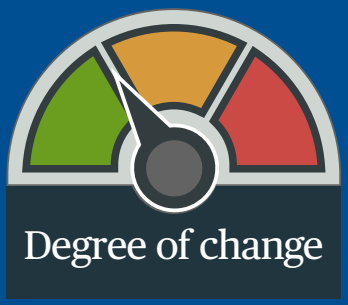
Sensitive data and lawful processing

At a glance

- "*Special categories of personal data*" (sensitive data) now expressly include *"genetic data"* and *"biometric data"* where processed *"to uniquely identify a person"*.
- The grounds for processing sensitive data under the GDPR broadly replicate those under the Data Protection Directive, although there are wider grounds in the area of health and healthcare management.
- There is also a broad ability for Member States to adduce new conditions (including limitations) regarding the processing of genetic, biometric or health data.

To do list

- ☐ Ensure you are clear about the grounds relied on by your organisation to process sensitive data, and check these grounds will still be applicable under the GDPR;
- ☐ Where relying on consent, ensure the quality of consent meets new requirements in relation to the collection of consent (see section on consent);
- ☐ Consider whether rules on children are likely to affect you, and, if so, which national rules you will need to follow when obtaining their consent (see section on children for further details); and
- ☐ If you process substantial amounts of genetic, biometric or health data, ensure you pay attention to national developments as Member States have a broad right to impose further conditions - including restrictions - on the grounds set out in the GDPR.



Commentary

Article 9(2) sets out the circumstances in which the processing of *sensitive personal data* which is otherwise prohibited, may take place. The following categories of data are considered *"sensitive"*, as set out in Article 9(1):

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data (*new*); and
- biometric data where processed to uniquely identify a person (*new*).

Note that Recital 51 suggests that the processing of photographs will not automatically be considered as sensitive processing (as has been the case in some Member States to date); photographs will be covered only to the extent they allow the unique identification or authentication of an individual as a biometric (such as when used as part of an electronic passport).

The grounds for processing sensitive data broadly replicate those in the Data Protection Directive. These are:

9(2)(a) - Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

There is no change here, although new conditions for consent should be considered (see section on consent).

9(2)(b) - Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement

This expands slightly on the wording of the Data Protection Directive by making express reference to compliance with collective agreements and obligations under social security and social protection law.

9(2)(c) - Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent

This replicates an equivalent provision in the Data Protection Directive.

9(2)(d) - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

This replicates an equivalent provision in the Data Protection Directive.

9(2)(e) - Data manifestly made public by the data subject

This replicates an equivalent provision in the Data Protection Directive.

9(2)(f) - Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

The processing of data by courts acting in their judicial capacity is added to the equivalent provision in the Data Protection Directive.

9(2) (g) - Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures.

This enables Member States to extend by law the circumstances where sensitive data may be processed in the public interest.

9(2)(h) - Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

AND

9(2)(i) - 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 healthcare and of medicinal products or medical devices

These two provisions expand the equivalent provision in the Data Protection Directive and address acknowledged gaps in that Directive, by providing a formal legal justification for regulatory uses of healthcare data in the health and pharmaceutical sectors, and by providing for the sharing of health data with providers of social care

Both conditions require obligations of confidentiality to be in place by way of additional safeguards.

9(2)(j) - necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

This makes new provision for the processing of sensitive personal data for the purposes of archiving, research and statistics, subject to compliance with appropriate safeguards, including safeguards to ensure respect for the principle of data minimisation (see section on derogations and special conditions for further details).

Genetic, biometric, or health data

Member States are entitled, under Article 9(4) GDPR, to maintain or impose further conditions (including limitations) in respect of genetic, biometric or health data. As such, existing differences in approach on these topics will likely be maintained, and further divergence will be permitted. Entities that process these categories of data should continue to keep the development of relevant national law under review and consider the need for further lobbying work in this area.

Criminal convictions and offences

Data relating to criminal convictions and offences are not categorised as *"sensitive"* for the purposes of GDPR. This does not, however, amount to a change as (although the UK Data Protection Act treats personal data relating to criminal proceedings and convictions as sensitive data), data of this kind was not treated as sensitive data under the Data Protection Directive.

The rules under the GDPR in relation to data concerning criminal convictions and offences mirror those which applied under the Data Protection Directive. Article 10 provides that such data may be processed only under the control of official authority or where the processing is authorised by Union law or Member State law that provides appropriate safeguards. This provision is likely to lead to continued national divergence in this area.

Where can I find this?

Article 9 *Recitals 51-56*