New and significantly changed concepts

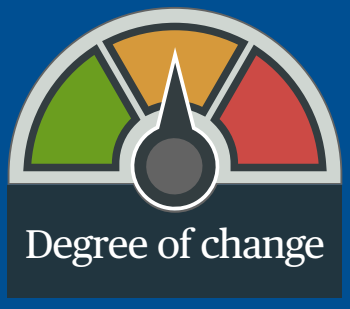
At a glance

The GDPR will introduce significant changes, including via the following concepts:

- *Transparency and Consent* – i.e. the information to be provided to and permissions required from individuals to justify use of their personal data. The GDPR's requirements, including for consent to be unambiguous and not to be assumed from inaction, will mean that many data protection notices will need to be amended.
- *Children and consent* – for online services which rely on consent to processing, verifiable parental consent is required for use of a child's personal data. Member States are free to set their own rules for those aged 13-15 (inclusive). If they choose not to, parental consent is required for children under 16.
- *Regulated data* – the definitions of "Personal Data" and "Sensitive Data" have been expanded, for instance, the latter now includes genetic and biometric data.
- *Pseudonymisation* – a privacy enhancing technique where information which allows data to be attributed to a specific person is held separately and subject to technical and organisational measures to ensure non-attribution.
- *Personal Data Breach* – a new security breach communication law is introduced for all data controllers regardless of their sector.
- *Data protection by design and accountability* – organisations are required to adopt significant new technical and organisational measures to demonstrate their GDPR compliance.
- *Enhanced rights* – Data Subjects are given substantial rights including the right to be forgotten, data portability rights and the right to object to automated decision making.
- *Supervisory authorities and the EDPB* – regulator oversight of data protection will change significantly, including via the introduction of a new lead authority for certain organisations.

To do list

No action is required



The GDPR's provisions and the obligations which they bring are extensive, but the following stand out as material new, or varied, concepts. More detailed information on each appears elsewhere in this guide.

Consent

The conditions for obtaining consent have become stricter:

- the data subject must have the right to withdraw consent at any time; and
- there is a presumption that consent will not be valid unless separate consents are obtained for different processing activities and there is a presumption that forced, or 'omnibus', consent mechanisms will not be valid. Further guidance is expected but organisations will need to review existing consent mechanisms, to ensure they present genuine and granular choice.

Consent is not the only mechanism for justifying the processing of personal data. Concepts such as contractual necessity, compliance with a (Member State or EU) legal obligation or processing necessary for legitimate interests remain available.

For more information on this topic, see sections on consent; children; and sensitive data and lawful processing (under the chapter on principles).

Transparency

Organisations will need to provide extensive information to individuals about the processing of their personal data.

The GDPR combines the various transparency obligations which apply across the EU. The list of information to be provided runs to 6 pages in the GDPR, yet data controllers have to achieve what EU law makers have failed to do and must provide information in a concise, transparent, intelligible and easily accessible way.

The use of standardised icons is mooted in the GDPR and the Commission is given the option to choose to introduce these via delegated acts at a later stage.

For more information on this topic, see section on information notices

Children

Children under the age of 13 can never, themselves, give consent to the processing of their personal data in relation to online services.

For children between the ages of 13 and 15 (inclusive), the general rule is that if an organisation seeks consent to process their personal data, then parental consent must be obtained, unless the relevant individual Member State legislates to reduce the age threshold – although the threshold can never drop below 13 years of age.

Children aged 16 or older may give consent for the processing of their personal data themselves.

There are no specific rules relating to parental consent for offline data processing: usual Member State rules on capacity would apply here.

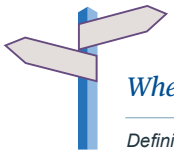
For more information on this topic, see section on children.

Personal data/ sensitive data ("special categories of data")

The GDPR applies to data from which a living individual is identified or identifiable (by anyone), whether directly or indirectly. The Directive's test of *'all means reasonably likely to be used'* to identify is retained.

The GDPR's recitals highlight that certain categories of online data may be personal – online identifiers, device identifiers, cookie IDs and IP addresses are referenced. In October 2016 the CJEU provided long awaited clarity on the status of dynamic IP addresses in the case of Patrick Breyer v Germany (C-582/14), holding that an IP address is personal data when held by an ISP, but does not constitute personal data if held by a party that does not have the "means likely reasonably to be used to identify the individual". Interestingly, the CJEU did not reference the Article 29 Working Party guidance that unique identifiers that "enable data subjects to be 'singled out' for the purpose of tracking user behaviour while browsing on different websites" are personal data (Opinion 188). It may, however, be unwise for those engaged in Online Behavioural Advertising or similar activities to read too much into the absence of this test in the CJEU judgment (at least post GDPR), as Recital 30 of the GDPR states that such identifiers will be personal data where used to create profiles of people and identify them.

"*Special categories of data"* (often referred to as sensitive data) are retained and extended – to cover genetic data and



Where can I find this?

Definitions *Article 4* *Various (predominantly 26-35)*

biometric data. As with the current Data Protection Directive, processing of such data is subject to more stringent conditions than other forms of personal data.

Pseudonymisation

A new definition, which refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific *"data subject"* without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Pseudonymised information is still a form of personal data, but the use of pseudonymisation is encouraged, for instance:

- it is a factor to be considered when determining if processing is *"incompatible"* with the purposes for which the personal data was originally collected and processed;
- it is included as an example of a technique which may satisfy requirements to implement *"privacy by design and by default"* (see section on data governance obligations);
- it may contribute to meeting the GDPR's data security obligations (see section on personal data breaches and notification); and
- for organisations wishing to use personal data for historical or scientific research or for statistical purposes, use of pseudonymous data is emphasised.

Personal data breach communication

The GDPR introduces a security breach communication framework for all data controllers regardless of the sector in which they operate.

Notification obligations (to supervisory authorities and to data subjects) are potentially triggered by *"accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".* For more information on this topic, see section on personal data breaches and notification.

Data protection by design/accountability

Organisations must be able to demonstrate their compliance with the GDPR's principles, including by adopting certain *"data protection by design"* measures (e.g. the use of pseudonymisation techniques), staff training programmes and adopting policies and procedures.

Where "high risk" processing will take place (such as monitoring activities, systematic evaluations or processing special categories of data), a detailed privacy impact assessment ("PIA") must be undertaken and documented. Where a PIA results in the conclusion that there is indeed a high, and unmitigated, risk for the data subjects, controllers must notify the supervisory authority and obtain its view on the adequacy of the measures proposed by the PIA to reduce the risks of processing.

Controllers and processors may decide to appoint a Data Protection Officer ("DPO"). This is obligatory for public sector bodies, those involved in certain listed sensitive processing or monitoring activities or where local law requires an appointment to be made (e.g. German law is likely to continue to require this after May 2018). Group companies can jointly appoint a DPO.

For more information on these topics see section on data governance obligations.

Enhanced rights for individuals

The GDPR enshrines a wide range of existing and new rights for individuals in respect of their personal data.

These include the right to be forgotten, the right to request the porting of one's personal data to a new organisation, the right to object to certain processing activities and also to decisions taken by automated processes.

For more information on these topics see section on information notices.

Supervisory authorities and the EDPB

Data protection regulators are referred to as supervisory authorities.

A single lead supervisory authority located in the Member State in which an organisation has its "main" establishment will regulate that organisation's compliance with the GDPR.

A European Data Protection Board (EDPB) will be created to (amongst many other things) issue opinions on particular issues and adjudicate on disputes arising from supervisory authority decisions.

For more information on this topic see individual rights.