# DATA PROTECTION LAWS OF THE WORLD

Denmark

DLA PIPER

Downloaded: 13 March 2024

# DENMARK

*Last modified 19 January 2024*

## LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

### Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

To implement the GDPR, the Danish Parliament enacted the Danish Act on Data Protection (the 'Danish Data Protection Act’) on May 17, 2018, enforceable on May 25, 2018 and replacing the previous Danish Act on Processing of Personal Data (Act no. 429 of 31/05/2000). Hence, data protection and processing in Denmark is now regulated by the GDPR as supplemented by the Danish Data Protection Act.

The Danish Data Protection Act does not apply to Greenland and the Faroe Islands.

## DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions used in the Danish Data Protection Act correspond to the definitions as set out in the GDPR.

## NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party), also known as the “EDPB”, is comprised of delegates from the national supervisory authorities and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T +45 33 19 32 00
dt@datatilsynet.dk

## REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

In Denmark, the following types of processing require the DPA’s preapproval:

- private data controllers’ processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (‘Special Categories of Personal Data’), solely in the public’s interest
- disclosure of personal data as mentioned in Articles 9(1) and 10 of the GDPR, originally processed for the sole purpose of carrying out scientific or statistic studies, if i) such data is to be processed outside the geographical scope of the GDPR, ii) the data constitutes biological material or iii) if the data is to be published in a recognised scientific journal or similar
- processing personal data in a register on behalf of a private data controller:
  - solely for the purpose of warning other businesses from engaging in business with or employing a natural person
  - with the intention of commercial exploitation of data on the natural person’s creditworthiness and financial solidity, or
  - for the creation of a register on judicial information

## DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;

- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Under the Regulation, organizations shall designate a data protection officer (‘DPO’) in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- the core activities of the data controller or the processor consist of processing operations which, by their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects on a large scale, or
- the core activities of the controller or the processor consist of processing on a large scale of Special Categories of Personal Data and personal data relating to criminal convictions and offences

The DPO shall be selected based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in the GDPR.

Under the Danish Data Protection Act, the DPO is subject to a duty of secrecy and is prohibited from wrongful disclosure or use of any personal data processed in their capacity of being DPO.

## COLLECTION & PROCESSING

### Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

### Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);

- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

## Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise, or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

## Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

## Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation, that is to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider when assessing whether the new process is compatible with the purposes for which the personal data was initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are

processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

## Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data is used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible privacy notices should therefore be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

## Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

### Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

### Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

### Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when

Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

### Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

### Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

### Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

*The right not to be subject to automated decision making, including profiling (Article 22)*

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are made based on grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The GDPR differentiates between 1) Personal data, 2) Special Categories of Personal Data, 3) Data on criminal offences and 4) National identification numbers (CPR numbers). See below.

## 1. Personal data

Under the GDPR, data controllers may legally register and process personal data (all data except the Special Categories of Personal Data, Data on criminal offences and national identification numbers) only when at least one of the following conditions are met:

- the data subject has given his explicit consent in accordance with article 7 and 8 (children’s consent) of the GDPR;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or any other natural person;
- processing is necessary for the performance of a task carried out in the public interest or for the performance of a task carried out in the exercise of official authority vested in the data controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third-party to whom the data is disclosed, unless these interests are overridden by either the data subject’s fundamental rights including its civil rights or other interests of the data subject.

## 2. Special Categories of Personal Data

Special Categories of Personal Data (as detailed under 'Registration') may be processed only when at least one of the following conditions are met:

- the data subject has given his explicit consent to the processing of such data for one or several purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy;
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by a public organization.

Personal data and Special Categories of Personal Data may be processed, if such process is carried out in relation to the data subject’s employment at the data controller, if such process is necessary for the data controller to comply with employment-related obligations or rights under applicable law or collective agreements, or if the process is necessary for the data controller or third-party’s possibility to pursue legitimate interests originating from other legislation or collective agreements as long as the civil rights and interests of the data subject precedes.

Furthermore, personal data may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant importance to society and where such processing is necessary in order to carry out these studies. Sharing of personal data for such purposes will, however, be subject to the conditions set forth in the Danish Ministerial Order no. 1509 of 18 December 2019, according to which personal data shared for the purpose of carrying out statistical or scientific studies must, amongst other, be pseudonymised before sharing, unless direct identifications is strictly necessary.

## 3. Data relating to criminal convictions and offences

Data relating to criminal convictions and offences may be processed by public data controllers only if the processing is strictly necessary for the performance of regulatory and public tasks. No such data can, however, be disclosed, unless at least any of the following conditions are met:

- the data subject has given explicit consent to such disclosure;
- disclosure takes place for the purpose of safeguarding private or public interests which clearly override the

interests of secrecy, including the interests of the person to whom the data relate;

- disclosure is necessary for the performance of the activities of an authority or required for a decision to be made by that authority; or
- disclosure is necessary for the performance of tasks for a public authority by a person or an enterprise.

Private data controllers may process data relating to criminal convictions and offences, if the data subject in question has given his or her explicit consent in accordance with article 7 of the GDPR, or if the processing is strictly necessary to carry out interests significantly exceeding the interests of the data subject. None of the data may be disclosed without the explicit consent of the data subject, unless such disclosure takes place for the purpose of safeguarding public or private interests, including the interests of the person concerned, which clearly override the interests of secrecy.

Both public and private actors may process personal data about criminal convictions and offences if at least one the following conditions are met:

- processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy; or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by the public organization.

## 4. National identification numbers

National identification numbers (in Danish ‘*CPR-nummer*.’) may be processed by public organizations for the purpose of identification or as reference number.

Private data controllers may process *CPR-nummer* when at least one of the following conditions are met:

- the process is required under statutory law;
- the data subject concerned has given his or her explicit consent in accordance with article 7 of the GDPR;
- the processing is carried out for scientific or statistic purposes (however not for publication which requires a specific consent);
- the CPR-nummer disclosed as part of the company’s natural operations and such disclosure is of significant importance to the company to ensure identification of the data subject in question or requested by a public authority;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons

who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy; or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless it is carried out by a public data controller.

### 5. Transparency requirements

The data controller must, at the time when personal data are obtained (no later than within one month after), provide the data subject with the necessary information to fulfil the duty of information, including information about:

- the identity of the data controller, his representative and the DPO (if applicable);
- the contact details of the data controller / the representative;
- the categories of data concerned;
- the purposes of the processing for which the data is intended as well as the legal basis for the processing;
- the legitimate interests pursued by the data controller, where the processing is based on article 6(1)(f) of GDPR;
- the recipients or categories of recipients of the personal data, (if any);
- (where applicable), information of transfer of data to third countries or international organizations or the intention hereof, as well as reference to the appropriate and suitable safeguards in connection with such transfers;
- The period for which the data will be stored;
- The data subject’s right to withdraw a consent at any time;
- The data subject’s rights, including to lodge a complaint, deletion, insight and correction;
- From which source the personal data originate (if applicable), and whether it came from publicly accessible sources (if applicable);
- The existence of automated decision making (if applicable).

Under the Danish Data Protection Act the above-mentioned obligations do not apply if interests of the public, other people, or the data subject itself, exceed the data subject’s interest in obtaining the information.

## TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;

b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available, and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Danish Data Protection Act does not regulate transfer of personal data. Thus, the article of the GDPR applies, under which data controllers may transfer all types of personal data to a third country or an international organization out of the EU/EEA if any of the following conditions are met:

- the EU Commission has established that the third-country / area or one or more specific sectors in the third country, or the international organization has adequate safeguards with respect to the protection of the rights of the data subject;
- the controller or processor has provided appropriate safeguards, on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (such as through binding corporate rules – approved by the DPA);
- the data controller or data processor and the international organization enter into the standard terms approved by the EU Commission.

If no approval has been obtained on the third country’s adequate safeguards and no appropriate safeguards have been provided including binding corporate rules, personal data can be transferred to a third country or an international organization if one of the following criteria are met:

- the data subject has given his explicit consent;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject’s request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- the transfer is necessary or legally required on important public interest grounds;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or other natural person, where the person concerned is physically or legally incapable of giving his or her consent;
- the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

---

For more information, please visit our Transfer - global data transfer methodology website.

## SECURITY

### Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Danish Data Protection Act does not set out provisions on security requirements. Thus, the articles of the GDPR apply, under which data controllers and data processors must implement appropriate technical and organizational security measures necessary to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Danish Data Protection Act.

## BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Danish Data Protection Act does not set out provisions on notification in case of security breach. Thus, the articles of the GDPR apply, under which the data must notify the DPA no later than 72 hours after becoming aware of the security breach.

Breaches can be reported to the Danish Data Protection Agency by filling out a form on the Danish Business

Authority’s website.

Further, if the security breach is likely to expose the data subject to risk related to its rights and civil rights, the data controller shall notify the data subject without unnecessary delay.

## ENFORCEMENT

### Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

**The highest fines** (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

**The lower category of fines** (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

### Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

### Right to claim compensation

The GDPR provides specific provisions for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" because of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA is responsible for the supervision of all processing operations covered by the Danish Data Protection Act.

The DPA can request any information provided necessary for the DPA’s operations including decision-making on whether the Danish Data Protection Act and the GDPR apply or not.

The DPA and its personnel can without a court order request access to premises from which processing of personal data is performed.

The DPA’s decisions are final and not subject to recourse.

The DPA may investigate data processing occurring in Denmark and the legality thereof, despite the processing being subject to foreign law.

The DPA may publish its findings and decisions.

Any person suffering material or nonmaterial damage due to non-legal data processing can claim damages.

Unless a higher penalty is impeded, processing deemed unlawful under the Danish Data Protection Act, is sanctioned with a fine or prison for up to six months.

In general, the GDPR aims to sanction with fines which are effective, reasonable and have preventive effect. More specific, certain violations can be sanctioned with a fine of a maximum of EUR 10,000,000 or 2% of the total annual turnover (if a company). Other types of violations can be sanctioned with a fine of a maximum of EUR 20,000,000 or 4% of the total annual turnover (if a company).

The statute of limitation period is five years.

## ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive

2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the ‘same service / product’ exemption. The exemption concerns marketing emails related to the same products / services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt out prior to the first marketing email;
- the user did not opt out; and
- the user is informed of the right to opt out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

The GDPR applies to electronic marketing activities involving usage of personal data (e.g. an email address which includes the recipient's name).

Under the GDPR companies are prohibited from disclosing personal data to another company for direct marketing purposes or use the data on behalf of a company for marketing purposes, unless the data subject has given his or her explicit consent. In this regard, the strict standard for consent under the GDPR must be noted, and marketing consent forms must include a clearly worded opt-in mechanism (such as a ticking of an unticked consent box, or the signing of a statement, and not merely an acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

General customer information (general information forming the basis for customer classification) may, however, be disclosed and processed without the data subject’s consent, if such is necessary for the purposes of legitimate interests pursued by the company and these interests are not overridden by the interests of the consumer. However, Special Categories of Personal Data and CPR-numbers can only be processed for marketing purposes by the consent of the data subject.

The company disclosing the personal data or processing the personal data on behalf of a company for marketing purposes, must prior hereto ensure that the data subject has not declined receiving marketing material by registering as such in the Danish Central Office of Personal Registration.

Particularly for controllers selling catalogues of data on natural persons or addressing these natural persons on behalf of a company it applies that only the natural person’s name, work position, address, occupation, email, phone- and fax number and business information published in business registers can be processed. Any other kind of data can only be processed if the data subject has consented thereto.

Further, specific rules on electronic marketing (including circumstances in which consent must be obtained) are regulated in Directive 2009/136/EC (the ePrivacy Directive), as transposed into the local laws of each Member State. In Denmark, the ePrivacy Directive has among other things been implemented in the Danish Marketing Practices Act.

Under the Danish Marketing Practices Act, a trader must not approach anyone by means of electronic mail, an automated calling system or a facsimile machine (fax) for the purposes of direct marketing unless the natural person concerned has given his prior consent. The trader must allow free and easy revocation of the consent.

Notwithstanding the above, a trader that has received a customer's electronic contact details in connection with the sale of products may market similar products to that customer by electronic mail, provided that the trader has clearly and

distinctly given the customer the opportunity, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in all subsequent communications.

The ePrivacy Directive is to be replaced by the ePrivacy Regulation, a change which was forecast for spring 2018, however, now postponed indefinitely. From the wording of the latest draft, we can expect a significant toughening of the online and direct marketing landscape and, predictably, a convergence with the provisions in the GDPR.

## ONLINE PRIVACY

### Traffic data

Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal;
- authorization codes, additionally the card number when customer cards are used;
- location data when mobile handsets are used;
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
- the telecommunications service used by the user;
- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted; and
- any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or where the user has requested a connection overview.

The service provider may collect and use the customer data and traffic data of subscribers and users to detect, locate, and eliminate faults and malfunctions in telecommunications systems. This applies also to faults that can lead to a limitation of availability of information and communications systems or that can lead to an unauthorized access of telecommunications and data processing systems of the users.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Service providers must inform the users immediately, if any faults of data procession systems of the users become known. Furthermore, the service provider must inform the users about measures for detecting and rectifying faults.

### Location Data

Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user’s informed consent must be obtained. According to Section 4a BDSG, 13 German Telemedia Act (TMG) this means that:

- the user’s consent must be intentional, informed, and clear. For this purpose, the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties;
- the user’s consent must be recorded properly;
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information is provided upon the user's request;
- the user’s consent must be revocable at all times with effect for the future.

Users must always be informed of the use of cookies in a privacy notice. Cookies may generally be used if they are required to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information about the use of cookies together with a link about how to adjust browser settings to prevent future use are

sufficient.

Germany has not yet taken any measures to implement the e-privacy directive. However, in February 2014 the German Federal Ministry of Economic declared that the European Commission considers the Cookie Directive as implemented in Germany. However, since the European Commission´s exact interpretation is not known, a final official clarification is awaited. It therefore remains to be seen whether an active opt-in, e.g., by clicking on a pop-up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user’s IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

Directive 2009/136/EC (the ePrivacy Directive) was among other things also implemented in the Danish Act on Electronic Communications Services and Networks which came into force on May 25, 2011 in accordance with the implementation deadline in the Directive. In accordance with this act, the Danish Parliament adopted the Danish Executive Order on Electronic Communications Services and Networks which came into force on May 25, 2018 (the ‘Cookie Order’).

The Cookie Order should be read in the light of GDPR, where the rules regulate collection of data in a broader sense, not considering whether such information may be used to identify a natural person.

Under the “Cookie Order” the use of cookies requires a consent. The consent must be freely given and specific. However, this does not imply that consent must be obtained each time a cookie is used but a user must be given an option. Furthermore, the consent must be informed which implies that a user must receive information about the consequences of consenting. To meet the information requirement, one must:

- Provide the information in a clear and explicit language, that is easy to understand or a similar imagery that is easy to understand, e.g. pictograms;
- Explain the purpose of using cookies;
- Tell the users who is behind the cookies used – this may be the website owner or a third party;
- Inform the user how to give consent or reject the use of cookies;
- Explain how the user can withdraw his or her consent;
- State the duration of the cookies (expiry date).

Finally, the consent must be a clear indication of the user’s wishes, which entails meeting the following requirements:

- The user must be able to consent or refuse to consent to the use of cookies;
- The user must be able to withdraw a previously given consent;
- The user should easily be able to find further information about the use of cookies on the website;
- The consent must be linked to the purpose for which the data collection is to be used.

Previously, the use of a homepage after having received relevant information could (to some extent) be considered to be a valid consent in Denmark. This is no longer the case and now a more explicit consent is required (e.g. the clicking of an “accept” button).

The ePrivacy Directive is to be replaced by the ePrivacy Regulation, a change which was forecast for spring 2018, however, now postponed indefinitely and the timeframe for changes to abovementioned rules are thus currently unknown.

From the wording of the latest draft, however, it is unsurprisingly safe to say that the definition of consent used in the GDPR is carried on and is to be read across into the draft e-Privacy Regulation text. Further, the draft also introduces significant practical changes, so that obtaining consent will require much more effort. Technology providers are required to include default settings which must all be set to preclude third parties from storing information on, or using information about, an end-user’s device. So, browsers would have to be pre-configured so that cookies used for frequency capping of ads or ad-serving would be blocked by default unless a user opts to enable them.

## Current position

There has not been changes in the Danish data protection legislation. The Danish supervisory authority (the Danish Data Protection Agency) has had several focus areas for 2023 including child protection, TV surveillance, processing of personal data in pan-European information systems, etc.

With effect from 1 January 2023, an amendment has been made to the executive order on disclosure for research and statistical purposes, which specifies the conditions for disclosure of personal data from statistical or scientific studies under section 10 of the Danish Data Protection Act. In this connection, the rules for erasure of personal data at the end of research projects have been clarified. This has been done to clarify that the data controller may have a legitimate need to process data for a period after the end of the study - e.g. for the purpose of addressing allegations of scientific misconduct. This is because controllers will often be subject to requirements to prove, for a period after the end of their study, that the study is not based on false information or that other researchers must be able to recreate the results. Controllers should consider whether the purpose of processing personal data after the end of the study can be achieved by processing the data in another – e.g. anonymized – form, in accordance with the fundamental data protection law principle of data minimization.

In relation to the right of access regarding children, the Danish Data Protection Agency has stated that the right of access (Article 15) is a personal right that belongs to the individual data subject. This also applies in the case of a child. The child is an independent rights holder. Parents can support their child in exercising the child's right of access by requesting access on behalf of the child. As a rule, each parent can make such a request without documentation of consent from the other parent.

The Danish Data Protection Agency has published various new guidelines, practices and statements including among others:

- guidelines about data processing in connection with direct marketing. This is because direct marketing is one of the most widespread forms of marketing and because direct marketing almost always involves the processing of personal data;
- guidelines about the different GDPR roles in research projects, e.g. the different roles that may apply in clinical research, the role of Ph.D. students, collaboration between public authorities, hospitals, and private actors etc;
- guidelines about public authorities’ use of Artificial Intelligence (AI);
- three guidelines on CCTV surveillance for private organisations, public authorities, and housing organizations. The guidelines go through relevant rules to be aware of when processing and disclosing personal data related to CCTV surveillance, especially related to crime prevention;
- two fundamental decisions regarding the use of cookie walls. Following these decisions, the Danish Data Protection Agency has prepared some general guidelines on the use of cookie walls that companies should use and introduces four conditions to place cookie walls: 1) it must be a reasonable alternative to consent, 2) the price must be fair, 3) cookie walls must respect the purpose limitation principle, and 4) processing may start after payment has been received;
- a catalogue of security measures (*Katalog over foranstaltninger* (datatilsynet.dk)), which includes a list of organisational and technical measures and descriptions and examples about how to use and implement the measures to mitigate, reduce, or eliminate certain risks. The measures are based on experiences from audits in the private and public sector, data security breach cases, EDPB guidelines, ISO 27001, and ISO 27002;
- guidelines about user and access rights to it-systems, physical locations etc.

Further, at the annual meeting of the Nordic supervisory authorities (Denmark, Faroe Islands, Finland, Iceland, Norway, Sweden, and Åland), the "*Reykjavik Declaration*" was adopted: Reykjavik Declaration.pdf (datatilsynet.dk). One of the goals of the Reykjavik Declaration is to continue to explore the possibilities for a more data- and risk-based process in the selection of where to carry out supervision. In this context, the countries also agreed to work towards greater knowledge-sharing at the European level.

## KEY CONTACTS

Marlene Winther Plas
Partner
T +45 33 34 00 47
marlene.plas@dlapiper.com

## DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

**Disclaimer**

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.