Terminology in the IDPro Body of Knowledge

Heather Flanagan, editor - @ 2020 IDPro

Term	Definition	Source
Access Control	Controlling who can have access to data, systems, services, resources, locations. The 'Who' can be a user, a device or thing, a service	Introduction to Access Control
Access Governance	The assurance that all access has been given based on the correct decision criteria and parameters	Introduction to Access Control
Access Management	Use of identity information to provide access control to protected resources such as computer systems, databases, or physical spaces.	Introduction to IAM Architecture
Access Policy	Definition of the rules to allow or disallow access to secured objects.	Introduction to Access Control
Access Requester	The person, process, system, or thing that seeks to access a protected resource.	Introduction to Access Control
Access Supplier	The component granting access to data, systems, services after the access policy requirements (set in the Policy Administration Point) have been met by the Access Requester.	Introduction to Access Control
Accountability	The obligation of a person to accept the results of one's actions, be they positive or negative. This person is probably also a species of an owner.	Introduction to Access Control

Agile Project Management	A framework that uses a continuous, iterative process to deliver a defined piece of functionality, typically a component of a product or service. Scrum is a popular framework (https://www.scrumalliance.org/about-scrum/overview)	Introduction to IAM Project Management
Architecture	Framework for the design, deployment, and operation of an information technology infrastructure. It provides a structure whereby an organization can standardize the technology it uses and align its IT infrastructure with digital transformation policy, IT development plans, and business goals.	Introduction to IAM Architecture
Architecture Overview	Describes the architecture components required for supporting IAM across the enterprise.	Introduction to IAM Architecture
Architecture Patterns	Identifies the essential patterns that categorize the IT infrastructure architecture in an organization and will guide the deployment choices for IAM solutions.	Introduction to IAM Architecture
Authentication	The ability to prove that a user or application is trustworthy and has the authority to access a protected resource by validating credentials of an access requester (a user, a process, a system, or a thing).	Introduction to Access Control
Authorization	Determining a user's rights to access functionality with a computer application and the level at which that access should be granted. In most cases, an 'authority' defines and grants access, but in some cases, access is granted because of inherent rights	Introduction to Access Control

	(like patient access to his/her own medical data)	
Ceremonies	Predictable interactions that users can infrequently navigate in a well-watched place	Introduction to Identity – Part 2: Access Control
Consent	Permission for something to happen or agreement to do something.	Introduction to Privacy and Compliance for Consumers
Consumer Protection Law	Laws and regulations that are designed to protect the rights of individual consumers and to stop unfair, deceptive, and fraudulent business practices.	Laws Governing Identity Systems
Contract Law	Laws that relate to making and enforcing agreements between or among separate parties.	Laws Governing Identity Systems
Data Controller	Defined in Article 4(7) of the GDPR: "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;". This article uses the term "organisation" as a synonym for "data controller", since organisations involved in IAM will normally be data controllers.	An Introduction to the GDPR
Data Mapping	"a system of cataloguing what data you collect, how it's used, where it's stored, and how it travels throughout your organization and beyond."	Impact of GDPR on Identity and Access Management
Data Processor	Defined in Article 4(8) of the GDPR for situations where an organisation processes personal data solely on the instructions of others. A Data Processor must not determine the	An Introduction to the GDPR

	purposes of processing, for example by processing in its own interests, or, beyond limited technical choices, the means of doing so. Data Processors are regulated by Article 28: in particular they must have a contract with the Data Controller that covers all the subjects listed in Article 28(3). Data Processors are excluded from some, but not all, of the liabilities and duties of Data Controllers.	
Data Protection by Design	Data protection through technology design. See GDPR Article 25 for more detail	Impact of GDPR on Identity and Access Management
Data Protection Officer	An individual who must be appointed in any organization that processes any data defined by the GDPR as sensitive. The DPO is responsible for "Working towards the compliance with all relevant data protection laws, monitoring specific processes, such as data protection impact assessments, increasing employee awareness for data protection and training them accordingly, as well as collaborating with the supervisory authorities."(See GDPR Articles 35, 37, 38, and 39 for more detail)	Impact of GDPR on Identity and Access Management
Data Subject	Defined in Article 4(1) of the GDPR (see "Personal Data" above) as the formal term for the human to whom personal data relates. This article uses the term "individual" as a synonym for "data subject".	An Introduction to the GDPR
Delegated Authorization Framework	An access control framework that decouples authentication from authorization, allowing the password to stay local and protected	Introduction to Identity – Part 2: Access Control

Enterprise Architecture	An architecture covering all components of the information technology (IT) environment	Introduction to IAM Architecture
External identifier	The means by which a person in control of a digital identity refers to that identity when interacting with a system	Identifiers and Usernames
Federated Identity	The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems	Introduction to Identity – Part 2: Access Control
Fraud Law	Laws that protect against the intentional misrepresentation of information made by one person to another, with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage.	Laws Governing Identity Systems
Gantt Chart	A popular schedule format that displays both activity and timeframes in a single chart	Intro to Project Management
General Data Protection Act (GDPR)	Formally, Regulation 2016/679 of the European Union, in force May 25, 2018. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679	An Introduction to the GDPR
Identification	Uniquely establish a user of a system or application.	Introduction to Access Control
Identity Governance and Administration (IGA)	Includes the collection and use of identity information as well as the governance processes that ensure the right person has the right access to the right systems at the right time.	Introduction to IAM Architecture

Identity Theft Law	Laws governing crimes in which the perpetrator gains access to sensitive personal information belonging to the victim (such as birth dates, passwords, email addresses, driver's license numbers, social security numbers, financial records, etc.), and then uses this information to impersonate the victim for personal gain, such as to commit fraud, establish credit in the victim's name, or access the victim's accounts.	Laws Governing Identity Systems
Internal identifier	The way an identity management system refers to a digital identity	Identifiers and Usernames
Least Privilege	Also known as the Principle of Least Privilege; a resource, such as a user, must only be able to access the resources (e.g., applications, data) that are necessary for it to function.	Introduction to Identity – Part 2: Access Control
Multi-Factor Authentication (MFA)	An approach whereby a user's identity is validated to the trust level required according to a security policy for a resource being accessed using more than one factor (something you know (e.g., password), something you have (e.g., smartphone), something you are (e.g., fingerprint).	Introduction to Access Control
Personal Data	Defined in Article 4(1) of the GDPR: "'personal data' means any 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 identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic,	An Introduction to the GDPR

	mental, economic, cultural or social identity of that natural person;". Note: "natural person" (human) is used to distinguish from companies and other corporate entities that are "legal persons".	
Personal Data	Personal data are any information which are related to an identified or identifiable natural person.	Impact of GDPR on Identity and Access Management
Policy Access Point (PAP)	The location where the different types of owners define the access policy.	Introduction to Access Control
Policy Decision Point (PDP)	The policy engine validating Access requests and provided attributed against the Access Policy (as defined in the Policy Administration Point).	Introduction to Access Control
Policy Enforcement Point (PEP)	The authority that will only let an Access Requester connect to the Access Supplier if the Policy Decision Point allows it.	Introduction to Access Control
Policy Engine	It is a security component that validates whether an actor is allowed to access a protected resource, following the requirements in an access policy.	Introduction to Access Control
Policy Information Point	The authority that refers to the (external) trusted providers of attributes that will be used in the Access Decision. An example is the myacclaim.com service that administers Open Badges of certifications, such as CISSP and MSCP.	Introduction to Access Control
Privacy	An abstract concept, with no single, common definition	Introduction to Privacy and Compliance for Consumers
Privacy Law	Laws that regulate the collection, use, storage, and transfer of personal data	Laws Governing Identity Systems

	relating to identified or identifiable individuals.	
Processing	Defined in Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Note that even this long list of activities is not exhaustive: other activities may also fall within the definition of "processing". Additional rules, in Article 22, apply to "automated individual decision-making, including profiling". These generally have the effect of strengthening the rights of information and objection described later and may limit the use of automation for some high-impact decisions.	An Introduction to the GDPR
Project	A time-limited activity to achieve a defined outcome(s)	Intro to Project Management
Project Charter	Documented authority for the project manager to proceed with a project; it will usually include a succinct statement of the project's purpose	Intro to Project Management
Project Plan	A document that describes a project; it will usually include a scope statement, schedule, resource plan, communications plan, and quality plan	Intro to Project Management

Protected Resource	A system, a process, a service, an information object, or even a physical location that is subject to access control as defined by the owner of the resource and by other stakeholders, such as a business process owner or Risk manager.	Introduction to Access Control
Schedule	A document that defines the activity and resources required to achieve the planned deliverable(s) and outcome(s)	Intro to Project Management
Special Category Data (SCD)	Categories of data that are regarded as particularly sensitive, so subject to additional regulation. Defined in Article 9(1) of the GDPR as "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"; Article 10's "personal data relating to criminal convictions and offences" requires similar treatment, so is normally considered as another category of SCD.	An Introduction to the GDPR
Task	Lowest level of defined activity; multiple tasks will typically be grouped into stages of project phases	Intro to Project Management
Tort Law	The body of law that covers situations where one person's behavior causes injury, suffering, unfair loss, or harm to another person, giving the injured person (or the person suffering damages) a right to bring a civil lawsuit for compensation from the person who caused the injury. Examples	Laws Governing Identity Systems

	include battery, fraud, defamation, negligence, and strict liability.	
Trust Federation	a trust framework between multiple entities with the purpose of leveraging identity and access management information in a controlled fashion	Introduction to Identity – Part 2: Access Control
Username	a common term used for an external identifier	Identifiers and Usernames
Zero Trust	From NIST Draft Special Publication 800-207, “Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet)”	Introduction to Identity – Part 2: Access Control