Overview of key provisions in GDPR

Information duty

Obligation for the controller to inform the DS on:

- The identity and the contact details of the controller (and eventually the controller's representative and DPO)
- The purposes of the processing
- The legal basis for the processing
- The legitimate interests pursued by the controller or by a third party (if processing is based on legitimate interest)
- The recipients or categories of recipients of the PD (if any)
- Any intentions to transfer the PD to a third country
- The period the PD will be stored, or, if not possible, the criteria used to determine that period
- The right to request access to, rectification, erasure, restriction of processing and data portability
- The right to withdraw consent at any time (if the processing based on consent)
- The right to lodge a complaint with a supervisory authority
- Whether the DS is obliged to provide the PD, and the possible consequences of failure to do so (if the basis for processing is a statutory or contractual requirement/necessary to enter into a contract)
- If decision-making is automated (including profiling), applications of and information on the logic involved, and any consequences of such processing for the DS

If the PD has not been obtained from the DS, in addition inform of:

- The categories of PD concerned
- Where the PD originates from and if from publicly accessible sources

The DS shall be informed if the PD is to be processed for a purpose other than why the PD was collected.

The information shall be given in a concise, transparent, intelligible and easily accessible form using clear and plain language.

Information shall be given when the PD is obtained (if the PD was received from the DS) or within 1 month (if not collected from the DS) or at the latest at the first communication or disclosure of the PD.

The above shall not apply if the DS already has the information (or if the PD is not collected from the DS and the provision of such information proves impossible or would involve a disproportionate effort).

Article 12, 13 and 14 (39, 50, 53, 58, 57, 59, 60, 64, 66, 68, 75, 85 and 164).

Personal data breach

A personal data breach is a breach of security leading to:

- The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or
- Access to, PD transmitted, stored or otherwise processed

Article 4 no. 12 (73, 85, 86, 87 and 88).

Principles relating to processing of personal data

Personal data shall be:

- Processed **lawfully, fairly** and in a **transparent manner**
- collected for specified, explicit and legitimate **purposes** and not further processed in a manner that is incompatible with those purposes
- **adequate**, **relevant** and **limited** to what is necessary in relation to the purposes for which they are processed
- **accurate** and, where necessary, kept **up to date**
- kept in a form permitting identification of data subjects **not longer than necessary** for the purposes for which the personal data are processed
- processed in a manner that **ensures appropriate security** of the personal data, using appropriate technical or organisational measures

The controller shall be **responsible** for, and be able to demonstrate compliance with the above .

Article 5 (29, 39, 50, 58, 60, 65, 71, 73 and 85).

Right of access

Right for DS to get information on:

1. **Whether or not PD on the DS is being processed**
2. **Information on the processing:**

- The purpose of the processing
- The categories of PD concerned
- (Categories of) recipients to whom the PD are to be disclosed, incl. recipients in third countries
- The period in which the PD will be stored, or, if not possible, the criteria used to determine that period
- The right to request rectification, erasure, restriction of processing or to object to such processing
- The right to lodge a complaint with a supervisory authority
- Where the PD originates from and if from publicly accessible sources
- If automated decision-making, incl. profiling, apply and information on the logic involved and any consequences of such processing for the DS

3. **Providing a copy of the PD undergoing processing**

- Must be provided only to the DS
- Providing of the PD must not adversely affect the rights or freedoms of others

Request by electronic means: The PD must be provided in a commonly used electronic form.

Must be provided within 1 month (may be prolonged to 2 months).

The first copy of the PD shall be provided free of charge.

Exception from right of access: The request is manifestly unfounded or excessive (e.g. repetitive).

Article 12 and 15 (39, 57, 58, 59, 60, 64).

Processing of special categories

Processing special categories of PD is prohibited unless, inter alia:

a) Consent is given by the DS

b) Processing is necessary for carrying out obligations/specific rights of the controller or the DS in the field of employment and social security and protection law

c) Processing relates to PD which is manifestly made public by DS

d) Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity

e) Necessary for reasons of substantial public interest

Article 9 no. 2 (32, 42 and 51).

Lawful processing

Processing is lawful:

a) **Consent** is given by the DS

b) For the performance of a **contract** to which the DS is party or in order to take steps at the request of the DS prior to entering into a contract

c) In compliance with a **legal obligation** to which the controller is subject

d) To protect the **vital interests** of the DS or other natural person

e) For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) For the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the DS.

Article 6 (32, 39, 40, 41, 42, 43, 44, 45, 46, 47 and 48).

Consent

Consent must be:

- **Freely given**: Without any benefits or advantages attached to the consent.
- **Specific**: Relate to one or more specific purposes.
- **Informed:** The consent shall comprise all processing of the PD.
- **Unambiguous:** Clear affirmative action/indication/statement of the DS on processing of the PD.

The consent must:

- Be capable of withdrawal at any time (which the DS shall be informed of), and as easy to withdraw as to give consent.
- Demonstrate that the DS has consented.
- Be presented in a manner which is clearly distinguishable from other matters.
- Be in an intelligible and easily accessible form, using clear and plain language.

Article 4 no. 11, 6 and 7 (25, 32 and 42).

Note that this is only an overview. See reference to GDPR for more information (numbers in brackets are reference to the preamble).

Prepared by Jan Sandtrø
jan.sandtro@dlapiper.com
+4799731934
linkedin.com/in/sandtro/

Processing

Processing is:

- Any operation which is performed on PD (by use of automated (such as IT) means) and
- processing other than by automated means (such as paper) which (are intended to) form part of a filing system (ie. structured set of PD which are accessible according to specific criteria).

Does not comprise processing by a natural person in the course of a purely personal or household activity.

Article 2, 4 no. 2 and 6 (15, 16, 18 and 19)

Territorial scope

Controller or processor established in the EU/EEA regardless of whether the processing takes place in the EU/EEA or not.

If processing the PD of a DS in the EU/EEA for:

- Offering of goods or services, irrespective of whether a payment is required, or
- Monitoring behaviour of the DS as far as the behaviour takes place within the EU/EEA,

the controller or the processor shall designate in writing a representative in EU/EEA.

Article 3 (22, 23, 24 and 25).

Special categories of PD

Special categories of PD:

- revealing racial or ethnic origin,
- political opinions, religious or philosophical beliefs,
- trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Processing of PD relating to criminal convictions and offences shall be carried out only under the control of an official authority or if permitted by law.

Article 9 no. 1 and 10 (10, 34, 35 and 51).

Personal data breach notification

In the case of a personal data breach (see separate box):

The processor shall notify the personal data breach to:

- The controller by the processor without undue delay
- To the supervisory authority not later than 72 hours

after having become aware of the personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons.

Communicate the personal data breach to the DS:

- Without undue delay
- When the personal data breach is likely to result in a high risk to the rights and freedoms of the DS
- Not necessary if measures are taken to ensure that the high risk is not longer likely to materialise or would involve disproportionate effort.

Article 33 (73, 85, 86, 87 and 88).

Controller

Controller is:

- A natural or legal person, public authority, agency or other body which,
  - determines the purposes and
  - means of processing of PD.
- alone or jointly with others (joint controllers)

Article 4 no. 7, 24 and 26 (1, 27 and 79).

Processor

Processor is:

- A natural or legal person, public authority, agency etc. which
- processes PD on behalf of the controller.

The controller shall only use processors:

- Providing sufficient guarantees to implement appropriate technical and organisational measures.
- Adhering to approved codes of conduct or certification mechanisms.

Requirement to enter into a data processing agreement, see next page.

Article 4 no. 8, 27, 28 (29, 71, 77, 80, 81, 82, 83, 108, 109 and 156).

Personal data (PD)

Personal data means **any** information relating to an identified or identifiable natural person ('data subject', see below).

Article 4 no. 1 (27, 158 and 160).

Data subject (DS)

A natural person who can be identified directly or indirectly, in particular by reference to an identifier (such as name, id. number or by one or more factors).

Article 4 no. 1 (27, 158 and 160).

Erasure

PD shall be erased without undue delay if:

- The PD is no longer necessary to achieve the purposes for which it was collected or otherwise processed.
- The DS withdraws its consent on which the processing was based and where there is no other legal ground for the processing.
- The DS objects to the processing (cf. Art. 21) and there are no overriding legitimate grounds for the processing.
- The PD has been unlawfully processed.
- The PD has to be erased for compliance with a legal obligation

The obligation also applies if the PD has been made public or transferred to other controllers.

Exception to the above duty: The PD is necessary for the establishment, exercise or defense of legal claims, or for compliance with a legal obligation which requires processing, etc.

The controller has a duty, taking into account available technology and the cost of implementation, to take reasonable steps, to inform the controllers processing the PD that the DS has requested erasure.

Article 17 (4, 62, 65, 66, 68 and 153).

Versjon: januar 2018

Transfer of PD to a third country

Transfer of PD to a third country must have a lawful basis:

- A commission decision that the third country etc., ensures an adequate level of protection.
- Appropriate safeguards are provided and on condition that rights and effective legal remedies for DS are enforceable .
- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules (BCR)
- Standard data protection clauses (adopted by a supervisory authority and) approved by the Commission
- An approved CoC or approved certification mechanism together with commitments from the controller or processor in the third country to apply the appropriate safeguards, incl. as regards DS' rights

If a transfer could not be based on the above, a transfer:

- that is not repetitive,
- that concerns only a ltd. number of DS
- that is necessary for the purposes of compelling legitimate interests not overridden by the interests or rights and freedoms of the DS, and
- for which the controller has assessed all the surrounding circumstances and has on the basis of that assessment provided suitable safeguards with regard to the protection of the PD

On the following basis:

- that the DS has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the DS

Or the transfer is necessary for:

- the conclusion or performance of a contract between the DS and the controller or the implementation of pre-contractual measures taken at the DS' request
- important reasons of public interest
- the establishment, exercise or defence of legal claims
- protecting the vital interests of the DS or of other persons, where the DS is physically or legally incapable of giving consent

The controller shall inform

- the supervisory authority of the transfer
- The DS of the transfer and on the compelling legitimate interests pursued.

Article 45 to 49 (101 til 107).

Data portability

The right for the DS to receive or transmit PD in a structured, commonly used and machine-readable format.

Applies only to PD the DS has provided to a controller, and provided that

- the processing is based on consent or on a contract
- the processing is carried out by automated means.

Article 20 (68 and 73).

Data processing agreement

Processing by a processor shall be governed by a contract or legal act.

The contract shall include:

- The subject-matter and purpose, the duration and the nature of the processing
- The type of PD
- The categories of DS

Certain obligations and rights of the controller must be included, such as:

- The PD shall be processed only on documented instructions from the controller
- The PD shall not be transferred to a third country etc., unless required to do so by law to which the processor is subject
- Persons authorised to process the PD must have committed themselves to confidentiality or be under an appropriate statutory obligation of confidentiality
- Taking all measures with regard to security of the PD (see separate box).
- Assisting the controller using appropriate technical and organisational measures
- Assisting in the fulfilment of the controller's obligation to respond to requests for exercising the DS' rights under GDPR
- Assisting the controller in ensuring compliance with the obligations under Article 32–36.
- Deleting, or returning, all PD to the controller (as requested by the controller) after the end of the provision of services relating to processing, and deleting existing copies unless law requires storage of the PD
- Making available to the controller all information necessary to demonstrate compliance with the obligations under GDPR
- Allowing for and contributing to audits, incl. inspections, conducted by the controller or another auditor for the controller
- Only engaging another processor with the written authorisation of the controller, and only where such processor shall comply with the same obligations as the agreement with the processor.

The contract shall be in writing (but may be in electronic form).

The processor shall immediately inform the controller if, in its opinion, an instruction infringes GDPR or other regulation.

Article 28. (29, 71, 77, 81, 82, 83, 156).

Data protection by design and by default

Appropriate technical and organisational measures shall be implemented to ensure compliance with GDPR and protect the rights of the DS, taking into account:

- The state of the art
- The cost of implementation
- The nature, scope, context and purposes of processing
- The risks (of varying likelihood and severity) to rights and freedoms of natural persons posed by the processing,

at the time of the determination of the means for processing and at the time of the processing itself such as pseudonymisation, data minimisation etc. in an effective manner and to integrate the necessary safeguards into the processing

Ensuring that, by default, only PD which is necessary for each specific purpose of the processing is processed , and applies to:

- The amount of PD collected
- The extent of its processing, the period of storage
- Accessibility, in particular, such measures shall ensure that, by default, PD is not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 25 (26, 28, 29, 71, 75, 78, 156).

Security of personal data

Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering.

- Nature
- Scope
- Context
- Purposes of processing
- Risk (of varying likelihood and severity) to the rights and freedoms of natural persons

Be able to demonstrate performance in accordance with GDPR.

Implement appropriate data protection policies.

Adhere to approved codes of conduct and certification mechanisms.

Article 24, 28 and 32 (29, 71, 74, 77, 81-83).

Procedures and documentation

The following documentation is – *inter alia* – required under GDPR:

- Documentation to demonstrate processing in accordance with GDPR.
- Documentation on any personal data breaches, facts, effects and remedial action taken.
- Records of processing activities, if applicable.
- Documentation on the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The following procedures may be implemented (and documented):

- Procedures on informing the DS
- Procedures on complying with requirements as to erasure, right to access, right to correction etc.
- Complying with data portability and data protection by design and by default .
- Procedures on notification upon personal data breach
- Procedures on use of processors
- Procedures on transfer to third countries.

Automated individual decision-making, incl. profiling

The DS shall not be subject to decisions based solely on automated processing, incl. profiling, which produces legal effects or has similarly significantly affects.

Exceptions to the above where processing is:

1. Necessary for entering into, or performance of, a contract between the DS and the controller,
2. authorised by law to which the controller is subject and which also lays down suitable measures to safeguard the DS' rights and legitimate interests, or
3. based on the DS' explicit consent.

For 1 and 3 above, the controller shall implement suitable measures to safeguard the DS' rights and legitimate interests, including at least the right to obtain human intervention on the part of the controller, to express the DS' point of view and to contest the decision.

Shall not be based on special categories of PD unless suitable measures to safeguard the DS' rights and freedoms and legitimate interests are in place.

Article 22 (71 and 75).

Right to object

The DS has the right to object to the processing of PD on grounds of the DS's particluar situation.

If processing is based on public interest/authority or legitimate interest.

Exception: If it is demonstrated that there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the DS or for the establishment, exercise or defence of legal claims.

Processing for direct marketing may always be objected to.

Article 21 (50, 59, 69, 70, 73, and 156).

Data protection impact assessment (DPIA)

DPIA is to carry out assessment of impact of the envisaged processing operations on the protection of PD prior to the processing.

Processing likely to result in a high risk to the rights of natural persons.

By using new technologies, and taking into account the nature, scope, context and purposes of the processing.

Involve the processor and the DPO.

Shall contain at least:

- A systematic descr. of envisaged processing operations and the purposes of the processing, incl. the legitimate interest pursued
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of DS
- Measures envisaged to address the risks, incl. safeguards, security measures and mechanisms to ensure protection of PD and to demonstrate compliance.

Article 35 (77, 84, 90 to 95).

Right of rectification

The DS shall have the right

- to rectify PD without undue delay.
- to have incomplete PD completed, incl. by means of providing a supplementary statement, taking into account the purposes of the processing.

Any rectification of PD shall be communicated to recipients the PD has already been disclosed to, unless this proves impossible or involves disproportionate effort.

Article 16 and 19 (39, 59, 65, 66, 68, 73).

Restriction of processing

May be required by the DS if:

- The accuracy of the PD is contested by the DS (until the accuracy of the PD is verified)
- The processing is unlawful and the DS opposes the erasure of the PD and requests the restriction of its use instead
- The controller no longer needs the PD for the purposes of the processing, but it is required by the DS for the establishment, exercise or defence of legal claims
- The DS has objected to processing pursuant to Article 21(1) pending verification as to whether the legitimate grounds of the controller override those of the DS.

Where processing has been restricted , such PD shall, with the exception of storage, only be processed with the DS's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person etc.

A DS who has obtained restriction of processing shall be informed by the controller before the restriction of processing is lifted.

Any rectification of PD shall be communicated to recipients the PD has already been disclosed to, unless this proves impossible or involves disproportionate effort.

Article 18 and 19 (67 and 156).

Data protection officer (DPO)

A DPO shall be designated if:

- processing by a public authority or body
- core activities require regular and systematic monitoring on a large scale
- core activities on processing on a large scale of special categories of data/criminal convictions and offences

Requirements of the DPO:

- Expert knowledge of data protection law and practises
- Independent

Position of the DPO:

- Involvement and consultation
- Contact point for supervisory authority and DSs

Article 37 til 39 (97).

Jan Sandtrø
jan.sandtro@dlapiper.com
+4799731934
linkedin.com/in/sandtro/