artistic or literary activities.
• Processing of personal data in unstructured material, for example running text, may take place as long as this processing does not entail a violation of the registered person's personal integrity. Most of the other provisions of the Act shall not be applied to processing of this kind.
• If another act or ordinance contains rules that deviate from the Personal Data Act, those other provisions apply instead.
• The old system with licenses and permits is abolished. Responsibility for ensuring that processing of personal data is conducted in a lawful manner is imposed in the first instance, upon the person processing such data. The Data Inspection Board exercises supervision of compliance with the Personal Data Act.
• The Personal Data Act lists certain fundamental requirements concerning the processing of personal data. These demands include, inter alia, that personal data may only be processed for specific, explicitly stated and justified purposes.
• Personal data may, if these fundamental requirements are satisfied, in principle, only be processed if the registered person gives his or her consent. However, there are several exceptions to this rule, for example, if it is necessary – in the exercise of official powers – when a work task of public importance is to be performed – in order to enable the controller of public data to fulfil a legal obligation – in order that a contract with the registered person may be performed.
• Particularly stringent rules apply to the processing of sensitive personal data – e.g. concerning political views or health. These rules also apply to the transfer of personal data to other countries.
• The registered person is entitled to information concerning processing of personal data that concerns him/her.
• The processing of personal data shall be notified to the Data Inspection Board. However, this does not apply if the person who is responsible for the processing has appointed a personal data representative.
• A person who contravenes the Personal Data Act may be liable to pay damages or be sentenced to a criminal penalty.

# SWITZERLAND

Data Privacy in Switzerland is mainly ruled by the Federal Act on Data Protection (FADP) of 19 June 1992. It applies to the processing of data pertaining to both natural persons and legal persons, by whether private persons or federal administrative bodies. Data protection for the processing of data by the cantonal administrative bodies is ruled by the corresponding cantonal laws.

The Federal Act on Data Protection does however not apply, notably, to personal data processed by a natural person exclusively for personal use if it is not disclosed to the public, to pending civil, criminal or administrative proceedings, except administrative proceedings of first instance.

The main principles are that the data must be processed lawfully, in good faith, in a proportionate manner and protected against unauthorized processing. Furthermore, the persons processing personal data must take all reasonable measures to ensure the accurateness of the data.

According to the purpose specification and limitation principles, personal data may only be processed for the purpose indicated at the time of collection, which must be evident to the data subjects.

The cross-border transmission of personal data from Switzerland is not allowed in the presence of a risk for the data subject's right to privacy, which is the case of a communication of personal data to countries not ensuring a sufficient level of data protection comparable to Switzerland. The Federal Data Protection and Information Commissioner (FDPIC) provides for a list about the level of protection of each country from the Swiss data protection perspective (available at : www.edoeb.admin.ch).

The data subjects have the right to be informed about data concerning him or her being processed and to require the rectification of incorrect data.

As a principle, private persons processing personal data cannot process the data in contravention to the above mentioned principles or process personal data against the data subject's consent without a valid justification, such as an overriding private or public interest or by the authority of law (for example if the processing is in direct connection with the conclusion or the execution of a contract, for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics or if it is relating to persons of public interest, provided that the data relates to the public activities of that person).

A higher level of protection is provided for sensitive personal data (*i.e.* religious, ideological or political views or activities, health, the intimate sphere or the racial origin, social security or administrative or criminal proceedings and sanctions or measures) or personality profiles, such as the obligation to inform the data subject of the collection and data processing.

Data subjects may raise a legal claim against anyone not processing personal data according to the law, in particular request that the data processing be stopped, that no data be disclosed to third parties or that the personal data be corrected or destroyed.

The Federal Data Protection and Information Commissioner notably supervises compliance by federal bodies with the federal data protection legislation, advises private persons on data protection matters, may investigate on data protection matters on his own initiative or at the request of a third party and issue recommendations.

A revision procedure of the Federal Act on Data Protection has been initiated in 2015 in order to take into account the ongoing process of revision of the EU data protection legislation and of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

# UNITED KINGDOM

**Introduction**

The Data Protection Act 1998 (**DPA**) which implemented Directive 95/46/EC on data protection governs the collection and use of personal data in the UK and is enforced by the Information Commissioner's Office (**ICO**) who supervise and enforce it.

The DPA applies to the processing of personal data. The terms "processing" and "personal data" have been very widely defined and any business operating in the UK which holds any personal information about individuals will be affected by the legislation.

**Personal Data**

Personal data is defined as anything that can be used to identify a living person and also includes sensitive data such as race, sexuality, health, trade union membership and any criminal offence or related legal proceedings.

**Data Controllers and Data Processors**

The DPA imposes obligations on data controllers who are responsible for ensuring that data processors also comply. Data controllers are defined as the person who determines for which purpose and the manner in which any personal data is to be processed. Data processors are those who process personal data on behalf of a data controller.

Data controllers must register with the ICO and inform them of what type of personal data is stored. Registration with the ICO must be renewed each year. If a data controller breaches the DPA, the ICO can require them to modify the data and impose a fine up to the amount of £500,000.

**The DPA Principles**

Schedule 1 of the DPA contains eight principles which data controllers must follow. These principles state that personal data must:

1. be processed fairly and lawfully;
2. be processed for narrow and clearly defined purposes;
3. be adequate, relevant and not in excess of what is required to achieve the purposes for which they are processed;
4. be accurate and up to date;
5. not be kept for longer than necessary;
6. be processed in accordance with the individual's rights;
7. be kept secure; and
8. not be transferred to a country outside the European Economic Area (EEA) if equivalent protection for an individual's rights and freedoms cannot be guaranteed.

The ICO has also published practice notes to aid interpretation of the principles in order to aid compliance and give guidance on issues such as when it is acceptable to share data with third parties and disclosing employee information in the event of a business transfer.

**Rights of Individuals**

Under the DPA, individuals are entitled to know what information is being held about them and have the right for that data not to be used in certain ways. They can also among other things, request data being held in relation to them, amend it if it is incorrect and opt out of direct marketing. An individual can also claim compensation for damage and distress caused by a breach of the DPA.

**Future Developments**

In January 2012, the European Commission published proposals for reform of EU data protection law. This proposes changed to the obligations of data controllers and processors and contains measures to harmonise data protection procedures and enforcement across the EU Regulation (EU) 2016/679 known as the General Data Protection Regulation (**GDPR**) will apply to all member states of the EU from 25th May 2018 following a two-year transition period.

In light of Brexit, the UK Data Protection Minister at the Department for Culture Media and Sport published a statement that EU rules on personal data might continue to apply fully in the UK if it remains within the Single Market. However, if the UK leaves the Single Market, the EU rules might be replaced with national ones.

In the Queen's Speech on 21 June 2017, a Data Protection Bill was announced which will replace the DPA further to the implementation of the GDPR. This will aim to put the UK in the best position to maintain its ability to share data internationally after it leaves the EU. The UK government has advised that businesses should continue to prepare and comply for the GDPR in the meantime

## CONTACT

**Alliance of Business Lawyers**
2, rue Charles-Bonnet
CH – 1206 Geneva
Switzerland
Phone: +41 223 476 262
Fax: +41 223 476 796
Email: info@ablglobal.net
Web: www.ablglobal.net

## DISCLAIMER

This publication is issued by the Alliance of Business Lawyers (ABL), a global association of independent law firms operating under Swiss law. As an association, ABL does not practice law or provide legal consultation or any other professional law services to third parties. Each member firm is independent, and no partnership, implied or otherwise, exists between ABL member firms.

The content of this publication is not a substitute for specific legal advice or opinions. Persons in need of legal advice related to any subject discussed in this publication should contact a legal professional who is qualified to practice in that area of law.
ABL expressly disclaims any and all liability resulting from actions taken or not taken based on any and all contents of this publication. This publication was revised in August 2017 and is based on accurate information and the law enforceable at that time.


ABL
LEGAL SOLUTIONS
ACROSS BORDERS
www.ablglobal.net