

DATA PROTECTION LAWS OF THE WORLD

Norway



Downloaded: 29 April 2024

NORWAY



Last modified 26 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.

The GDPR was incorporated in the EEA Agreement by a Joint Committee Decision dated July 6, 2018. The new Norwegian Personal Data Act (LOV-2018-06-15-38) ("**PDA**") implements GDPR and became effective as of July 20, 2018.

In addition to implementing GDPR, the PDA includes specific regulations as described below. In connection with the implementation of GDPR, several sector-specific regulations, e.g. in the healthcare sector, has been updated to ensure compliance with GDPR.

The PDA has a similar geographical scope as GDPR article 3 in that it applies to:

1. data controllers and processors established in Norway regardless of whether the processing activities takes place Norway / EEA or not; and
2. processing activities by a data controller or data processor which is not established in the EEA to the extent the processing activity relates to:

- a. offering of goods and services to data subjects in Norway, irrespective of whether a payment of the data subject is required; or
- b. the monitoring of their behavior, to the extent that such behavior takes place within Norway.

The PDA applies to processing of personal data by controller who is not established in Norway, but in a place governed by Norwegian law according to public international law.

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.

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) is comprised of delegates from the 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 (ie, 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.

The Norwegian Data Protection Authority is:

Datatilsynet

www.datatilsynet.no

Together with other EEA countries (Iceland and Lichtenstein) the Norwegian Data Protection Authority became members of the EDBP however without voting rights and without the right to be elected as chair and vice-chair, for GDPR-related matters.

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 (eg, 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 organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

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 penalized 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.

The government may issue further regulations as regards the duty to appoint a DPO. No such regulations have been issued yet.

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 defense 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 - ie, 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; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were 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, ie, the right for a data subject to understand how and why his or her data are 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, whilst 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 recognised by mainstream software applications, such as .xml).

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 (ie, opt-in) consent.

Further, where significant automated decisions are taken on the basis of 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.

Scope

The PDA and GDPR does not apply to processing activities by physical persons for purely private or family purposes or for processing activities within the justice administration sector. For processing activities for journalistic purposes or academic, artistic or literary expressions, only GDPR articles 24, 26, 28, 29, 32 and 40-43 applies, as well as PDA chapter 6 on supervision and complaints and chapter 7 on sanctions and coercive fines.

Age limit to consent to information society services

According to the PDA section 5, the age limit to consent to information society services is 13 years.

Processing of special categories of personal data

Processing of special categories of personal data is allowed when necessary to perform rights or obligations within the field of employment law.

The Norwegian Data Protection Authority may authorize the processing of sensitive personal data where the processing is in the public interest.

The Norwegian Data Protection Authority can also issue specific regulations allowing for the processing of special categories of data.

Processing of information relating to criminal offences

According to the PDA, the processing of information about criminal offences is subject to the regulations as GDPR article 9(2)(a), (c) and (f) as well as the PDA sections 6, 7 and 9, i.e. the same provisions as the processing of special categories of personal data.

Use of personal ID numbers

Personal ID numbers unique identifiers may only be processed where there are reasonable grounds to require proper identification and the use of personal ID numbers is necessary for such identification.

Specific rules on consent

The PDA contains provisions relating to processing of special categories of personal data for e.g., scientific purposes without the consent of the data subject provided that the processing is covered by necessary warranties in accordance with the GDPR Article 89(1). There is no specific general regulation as regards safeguards according to GDPR Article 89, paragraph 1.

Before processing special categories of data, the data controller should consult and seek advice from the Data Protection Officer ("DPO") in accordance with GDPR Article 37.

The above-mentioned advice from the DPO must consider whether the processing will meet the requirements of GDPR and other provisions laid down in the Norwegian Implementation Act. The consultation obligation with the DPO does not apply if an assessment has been made of privacy implications according to GDPR Article 35.

The duty to consult with a DPO also applies to the extent that processing of special categories of data for statistics of scientific purposes is based on consent.

Exemption to data subject rights to access and information

The PDA contains some exemption to the right to access and information according to GDPR Article 13-15 to if the information:

- a. is of relevance for Norwegian foreign policy or national security;
- b. must be kept secret in order to prevent, investigate, disclose and prosecute criminal acts;
- c. that is considered that inadvisable that the data subject obtains due to the health situation of the relevant person or the relationship to close relationships of such persons;
- d. subject to duty of confidentiality by law;
- e. which only is found in text prepared for internal purposes and not disclosed to others;
- f. where disclosure would be in breach of obvious and fundamental private or public interests.

Any denial of access according to the above shall be provided by way of a written explanation.

The right of access according to GDPR Article 15 does not apply to the processing of personal data for archival purposes in the public interest, purpose related to scientific or historical research or statistical purposes in accordance with GDPR Article 89. No. 1 so far as:

- a. it will require a disproportionate effort to give access; or
- b. the right of access will make it impossible or seriously impair the achievement of the specific purposes.

The right to rectification and restriction in accordance with GDPR Article 16 and 18 does not apply to processing for archival purposes in the public domain interest, purposes related to scientific or historical research or statistical purposes in accordance with GDPR Article 89 No. 1 as far as it is likely that the rights make it impossible or seriously impair the achievement of the specific purposes.

The above exemptions do not apply if the processing has legal effects or directly has factual effects for the data subject.

Access to employee email

A separate regulation (FOR-2018-07-02-1108) issued under the Working Environmental Act (LOV-2005-06-17-62) contains the conditions and procedures that have to be followed for accessing employee emails by an employer. Access to employee email can only take place if there is a legitimate interest or if it is necessary to secure daily operations or if

there is a suspicion that the email has been used in such a manner that it is a clear violation of the working relationship or could lead to dismissal or termination of employment.

The employee shall, as far as possible, be given notice and be able to participate when access to email is made.

CCTV surveillance in the workplace

A separate regulation (FOR-2018-07-02-1107) has also been adopted under the Working Environmental Act and contains provisions on the legality of CCTV surveillance in the workplace, notification and deletion obligations, as well as the legality of transfer of CCTV recordings. CCTV monitoring in the workplace may only take place where it is needed to prevent dangerous situations from arising and to safeguard the safety of employees or others, or where there otherwise is a special need for the monitoring. The regulation also applies to dummy cameras.

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, Japan, Jersey, Uruguay, New Zealand, Republic of Korea and the United Kingdom.

With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).

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 and standard contractual clauses. 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.

Please note that pursuant to a recent decision in the Court Justice of the European Union (Case C-311/18 Schrems II) the EU US Privacy Shield Framework may no longer serve as a legal basis for transfers of personal data between the EEA and USA.

On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). These SCCs contain a practical toolbox to comply with the Schrems II judgment; i.e. an overview of the different steps companies have to take to comply with the Schrems II judgment as well as examples of possible 'supplementary measures', such as encryption, that companies may take if necessary.

These modernised SCCs replace the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46. Since 27 September 2021, it is no longer possible to conclude contracts incorporating these earlier sets of SCCs.

Until 27 December 2022, controllers and processors can continue to rely on those earlier SCCs for contracts that were concluded before 27 September 2021, provided that the processing operations that are the subject matter of the contract remain unchanged.

On 12 December 2022, the European Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its Schrems II decision.

Once the adequacy decision is adopted, European entities will be able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

Hopefully this adoption process will be completed during the spring of 2023.

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 defense 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 recognized 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.

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 organizational 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 organisational measures for ensuring the security of the processing.

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.

Data breaches that require notification to the Norwegian DPA, can be notified by completing an online form through Altinn, a Norwegian internet portal for digital dialogue between businesses and public agencies.

The form is [available online](#).

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 scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law 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 makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result 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).

Fines

Fines may be imposed on public authorities. Furthermore the PDA sets out that fines under GDPR will also apply to a breach of GDPR article 10 (processing of data relating to criminal convictions) and 24 (obligation on the controller to implement appropriate technical and organizational measurements to demonstrate that processing is in accordance with GDPR).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will 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.

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg, an email address is likely to be personal data; for the purposes of the Act).

Pursuant to the Marketing Control Act (LOV-2009-01-09-2, Nw: *Markedsføringsloven*) section 15, it is prohibited in the course of trade, without the prior consent of the recipient, to send marketing communications to natural persons using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems (calling machines).

Prior consent is however not required for electronic mail marketing where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader's own goods, services or other products corresponding to those on which the customer relationship is based.

At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

Electronic mail; in the context of the Marketing Control Act means any communication in the form of text, speech, sound or image that is sent via an electronic communications network, and that can be stored on the network or in the terminal equipment of the recipient until the recipient retrieves it. This includes text and multimedia messages sent to mobile telephones.

Direct marketing emails must not conceal or disguise the identity of the sender. If the email is unsolicited, it shall clearly state that the email contains a marketing message upon receipt of the message (The Norwegian E-Commerce Act (LOV-2003-05-23-35), Nw: *Ehandelsloven*, section 9).

ONLINE PRIVACY

Traffic Data

Traffic data is defined in Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services (FOR-2004-02-16-401, Nw: *Ekomforskriften*) section 7-1 as data which is necessary to transfer communication in an electronic communications network or for billing of such transfer services.

Processing of traffic data held by a Communications Services Provider ('CSP') (Nw: *Tilbyder*) may only be performed by individuals tasked with invoicing, traffic management, customer enquiries, marketing of electronic communications networks or the prevention or detection of fraud.

Traffic Data held by a CSP must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication (Electronic Communications Act (LOV-2003-07-04-83) section 2-7 (Nw: *Ekomloven*). However, Traffic Data can be retained if it is being used to provide a value added service and consent has been given for the retention of the Traffic Data.

Location Data

Location data may only be processed subject to explicit consent for the provision of a value added service which is not a public telephony service, and the users must be given understandable information on which data is processed and how the data is used. The user shall have the opportunity to withdraw their consent. See Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services section 7-2.

Cookie Compliance

The Electronic Communications Act has been changed in accordance with directive 2009/136/EC regarding the use of cookies. According to section 2-7 b, the user must give their consent before cookies or any other form of data is stored in their browser. The users must receive clear and comprehensive information about the use of cookies and the purpose of the storage or access.

However, obtaining user consent is not required if the cookie solely has the purpose of transferring communication in an electronic network, or if it is deemed to be necessary for the delivery of a service requested by the user. The decision of the Court Justice of the European Union in case C-673/17 (Planet 49) entails that consent to non-essential cookies no longer can be expressed through browser settings, at least if the cookie entails processing of personal data. The National Communications Authority, the authority responsible for supervising the Electronic Communications Act, recommends adhering to the consent regime of GDPR (i.e. freely given, specific, informed and unambiguous) if a website operator is uncertain of its compliance with regards to consent.

The Norwegian Government has proposed changes in relation to obtaining cookie-consent in connection with the proposed new Electronic Communications Act. According to the proposal the definition of a legal consent will be equal to the definition in GDPR (i.e. clear opt-in). These changes are expected to enter into force during 2023 and if implemented in accordance with the proposal, the changes will clarify the current uncertainty regarding the consent regime regarding the use of cookies. The Norwegian Government does not preclude that one can provide a general consent for cookies (when required) through browser settings for as long as this is by way of an affirmative action. However, it still remains to be seen whether it is technically and legally possible to implement a general GDPR compliant consent through browser settings.

KEY CONTACTS



Ketil Sellæg Ramberg

Partner

T +47 24 13 15 57

ketil.ramberg@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.