LAPSI
The European Thematic Network on Legal Aspects of Public Sector Information

PSI Glossary

Accessibility
There are several elements included in accessibility. Some examples from literature: e.g. Beers makes a distinction between the legal availability of information, the practical accessibility and the usability. Bovens makes a distinction between physical accessibility, financial accessibility, and intellectual accessibility. Baten and Van der Starre discern five elements of accessibility: 1) access to the medium on which the information is made available; 2) the possibility or the means to find the information; 3) the intelligible character of the information; 4) the intelligible presentation of the content; 5) the price for consulting the information.

Anonymization
The process of turning data that could result into the identification of individuals.
Source:
http://opendatamanual.org/glossary.html

Article 29 Working Party
The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States. It is composed of representatives of the national supervisory authorities in the Member States; a representative of the European Data Protection Supervisor (EDPS); and a representative of the European Commission (the latter also provides the secretariat for the Working Party).
Source:
http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#article29

Data controller
The data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law (Article 2, d) of Directive 95/46/EC).
In particular, the controller has the duties of ensuring the quality of data and of notifying the processing operation to the national data protection authorities (NSAs). In addition, the data controller is also responsible for the security measures protecting the data.

This work is distributed under a Creative Commons Attribution 3.0 (Unported) License

The controller is also the person or entity that receives a request from a data subject to exercise his or her rights.
Source:
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74

Data processor
The processor shall mean "*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the (data) controller*" (Article 2, e) of Directive 95/46/EC).
Source:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Dir_1995_46_EN.pdf

Data minimization
The principle of "data minimization" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.
The data minimization principle derives from Article 6.1(b) and (c) of Directive 95/46/EC and Article 4.1(b) and (c) of Regulation EC (No) 45/2001, which provide that personal data must be "*collected for specified, explicit and legitimate purposes*" and must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*".
Source:
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74

Data protection authority or National Supervisory Authorities (NSAs)
A data protection authority is an independent body which is in charge of monitoring the processing of personal data within its jurisdiction (country, region or international organization); providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data; and hearing complaints lodged by citizens with regard to the protection of their data protection rights.
According to Article 28 of Directive 95/46/EC, each Member State shall establish in its territory at least one data protection authority, which shall be endowed with investigative powers (such as access to data, collection of information, etc.), effective powers of intervention (power to order the erasure of data, to impose a ban on a processing, etc.), and the power to start legal proceedings when data protection law has been violated.
National data protection authorities have been established in almost all European countries, as well as in many other countries worldwide.
At the EU level, it is the EDPS who ensures these tasks within EU institutions.
Source:
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74

Data Protection Directive 95/46/EC
Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (also known as "Data Protection Directive") is the centrepiece legislation at EU level in the field of data protection.
The Directive is a framework law, meaning that it is implemented in EU Member States through

national laws.
It aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when the processing is lawful. The guidelines mainly relate to the quality of the data; the legitimacy of the processing; the processing of special categories of data; information to be given to the data subject; the data subject's right of access to data; the right to object to the processing of data; the confidentiality and security of processing; and the notification of the processing to a supervisory authority (NSAs).
The Directive also sets out principles for the transfer of personal data to third countries and provides for the establishment of data protection authorities (NSAs) in each EU Member State.
Source:
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74
On 25th January 2012 the EC has launched its "Proposal of Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", which should replace the Directive 95/46/EC.
Source:
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Data subject
The data subject is the person whose personal data are collected, held or processed.
According to Article 2, a) of Directive 95/46/EC he/she is "*an identified or identifiable natural person to whom specific personal data relates*".
Some Member States also consider as 'data subject' a legal person (i.e. an enterprise).

Document
Document is defined in the PSI directive as: "*(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording); (b) any part of such content*" (article 2.3).

The European Data Protection Supervisor (EDPS)
The EDPS is an independent supervisory authority established in accordance with Regulation (EC) No 45/2001, on the basis of Article 286 of the EC Treaty. His mission is to ensure that the fundamental rights and freedoms of individuals - in particular their privacy - are respected when the EU institutions and bodies process personal data.
The EDPS is responsible for monitoring and ensuring that the provisions of Regulation 45/2001, as well as other Community acts on the protection of fundamental rights and freedoms, are complied with when EC institutions and bodies process personal data (supervisory tasks); advising the EC institutions and bodies on all matters relating to the processing of personal data. This includes consultation on proposals for legislation and monitoring new developments that have an impact on the protection of personal data (consultative tasks); and cooperating with national supervisory authorities and supervisory bodies in the "third pillar" of the EU with a view to improving consistency in the protection of personal data (cooperative tasks).
The EDPS also intervenes in cases before the Court of Justice of the European Communities.
Source:
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/75

Exclusive Arrangements
Contracts or other arrangements between the public sector bodies and third parties providing for exclusive rights to use public sector information. Exclusive arrangement might be for example a license agreement for re-use of public sector information or even a service agreement granting a

service provider exclusive rights to information that are being processed in contracted public sector information system. Unless reasoned by specific social or security interest, exclusive arrangements are prohibited and *per se* unenforceable.

Geo-data
Also known as spatial data, geospacial data or geographic data. The syllable “Geo” implies that the dataset has a spatial component that allows to georeference the described phenomena to a location or region on the earth. Therefore Geo-Data can be defined as data that identifies the geographic location of features and boundaries on the earth, such as natural or constructed features, oceans, and more. Spatial data is usually stored as coordinates and topology, and is data that can be mapped. Geo-data is often accessed or analysed through Geographic Information Systems (GIS). Geo-data is the most important and often the most expensive ingredient of a GIS. It can be linked to other data sources using spatial, temporal or thematic relations. Based on Geo-data one can do queries, spatial analysis and simulations.
Source:
http://geodata.ethz.ch/geovite/tutorials/L1IntroToGeodata/en/text/L1IntroToGeodata.pdf;
http://www.webopedia.com/TERM/S/spatial_data.html

Spatial data is defined in the INSPIRE directive as “*any data with a direct or indirect reference to a specific location or geographical area*” (article 3.2).

Interoperability
Is a measure of the degree to which various organizations or individuals are able to operate together to achieve a common goal. It is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. Interoperability is an enabler for coalition building. It facilitates meaningful contributions by coalition partners.
Source:
http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1235/MR1235.chap2.pdf

Location data
Any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of someone using a publicly available electronic communications service.
Source:
http://ec.europa.eu/justice/data-protection/glossary/index_en.htm

Marginal cost
In economics, marginal cost is defined as the change in the total cost entailed by the production of a further unit of a good. In the PSI-related literature and legislation, marginal cost is often applied to the reproduction and dissemination activities, i.e. the cost of making available for reuse one more unit of PSI. In a digital environment, marginal cost of reproduction and dissemination tends to zero.

Marginal cost pricing
With "marginal cost pricing" we intend the application of charges aimed at recouping only marginal costs of reproduction and dissemination (the latter therefore representing a cap for charges). Under this regime, the price applied to one unit of PSI cannot overcome its (marginal) cost of reproduction and dissemination.

Metadata
In the INSPIRE directive, metadata is defined as "*information describing spatial data sets and spatial data services and making it possible to discover, inventory and use them*". This definition could also be used for non-spatial information.

Open Data
According with the 'Open Definition' provided by the Open Knowledge Foundation, we assume that "*A piece of content or data is open if anyone is free to use, reuse, and redistribute it - subject only, at most, to the requirement to attribute and share-alike*". This definition implicitly encompasses technological aspects (meaning that datasets are machine readable and made available in open formats) and legal aspects (meaning that datasets are accessible, reusable and not subject to intellectual property rights or other legal constraints preventing copy, redistribution and reuse).

Personal data
Personal data shall mean any information relating to an identified or identifiable natural person (so called 'data subject'): an identifiable person is one who "*can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*" (Article 2, a) of Directive 95/46/EC).

Privacy by design
Privacy by design aims to build privacy and data protection upfront, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.
Source:
http://ec.europa.eu/justice/data-protection/glossary/index_en.htm

Privacy enhancing technologies (PETs)
They aim to protect privacy by eliminating or reducing personal data or by preventing undesired processing of personal data, without losing the functionality of the information system.
The use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules. It should result in making breaches of certain data protection rules more difficult and/or helping to detect them.
It either requires positive action by consumers, or should be directly included in the information systems.
Source:
http://ec.europa.eu/justice/data-protection/glossary/index_en.htm;
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/84

Processing of personal data
Processing shall mean "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*" (Article 2, b) of Directive 95/46/EC).

Public Sector Body

According to the PSI Directive definition, Public Sector Body means "*the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law*" (article 2.1).

Public Sector Information

PSI (acronym for Public Sector Information) can be defined as the wide range of information that public sector bodies collect, produce, reproduce and disseminate in many areas of activity while accomplishing their institutional tasks. PSI may include (among others) social, economic, geographical, cadastral, weather, tourist, and business information. Particularly, PSI acquires a specific legal meaning within the European Union, since it has been provided with a minimum set of rules contained in the Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information (often referred to as the PSI Directive).

Re-Use

According to the PSI Directive definition, re-use is "*the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. Exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute re-use*" (article 2.4).