EU Data Protection - glossary

Date : January 22, 2016

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

Agencia de Protecccíón 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 alone.

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

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 An international summer: are binding corporate rules the way forward?

Commission Nationale de l'Informatique et des Libertés = the French data protection regulator, 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 are 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 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 Impact Assessment = DPIA. The successor to the PIA. See Privacy Impact Assessment below.

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.

Garante = the Italian data protection authority, more formally known as the Garante per la protezione dei dati personali.

ICO = The Information Commissioner's Office, the data protection regulator for the UK.

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.

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. 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.

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. The GDPR features PIAs (to be called data protection impact assessments or DPIAs) in Article 33 of the current draft of the GDPR. Saying "*where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*". In some cases (outlined in Article 33) 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 data protection regulators 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 proposed replacement scheme for Safe Harbor announced by the European Commission in February 2016. More information here.

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 employees name to an identification number instead and removing all of their other personal details could be pseudonymisation. The Article 29 Working Party in its paper on anonymisation have 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."*

Safe Harbor = the arrangement between the US Department of Commerce and the European Commission designed to allow personal data to be exported from the EU to the US which, further to 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. More information here.

For more information please contact Jonathan Armstrong, Gayle McFarlane or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

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

Gayle McFarlane, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1786

gayle.mcfarlane@corderycompliance.com