General Data Protection Regulation (GDPR)

Jargon buster

Sanlam

Wealth

Anonymisation: The process of turning personal data into a form such that the data subject is no longer identifiable. GDPR does not apply to data that has been fully anonymised.

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of his or her personal data.

Data at rest: An information technology term referring to inactive data that is stored physically in any digital form.

Data controller: An entity that determines the purposes and meanxs of the processing of personal data.

Data erasure: The right (in certain circumstances) of the data subject to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially have third parties cease processing the data. Also known as 'right to be forgotten'.

Data in transit: An information technology term referring to data that flows over a network, whether public (such as the internet) or private.

Data in use: An information technology term referring to active data which is in use and stored in a temporary digital state.

Data inventory: A record of processing activities under the responsibility of a data controller.

Data minimisation: The principle that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Data portability: The right of the data subject to receive the personal data concerning him or her, which he or she has previously provided to the data controller, in a commonly used and machine-readable format and to transmit that data to another data controller.

Data processing: Any operation that is performed on personal data, whether or not by automated means, including collection, storage, retrieval, use or erasure.

Data processor: An entity that processes personal data on behalf of the data controller.

Data Protection Act: The UK legislation that introduced GDPR (and makes derogations and other related provisions relating to data protection).

Data protection by default: Appropriate technical and organisational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.

Data protection by design: Appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner. See also 'privacy by design'.

Data protection impact assessment: A new term introduced in GDPR referring to an assessment of the impact of processing operations on the protection of personal data, where processing is likely to result in a high risk to the rights and freedoms of individuals. Also known as 'privacy impact assessment'.

Data protection officer (DPO): An individual with expert knowledge of data protection law and practices who must be appointed where the processing in question involves regular and systematic monitoring of data subjects on a large scale, or where the processing is of special categories of data on a large scale.

Data protection principles: The fundamental principles of data protection:

(a) lawfulness, fairness and transparency;

(b) purpose limitation;

(c) data minimisation;

(d) accuracy;

(e) storage limitation; and

(f) integrity and confidentiality.

Data subject: An individual who can be identified, directly or indirectly, from personal data held, for example by reference to a name, National Insurance number or address.

Derogation: An exemption at member state level from provisions of GDPR.

Encrypted data: Personal data that is protected through technological measures to ensure that the data is only accessible/ readable by those with specified access.

Fair processing notice: See 'Privacy notice'.

General Data Protection Regulation (GDPR): The European data protection regulation (Regulation (EU) 2016/679) that applies in all EU member states. This applies in the UK regardless of Brexit.

Information Commissioner's Office (ICO): The UK supervisory authority responsible for monitoring the application of GDPR in the UK, in order to protect the fundamental rights and freedoms of individuals in relation to processing.

Joint data controllers: Where two or more controllers jointly determine the purposes and means of processing.

Lawful processing: Processing on one of the following bases:

(a) consent;

(b) performance of a contract;

(c) compliance with legislation;

(d) protection of the vital interests of an individual;

(e) performance of a task in the public interest; and

(f) legitimate interests of the controller or third party.

Legitimate interest: One of the lawful bases for processing.

Personal data: Any information relating to a data subject by which he or she can be identified, directly or indirectly.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Privacy by design: A principle that calls for the inclusion of data protection from the designing phase when planning new systems and processes, rather than as an addition. See 'Data protection by design'.

Privacy impact assessment: The ICO's existing term for what is now called a 'data protection impact assessment' under GDPR.

Privacy notice: Information to be provided to a data subject to ensure fair and transparent processing of his or her personal data. Also known as 'fair processing notice'.

Processing: See 'Data processing'.

Pseudonymisation: Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, so long as the additional data remains separate to ensure that the data subject cannot be identified.

Right to be forgotten: See 'Data erasure'.

Rights of data subjects: Data subjects have the following rights:

(a) information ('right to be informed');

(b) access;

(c) rectification;

(d) erasure ('right to be forgotten');

(e) restriction of processing;

(f) data portability;

(g) objection ('right to object'); and

(h) automated processing ('right not to be subject to decisions based solely on automated processing').

Sensitive data: See 'Special categories of personal data'.

Special categories of personal data: 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 the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Also known as 'sensitive data'.

Subject Access Request: A request by a data subject for information about whether or not personal data concerning him or her is being processed, and, where that is the case, the provision of access to the personal data and information, including on the purposes of the processing.

enq@sanlam.co.uk

sanlam.co.uk

1900/05.2020