Okta GDPR Glossary

Is your organisation looking for a clear and simple explanation of key terms associated with the European Union's ("EU") General Data Protection Regulation ("GDPR")?

This glossary helps define key terms and will assist you in navigating Okta's GDPR White Paper and the wide range of published material that exists about the new laws.

For legal advice regarding your organisation's GDPR compliance needs, be sure to consult your organisation's lawyer. This sample glossary does not constitute legal advice and is provided for informational purposes only.

Article 29 Working Party—Established by the Data Protection Directive of 1995, this body is made up of a representative from the data protection authority of each member state of the European Union, as well as the European Data Protection Supervisor and the European Commission. The mission of the Article 29 Working Party is to provide expert advice to EU members about data protection, promote the consistent application of the Data Protection Directive in the EU, give the European Commission an opinion on laws affecting personal data, and make recommendations to the public about the processing of personal data and privacy in the EU.

Data controller—Under the GDPR, this is any individual or entity that exercises control over the processing of personal data of EU individuals and decides which personal data is to be collected.

Data flows—This refers to the flow of personal data throughout an organisation's technical infrastructure, including how it enters an organisation, who has access to it, where it is held and for how long, and whether it is transferred to or from third parties. Organisations benefit from "mapping" their data flows (i.e. creating diagrams that illustrate the paths on which personal data flows).

Data portability—The GDPR includes provisions regarding a data subject's ability to transfer his/her personal data from one processing system into another without hindrance by the data controller. The data controller also must provide the data subject's personal data to the individual in a commonly used, open-standard electronic format.

Data processor—Under the GDPR, a data processor is an individual or entity that acts at the direction of a data controller to collect, store, retrieve, or delete personal data.

Data Protection Authorities (DPAs)—Authorities established by the individual EU member states that are tasked with protecting the personal information of their citizens by enforcing EU data protection law. Each DPA is a member of the Article 29 Working Party.

Data Protection Directive—This 1995 directive adopted by the EU regulated the processing of personal data of EU individuals, and first established Data Protection Authorities in each EU member state. Because it was a directive, implementation was left up to the discretion of EU member states. The GDPR supersedes the Data Protection Directive in an effort to unify and streamline European data privacy laws.

Data Protection Officer (DPO)–The GDPR requires that organisations that process or store large amounts of personal data appoint individuals to this position, depending on several variables. Data Protection Officers are responsible for implementing the GDPR within the organisation and ensuring continuing compliance. Organisations should evaluate whether they need to appoint a Data Protection Officer with input from their own legal team.

Data subject–An EU individual whose personal data is subject to the GDPR.

Erasure request–A data subject's request that an organisation delete his/her personal data when it is no longer needed for its original purpose.

General Data Protection Regulation ("GDPR")–Approved by the European Parliament, the Council of the European Union, and the European Commission in 2016, the General Data Protection Regulation ("GDPR") is intended to unify and streamline data protection regulations for all citizens of the EU, as well as regulate citizen data exported outside of the EU. The GDPR's enforcement date is May 25, 2018.

Identity and Access Management (IAM)–The security discipline that enables the right individuals to access the right resources at the right times for the right reasons. Okta offers a range of enterprise IAM solutions.

Lifecycle Management–An Okta solution that can provide a map of which individuals in an organisation have access to certain types of personal data.

Multi-Factor Authentication (MFA)–A security process that requires multiple authentication factors based on the context of an authentication event to verify a user's identity. MFA can be integrated with apps and VPNs. Okta offers an Adaptive MFA solution that integrates with the entire organisation.

Open standard electronic format–A data provision format that is available to the public and in wide use. The GDPR requires that upon request from a data subject, a data controller provide personal data in this format so that it may be transferred from one electronic processing system to another. Examples include Comma Separated files (CSV) or other Text formats.

Personal data–Any information that identifies or could be used to identify an individual. This includes email addresses and employee ID numbers, as well as IP addresses and geolocation data. The GDPR is meant to be future-proof and therefore does not contain a bounded definition of what constitutes personal data.

Privacy by design–Mandated by the GDPR, privacy by design is an approach to systems and application design that takes privacy into account during the engineering process for any system that collects, processes, or stores personal data. This regulation requires that from the onset of the system or process development, a data controller use appropriate technical and organisational measures to protect personal data.

Right of access by the data subject–Under the GDPR, a data subject may make a written request to any data controller to confirm whether their personal data is being processed, where, for what purpose, and whether it will be given to any other organisations or people. The individual has the right to gain access to this data.

Right to data portability–A data subject must be able to obtain and reuse their personal data by transferring it from one processing system to another without interference from the data controller. The regulation also requires that the data be provided in a commonly used open standard electronic format by the data controller.

Right to erasure–The GDPR allows individuals to request that data controllers erase their personal data if it is no longer necessary for its original purpose, they withdraw their consent to the organisation having this data, the data is being used unlawfully, or the data does not comply with other regulations.

Sensitive personal data–Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Single Sign-On (SSO)—A software system that allows a user to log in with one ID and password (and/or other authentication credentials) in order to access a system or connected systems, rather than using multiple usernames and passwords for each individual application. Okta offers an SSO solution with reliable integration to all web and mobile apps.

Universal Directory—An Okta solution that may store data for employees, partners, and customers through fully encrypted and unified user profiles. It is capable of managing hundreds of millions of users.

Are you an IT manager looking to open the conversation with your legal team about the GDPR? Okta's Legal Checklist for IT Managers will get you started!