EU Data Protection - glossary

Date : March 3, 2021

We've put together this glossary to help explain some of the terms used in data protection and in GDPR. If there's a term you think we should add let us know.

AVG = Algemene Verordening Gegevensbescherming, the term used sometimes for GDPR in the Netherlands (although increasingly GDPR is used too there).

Adequacy Decision = this commonly refers to a process by which the European Commission determines whether a country outside of the EU (such as the UK) offers an adequate level of data protection. The adoption of an Adequacy Decision involves:

i. A proposal from the European Commission
ii. An opinion of the EDPB
iii. Approval from representatives of EU countries
iv. The adoption of the decision by the European Commission

As at 15 February 2021, the following countries had received an Adequacy Decision:

- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Japan
- Jersey
- New Zealand
- Switzerland
- Uruguay

Agencia Espanola de Protección de Datos = the Spanish data protection regulator, often known as the AEPD.

Anonymisation = the method of processing personal data in order to irreversibly prevent identification. Organisations try and anonymise data to make it more secure and to help them comply with their data protection responsibilities. It is a complicated topic however – for example in 2014 the Article 28 Working Party issued a detailed Opinion (approx. 37 pages long) on anonymisation.

Article 29 Working Party (sometimes known as WP29) = the (sort of) predecessor of EDPB. WP29 was set up under the 1995 European Directive as an advisory body. It comprised representatives of the supervisory authorities for each EU member state, representatives of the EU institutions and a representative of the European Commission. It issued opinions on matters of common interest involving data protection across the EU but those opinions were advisory and need not be followed by any local DPA.

Autoriteit Persoonsgegevens = the Dutch DPA. The Autoriteit Persoonsgegevens (AP) replaced the former Dutch DPA, The College Bescherming Persoonsgegevens (CBP), in January 2016.

Binding Corporate Rules = a binding global code of practice based on EU privacy standards, reinforced by an organisation's internal compliance system, and which national regulators approve in accordance with their own legislation. More information at http://www.corderycompliance.com/an-international-summer-are-binding-corporate-rules-the-way-forward/. BCRs receive statutory footing for the first time in GDPR. BCRs are defined by GDPR Article 4(20) as "*personal data protection policies which are adhered to by a controller or processor established on*

the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings or a group of enterprises engaged in joint economic activity". The system of BCRs under GDPR is set out in Article 47 of GDPR. Post-Brexit the UK will also still recognise BCRs.

Biometric Data = Biometric Data has its own definition in GDPR which is "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*".

Brexit = from 31 January 2020 the UK ceased to be a member of the EU. This has implications for data protection.

In addition to EU GDPR, a slimmed down version of GDPR exists in the UK which is known as "UK GDPR". In this glossary, we use GDPR to mean EU GDPR and UK GDPR. You can find out more details about the post-Brexit regime at www.bit.ly/brexdpfaq

Commission for the Protection of Privacy (CPP) = the Belgium DPA.

Commission Nationale de l'Informatique et des Libertés = the French DPA, often referred to as CNIL.

Data = information which:

i. is processed electronically, including computer, CCTV, card access data;
ii. is not processed electronically but forms part of a relevant filing system, structured to allow easy access to information; or
iii. is part of an accessible record, relating, broadly, to health, education or other public service.

Data Controller = any person, partnership or company who determines how and for what purposes personal data is processed. A third party may carry out processing on the controller's behalf, although the data controller remains responsible for the processing.

Data Processor = a person, partnership or company who processes personal data for a data controller, other than the controller's employee. Outsourced IT and HR service providers may be processors.

Data Protection Commission = DPC, the DPA in Ireland, formerly known as the Data Protection Commissioner.

Data Protection Impact Assessment = DPIA. The successor to the PIA. See Privacy Impact Assessment below.

DPA = Data Protection Authority. Be aware of confusion as some refer to the current UK legislation as DPA rather than the more correct form of DPA 2018.

DPO = Data Protection Officer. GDPR Articles 37, 38 and 39 deal with DPOs, when they need to be appointed and what they are responsible for. GDPR Navigator has more details on the DPO role, including a specimen Job Description and Role Profile.

DPR = Data Protection Representative. The role of the DPR is not be confused with the role of the DPO. A DPR may need to be appointed under GDPR Article 27 where a data controller or data processor is not present in the EU and/or UK. There's more information on how DPRs work post-Brexit here www.bit.ly/brexdpfaq.

Data Subject = an individual, of any nationality and age, who is the subject of the personal data.

Datainspektionen = the Swedish data protection regulator.

Datatilsynet = the data protection regulator in Denmark.

DSRs = data subject rights – data subjects have a number of rights in GDPR including Subject Access Rights, the

Right to be Forgotten and the Right to Data Portability.

European Data Protection Board (EDPB) = a pan-EU data protection board which was created by GDPR. This is an independent body to replace the Article 29 Working Party. One of its functions is to act as a dispute resolution authority for disputes between DPAs in each country.

European Data Protection Supervisor (EDPS) = The EDPS is an independent institution of the EU whose focus is largely on the workings of the European Commission. The EDPS was established under Article 41.2 of Regulation 45/2001. EDPS also acts as the Secretariat of the EDPB. In its own right EDPS has published a number of influential papers on topics like Big Data Digital Ethics.

Garante = the Italian DPA, more formally known as the Garante Per la Protezione dei Dati Personali.

GDPR = General Data Protection Regulation.

Genetic Data = Genetic data has its own definition in GDPR which is "*personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*".

IDPC = The Office of the Information and Data Protection Commissioner, the DPA in Malta.

The Information Commissioner's Office = the DPA for the UK, often referred to as the ICO.

Information Society Services = one of the stated aims of GDPR in Recital 21 was to *"contribute to the proper functioning of the internal market by ensuring the free movement of Information Society Services between Member States"*. Information Society Services is a term which has been used by the EU in the past, for example in the Directive on Electronic Commerce in 2000. Information Society Services include e-commerce operations. There is a formal definition in Directive 2015/1535 which says that an Information Society Service is "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"*. There is also an illustrative list in Annex 1 of the 2015 Directive of the type of services that aren't included, the main exceptions being voice telephony, TV and radio broadcast.

Model Contract Clauses = obligations imposed on both the exporter and the importer of data between the EU and third countries to ensure that data transfer arrangements protect the rights and freedoms of data subjects.

Natural Person = a term that appears quite a bit in GDPR and it is used to distinguish a real individual from a legal person such as a company.

NIS Directive = EU legislation adopted by the European Parliament on 6 July 2016 dealing with cyber security. The NIS Directive is not part of GDPR but has some overlapping provisions in areas like data breach reporting. The NIS regime is currently being updated (see https://www.corderycompliance.com/client-alert-nis-2-directive/).

Notification = data protection notification is essentially a form of data protection registration – see registration below.

Personal Data Breach = this has a specific definition in GDPR Article 4(12) and means "*a 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*".

Personal Data = data relating to a living individual who can be identified from that data, either alone or with other information in the data controller's possession. GDPR has a wide definition which says *"'Personal Data' means information relating to an identified or identifiable natural person 'Data Subject'; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identity such as a name, an identification, location data, an online identifier or to one or more factors specific to the physical, physiological,*

genetic, mental, economic, cultural or social identity of that natural person". It is important to remember however that Personal Data does not have a set specific exclusive list of things that are Personal Data, like the lists that define PII in some US laws. It includes opinions about, and intentions in relation to the data subject. Personal data can therefore include names, addresses, National Insurance (social security) numbers and CCTV images of individuals. This definition is expanded by GDPR Recital 26 and GDPR Article 4.

Privacy Impact Assessment = a privacy impact assessment (often known as a PIA) is a process to identify data protection and privacy risk. PIAs were developed by the UK ICO who first published their PIA handbook in December 2007. GDPR features PIAs (now called data protection impact assessments or DPIAs) in GDPR Article 35. In some cases (outlined in GDPR Article 35) DPIAs will be mandatory. They are effectively a risk assessment looking at data protection risks. There is no set format but we have provided tailored made DPIA processes for organisations and handbooks and training. DPIAs are subject to inspection by DPAs and in some cases prior authorisation to data processing will be required where a DPIA shows an unacceptable level of risk. There is more information on DPIAs in our GDPR FAQs.

Privacy Shield = the replacement scheme for Safe Harbor announced by the European Commission in February 2016. Privacy Shield no longer exists as a safe method for data transfer. More information at www.bit.ly/pshielddead.

Processing = obtaining, recording, holding, or carrying out any operation on personal data. It includes organisation or alteration; retrieval or use; disclosure and anonymisation, blocking or destruction. Most operations in relation to personal data will constitute processing.

Pseudonymisation = often confused with anonymisation but with pseudonymisation the individual can still be identified – for example at its most basic level changing an employee's name to an identification number instead and removing all of their other personal details could be pseudonymisation. WP29 in its paper on anonymisation has warned of the dangers of confusing pseudonymisation and anonymisation. They say "*pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a data set with the original identity of a data subject, and is accordingly a useful security measure*".

Registration = it was previously a requirement of national data protection law in a number of countries (for example Ireland, Malta, Poland, The Netherlands and UK) to register with the data protection authority. The general data protection registration requirement was abolished across Europe by GDPR although some registration obligations may remain, for example, where a DPIA discloses substantial risk which cannot be mitigated. The UK Data Protection Act 2018 retains a registration requirement for the UK.

RGPD = the initials used for GDPR in Spain and France.

Right to be Forgotten = the Right to be Forgotten (also called RTBF or the Right to Erasure) is contained in Article 17 of GDPR. The statutory Right to be Forgotten in GDPR is not to be confused with the Right to be Forgotten created by the 13 May 2014 ruling of the European Court of Justice (ECJ) in the Google case which you can read about at http://www.corderycompliance.com/european-court-google-ruling/. Article 17 of GDPR created the right of a data subject "*to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*" subject to a number of grounds laid down in GDPR. In some circumstances the Right to be Forgotten also obliges the data controller to contact other data controllers asking them to erase the data.

Right to Data Portability = this is a right created by GDPR Article 20. This right allows data subjects, in certain circumstances, to move their data from one company to another in re-usable form. Data subjects must usually be given a notice about the Right to Data Portability before collecting their data. There is a more detailed definition of the Right to Data Portability and when it applies in Cordery GDPR Navigator.

RODO = the Polish name for GDPR.

SA = Supervisory Authority – effectively the new name for a Data Protection Authority (DPA).

Safe Harbor = the now-defunct arrangement between the US Department of Commerce and the European Commission which was designed to allow personal data to be exported from the EU to the US which, in the European Court judgment in the 6 October 2015 case of Maximillian Schrems -v- Data Protection Commissioner, was held invalid in particular due to the lack of protection it afforded EU personal data in the US. Later replaced by the EU-US Privacy Shield (see Privacy Shield above). More information at http://www.corderycompliance.com/category/safe-harbor/.

SAR = A Subject Access Request. This is a request made by an individual who wants to see a copy of the information an organisation holds about them. More specifically, an individual is entitled to the following: to be told whether any personal data is being processed; to be given a description of the personal data, the reasons it is being processed, and, whether it will be given to any other organisations or people; to be given a copy of the information comprising the data; and, to be given the details of the source of the data, where this is available. Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. SARs also exist under domestic data protection legislation – see for example the UK Data Protection Act 2018. Under GDPR, responses to a SAR should be "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language…*". Be aware however of the possible confusion – some use an SAR to stand for a Suspicious Activity Report which is a key feature of money laundering legislation. SARs are also known as DSARs.

SCC = this stands for Standard Contractual Clauses – see Model Contract Clauses above.

Sensitive Personal Data = the old term for Special Categories of Personal Data (see below).

Special Categories of Personal Data = GDPR defines Special Categories of Personal Data as follows:

i. racial or ethnic origin;
ii. political opinions;
iii. religious or philosophical beliefs;
iv. trade union membership;
v. the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
vi. data concerning health; or
vii. data concerning a natural person's sex life or sexual orientation.

Subject Access Request = see "*SAR*" above.

TOMs = technical and organisational measures. Under GDPR Article 32 organisations must implement appropriate technical and organisational measures to keep personal data secure. TOMs are not defined under GDPR but we've worked on producing TOMs tables to enable audits or third party reviews.

UK GDPR = the UK has its own post-Brexit GDPR regime. More details are at www.bit.ly/brexdpfaq

Urz?d Ochrony Danych Osobowych = the Polish DPA. This is the new name for what was formerly the Generalny Inspektor Ochrony Danych Osobowych (or GIODO).

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com