Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1 Accountability

1.1 Definition[edit]

Accountability. Property that ensures that the actions of an entity may be traced uniquely to that entity.

In the GDPR context the principle of accountability intends to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with Data Protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence (such as audit reports) to demonstrate compliance to external stakeholders, including supervisory authorities.

1.2 Reference[edit]

- ISO/IEC 2382:2015
- EDPS Glossary

2 Adequacy Decision

2.1 Definition[edit]

An **Adequacy Decision** is a decision adopted by the European Commission on the basis of Article 45 of the GDPR, which establishes that a third country (i.e. a country not bound by the GDPR) or international organisation ensures an adequate level of protection of personal data.

Such a decision takes into account the country's domestic law, its supervisory authorities, and international commitments it has entered into.

The effect of such a decision is that personal data can flow from the EU Member States and the European Economic Area member countries to that third country, without any further requirements. The European Commission publishes a list of its adequacy decisions on its website

2.2 References[edit]

- https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- EDPS Glossary

3 Automated Individual Decision

3.1 Definition[edit]

An **Automated Individual Decision** is a decision which significantly affects a person and which is based solely on automated processing of personal data in order to evaluate this person.

Such an evaluation may relate to different personal aspects, such as

- performance at work
- Creditworthiness
- reliability
- conduct, etc.

Article 22 of Regulation (EU) 2016/679 and Article 24 of Regulation (EU) 2018/1725 lay down the right for individuals to object to decisions about them and solely based on automated means, unless certain conditions are fulfilled or appropriate safeguards are put in place.

3.2 See Also[edit]

- Automated Credit Decision

3.3 References[edit]

- EDPS Glossary

4 Best Available Techniques

4.1 Definition[edit]

In the context of GDPR, **Best Available Techniques** refer to the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU data protection framework. They are designed to prevent or mitigate risks on privacy and security.

Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control provides for the following definitions, which could be applied by analogy:

- "techniques" shall include both the technology used and the way in which the system is designed, built, maintained, operated and replaced;
- "available" techniques shall mean those developed on a scale which allows implementation in the relevant sector, under economically and technically viable conditions, taking into consideration the costs and advantages, whether or not the techniques are used or produced inside the Member State in question, as long as they are reasonably accessible to the operator;
- "best" shall mean most effective in achieving a high general level of protection.

4.2 References[edit]

- EDPS Glossary

5 Binding Corporate Rules

5.1 Definition[edit]

Binding Corporate Rules (BCRs) are a legal tool that can be used by multinational companies to ensure an adequate level of protection for the intra-group transfers of personal data from a country in the EU or the European Economic Area (EEA) to a third country.

The use of BCRs requires, in principle, the approval of each of the EU or EEA data protection authorities from whose country the data are to be transferred.

5.2 References[edit]

- EDPS Glossary

6 Biometrics

6.1 Definition[edit]

Biometrics (or biometric systems) are methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits.

Such methods have already been used for a long time. However, the new element which triggers Data Protection considerations is that a machine can now automatically conduct these methods and possibly recognise humans with measurable accuracy.

6.2 See Also[edit]

- ISCO Specialization 2120.6.1 Biometrician

6.3 References[edit]

- EDPS Glossary

7 Blockchain

7.1 Definition[edit]

Blockchain. It is a trust-less distributed data structure exchanging and storing data in blocks and linking each block to the previous block, using the hash of the previous block.

7.2 Use Cases in Risk Management[edit]

A number of use cases have been identified as potential areas where blockchain techologies may have an impact on improving Risk Management

- Risk Audit
- Risk Underwriting
- Counterparty Risk Management
- Fraud Risk Management
- Identity Theft Protection
- Liquidity Risk Management
- Capital Management
- Systemic Risk Management
- Operational Risk improvements

8 CCTV

8.1 Definition[edit]

CCTV stands for "closed circuit television". It is a television system comprised of a camera or a set of cameras monitoring a specific protected area, with additional equipment used for viewing and/or storing the CCTV footage. The term itself originates from the fact that, as opposed to broadcast television, CCTV is usually a "closed" rather than "open" system with a limited number of viewers.

CCTV has been traditionally used for surveillance in specific locations with increased security needs such as banks, airports, military installations. In addition, in industrial plants, CCTV equipment has been used to remotely observe processes, for example, in hazardous environments. Increasing use of CCTV in public places has caused debate over public surveillance versus privacy.

8.2 See Also[edit]

- Video Surveillance

8.3 References[edit]

- EDPS Glossary

9 Cloud Computing

9.1 Contents

9.2 Definition[edit]

Cloud Computing. It is a computing capability that provides convenient and on-demand network access to a shared pool of configurable computing resources. These resources can be rapidly provisioned and released with minimal management effort or vendor interaction.

Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand. It is a "paradigm shift" following the shift from mainframe to client?server in the early 1980s.

Cloud computing describes a new consumption and delivery model for IT services based on the Internet, and it typically involves the provision of dynamically scalable and often virtualised resources as a service over the Internet. It is a by-product and consequence of the ease-of-access to remote computing sites provided by the Internet.

9.2.1 Characteristics[edit]

Cloud computing has six essential characteristics:

- pay-per-use
- self-service
- broad network access
- resource pooling
- rapid elasticity, and
- measured service.

9.2.2 Modes[edit]

Cloud computing can be public, private, or hybrid. In general terms, cloud computing enables three possible modes:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS), and
- Software as a Service (SaaS).

9.2.3 Issues and Challenges[edit]

The public mode of cloud computing raises (in principle) issues of Data Privacy as potentially sensitive Personal Data are transferred over networks and processed in third party infrastructure.

10 Complaint

10.1 Contents

10.2 Definition[edit]

A (consumer or customer) **Complaint** is a more or less formal expression of dissatisfaction on a consumer's behalf to a responsible party.

10.3 Example[edit]

According to Article 63(1) of Regulation (EU) 2018/1725, "every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation".

10.4 See Also[edit]

- Legal Risk

10.5 References[edit]

- EDPS Glossary

11 Confidentiality

11.1 Definition[edit]

Confidentiality. Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. In a general sense refers to the duty not to share information with persons who are not qualified to receive that information (see Article 5(f) of Regulation (EU) 2016/679 and Article 4(f) of Regulation (EU) 2018/1725).

In a more specific sense, it refers to the confidentiality of communications provided for in Article 5 of the E-privacy Directive 2009/136/EC and in Article 36 of Regulation (EU) 2018/1725.

11.2 References[edit]

- EDPS Glossary
- Adapted from ISO/IEC 27000:2018

12 Consent

12.1 Definition[edit]

In Data Protection context and terminology, **Consent** refers to any freely given, specific and informed indication of the wishes of a Data Subject, by which he/she agrees to Personal Data relating to him/her being processed (see Article 4 sub 11 of Regulation (EU) 2016/679 and Article 3 sub 15 of Regulation (EU) 2018/1725).

Consent is an important element in Data Protection legislation, as it is one of the conditions that can legitimise processing of personal data. If it is relied upon, the data subject must unambiguously have given his/ her consent to a specific processing operation, of which he/she shall have been properly informed.

The obtained consent can only be used for the specific processing operation for which it was collected, and may in principle be withdrawn without retroactive effect.

12.2 References[edit]

- EDPS Glossary

13 Cookies

13.1 Definition[edit]

Cookies are short text files stored on the user?s device by a web site.

Cookies are normally used to provide a more personalised experience and to remember user profile without the need of a specific login. Also it can be placed by third parties (such as an advertising network) in end users´ devices and maybe be used to track users when surfing across different websites associated to that third party.

13.2 References[edit]

- EDPS Glossary

14 Customer Information

14.1 Definition[edit]

Customer Information means any of the following:

- account contact information
- account number
- billing history
- payment history
- domain specific information that depends on the product or service being provided

15 Data Breach

15.1 Definition[edit]

Data Breach. Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.

15.2 See Also[edit]

- Security Breach

15.3 Reference[edit]

- Adapted from ISO/IEC 27040:2015

16 Data Breaches List

This is a frozen copy (January 2019) of the List of data breaches. It is included here with modifications to enable the automated processing of the data.

Entity	Year	Records	Organization type	Method	Sources
object	datetime64	int64	category	category	object
21st Century Oncology	2016	2,200,000	healthcare	hacked	[1][2]
Accendo Insurance Co.	2011	175,350	healthcare	poor security	[3][4]
Bedford/St. Martin's	2012-2014	unknown	retail	unknown	[5]
Australian Immigration Department	2015	G20 world leaders	government	accidentally published	[6]
Barnes & Noble	2012	63 stores	retail	hacked	[7][8]
Adobe Systems	2013	152,000,000	tech	hacked	[9][10]
Advocate Medical Group	2013	4,000,000	healthcare	lost / stolen media	[11][12]
AerServ (subsidiary of InMobi)	2018	75,000	advertising	hacked	[13]
Affinity Health Plan, Inc.	2009	344,579	healthcare	lost / stolen media	[14]
Ameritrade	2005	200,000	financial	lost / stolen media	[15]
Ancestry.com	2015	300,000	web	poor security	[16]
Ankle & Foot Center of Tampa Bay, Inc.	2010	156,000	healthcare	hacked	[17]
Anthem Inc.	2015	80,000,000	healthcare	hacked	[18][19]
AOL	2004	92,000,000	web	inside job, hacked	[20][21]
AOL	2006	20,000,000	web	accidentally published	[22]
AOL	2014	2,400,000	web	hacked	[23]
Apple, Inc./BlueToad	2012	12,367,232	tech, retail	accidentally published	[24]
Apple	2013	275,000	tech	hacked	[25]
Apple Health Medicaid	2016	91,000	healthcare	poor security	[26]
Ashley Madison	2015	32,000,000	web	hacked	[27]
AT&T	2008	113,000	telecoms	lost / stolen computer	[28]
AT&T	2010	114,000	telecoms	hacked	[29]
Auction.co.kr	2008	18,000,000	web	hacked	[30]
Automatic Data Processing	2005	125,000	financial	poor security	[31]
AvMed, Inc.	2009	1,220,000	healthcare	lost / stolen computer	[32]
Bailey's Inc.	2015	250,000	retail	hacked	[33]
The Bank of New York Mellon	2008	12,500,000	financial	lost / stolen media	[34]
Betfair	2010	2,300,000	web	hacked	[28]
Bethesda Game Studios	2011	200,000	gaming	hacked	[35]
Bethesda Game Studios	2018		gaming	accidentally published	[36]
BlankMediaGames	2018	7,633,234	gaming	hacked	[37][38]
Blizzard Entertainment	2012	14,000,000	gaming	hacked	[39][40]
BlueCross BlueShield of Tennessee	2009	1,023,209	healthcare	lost / stolen media	[41]
BMO and Simplii	2018	90,000	banking	poor security	[42]
British Airways	2018	380,000	transport	hacked	[43][44]
British Airways	2015	tens of thousands	retail	hacked	[45]

Entity	Year	Records	Organization type	Method	Sources
California Department of Child Support Services	2012	800,000	government	lost / stolen media	[28][46]
CardSystems Solutions Inc. (MasterCard, Visa, Discover Financial Services and American Express)	2005	40,000,000	financial	hacked	[47][48]
Cathay Pacific Airways	2018	9,400,000	transport	hacked	[49]
CareFirst BlueCross Blue Shield - Maryland	2015	1,100,000	healthcare	hacked	[50]
Central Coast Credit Union	2016	60,000	financial	hacked	[51]
Central Hudson Gas & Electric	2013	110,000	energy	hacked	[52]
CheckFree Corporation	2009	5,000,000	financial	hacked	[53]
China Software Developer Network	2011	6,000,000	web	hacked	[54]
Chinese gaming websites (three: Duowan, 7K7K, 178.com)	2011	10,000,000	web	hacked	[55]
Citigroup	2005	3,900,000	financial	lost / stolen media	[56]
Citigroup	2011	360,083	financial	hacked	[57]
Citigroup	2013	150,000	financial	poor security	[58]
City and Hackney Teaching Primary Care Trust	2007	160,000	healthcare	lost / stolen media	[59]
Colorado government	2010	105,470	healthcare	lost / stolen computer	[60]
Community Health Systems	2014	4,500,000	healthcare	hacked	[61]
Philippines Commission on Elections	2016	55,000,000	government	hacked	
Compass Bank	2007	1,000,000	financial	inside job	[28][62]
Bank of America	2005	1,200,000	financial	lost / stolen media	[63]
Countrywide Financial Corp	2006	2,600,000	financial	inside job	[28]
Countrywide Financial Corp	2011	2,500,000	financial	inside job	[64]
Centers for Medicare & Medicaid Services	2018	75,000	healthcare	hacked	[65]
Cox Communications	2016	40,000	telecoms	hacked	[66]
Crescent Health Inc., Walgreens	2013	100,000	healthcare	lost / stolen computer	[52][67]
CVS	2015	millions	retail	hacked	[68]
Dai Nippon Printing	2007	8,637,405	retail	inside job	[69]
Data Processors International (MasterCard, Visa, Discover Financial Services and American Express)	2008	8,000,000	financial	hacked	[70]
Defense Integrated Data Center (South Korea)	2017	235 GB	military	hacked	[71]
Deloitte	2017		consulting, accounting	poor security	[72]
Democratic National Committee	2016	19,252	political		[73]
US Department of Homeland Security	2016	30,000	government	poor security	[74][75]
Domino's Pizza (France)	2014	600,000	web	hacked	[76]
UK Driving Standards Agency	2007	3,000,000	government	lost / stolen media	[77]
Dropbox	2012	unknown	web	hacked	[78]
Drupal	2013	1,000,000	web	hacked	[79]
DSW Inc.	2005	1,400,000	retail	hacked	[80]
Dun & Bradstreet	2013	1,000,000	tech	hacked	[81][82]
eBay	2014	145,000,000	web	hacked	[83]
Educational Credit Management Corporation	2010	3,300,000	financial	lost / stolen media	[84]
Eisenhower Medical Center	2011	514,330	healthcare	lost / stolen computer	[85]
Embassy Cables	2010	251,000	government	inside job	[86]

Entity	Year	Records	Organization type	Method	Sources
Emergency Healthcare Physicians, Ltd.	2010	180,111	healthcare	lost / stolen media	[85][87]
Emory Healthcare	2012	315,000	healthcare	poor security	[85]
Erie County Medical Center	2017	unknown	healthcare	poor security	[88]
Equifax	2017	143,000,000	financial, credit reporting	poor security	[89][90]
European Central Bank	2014	unknown	financial	hacked	[91][92]
Evernote	2013	50,000,000	web	hacked	[93][94]
Excellus BlueCross BlueShield	2015	10,000,000	healthcare	hacked	[95]
Experian - T-Mobile US	2015	15,000,000	telecoms	hacked	[96][97]
EyeWire	2016	unknown	tech	lost / stolen computer	[98]
Facebook	2018	50,000,000	social network	poor security	[99][100][101][102][103][104]
Facebook	2013	6,000,000	web	accidentally published	[105]
Federal Reserve Bank of Cleveland	2010	400,000	financial	hacked	[28]
Fidelity National Information Services	2007	8,500,000	financial	inside job	[106]
Florida Department of Juvenile Justice	2013	100,000	government	lost / stolen computer	[52]
Friend Finder Networks	2016	412,214,295	web	poor security / hacked	[107][108]
Formspring	2012	420,000	web	accidentally published	[109]
Gamigo	2012	8,000,000	web	hacked	[110]
Gap Inc.	2007	800,000	retail	lost / stolen computer	[111]
Gawker	2010	1,500,000	web	hacked	[112][113]
Global Payments	2012	7,000,000	financial	hacked	[114]
Gmail	2014	5,000,000	web	hacked	[115]
Google Plus	2018	500,000	social network	poor security	[116][117][118]
Greek government	2012	9,000,000	government	hacked	[119]
Grozio Chirurgija	2017	25,000	healthcare	hacked	[120][121][122]
GS Caltex	2008	11,100,000	energy	inside job	[123][124]
Gyft	2016	unknown	web	hacked	[125][126]
Hannaford Brothers Supermarket Chain	2007	4,200,000	retail	hacked	[127]
Health Net	2009	500,000	healthcare	lost / stolen media	[128]
Health Net ? IBM	2011	1,900,000	healthcare	lost / stolen media	[129]
Heartland	2009	130,000,000	financial	hacked	[130][131]
Heathrow Airport	2017	2.5GB	transport	lost / stolen media	[132][133][134]
Hewlett Packard	2006	200,000	tech, retail	lost / stolen media	[135]
Hilton Hotels	2015	unknown	hotel	hacked	[136]
Home Depot	2014	56,000,000	retail	hacked	[137]
Honda Canada	2011	283,000	retail	poor security	[138]
Hyatt Hotels	2015	250 locations	hotel	hacked	[139][140]
Internal Revenue Service	2015	720,000	financial	hacked	[141][142]
Inuvik hospital	2016	6,700	healthcare	inside job	[143]
Iranian banks (three: Saderat, Eghtesad Novin, and Saman)	2012	3,000,000	financial	hacked	[144]
Jefferson County, West Virginia	2008	1,600,000	government		[28][145]

Entity	Year	Records	Organization type	Method	Sources
				accidentally published	
JP Morgan Chase	2010	2,600,000	financial	lost / stolen media	[146]
JP Morgan Chase	2014	76,000,000	financial	hacked	[147]
KDDI	2006	4,000,000	telecoms	hacked	[148]
Kirkwood Community College	2013	125,000	academic	hacked	[52][149]
KM.RU	2016	1,500,000	web	hacked	[150]
Korea Credit Bureau	2014	20,000,000	financial	inside job	[151]
Kroll Background America	2013	1,000,000	tech	hacked	[81][82]
KT Corporation	2012	8,700,000	telecoms	hacked	[152][153]
LexisNexis	2014	1,000,000	tech	hacked	[81][82]
Landry's, Inc.	2015	500 locations	restaurant	hacked	[154][155]
Lincoln Medical & Mental Health Center	2010	130,495	healthcare	lost / stolen media	[85][156]
LinkedIn, eHarmony, Last.fm	2012	8,000,000	web	accidentally published	[157][158]
Living Social	2013	50,000,000	web	hacked	[159][160]
MacRumors.com	2014	860,000	web	hacked	[161]
Mandarin Oriental Hotels	2014	10 locations	hotel	hacked	[162][163]
Marriott International	2018	500,000,000	hotel	hacked	[164][165]
Massachusetts Government	2011	210,000	government	poor security	[28]
Massive American business hack including 7-Eleven and Nasdaq	2012	160,000,000	financial	hacked	[166]
US Medicaid	2012	780,000	government, healthcare	hacked	[28]
Medical Informatics Engineering	2015	3,900,000	healthcare	hacked	[167]
Memorial Healthcare System	2011	102,153	healthcare	lost / stolen media	[168][85]
Michaels	2014	3,000,000	retail	hacked	[169]
Militarysingles.com	2012	163,792	web, military	accidentally published	[170]
Ministry of Education (Chile)	2008	6,000,000	government	accidentally published	[171][172]
Monster.com	2007	1,600,000	web	hacked	[173]
Morgan Stanley Smith Barney	2011	34,000	financial	lost / stolen media	[28]
Mozilla	2014	76,000	web	poor security	[174]
MyHeritage	2018	92,283,889	genealogy	unknown	[175]
NASDAQ	2014	unknown	financial	hacked	[176]
Natural Grocers	2015	93 stores	retail	hacked	[177]
Neiman Marcus	2014	1,100,000	retail	hacked	[178][179]
Nemours Foundation	2011	1,055,489	healthcare	lost / stolen media	[85][180]
Network Solutions	2009	573,000	tech	hacked	[181][182]
New York City Health & Hospitals Corp.	2010	1,700,000	healthcare	lost / stolen media	[85]
New York State Electric & Gas	2012	1,800,000	energy	inside job	[28]
New York Taxis	2014	52,000	transport	poor security	[183]
Nexon Korea Corp	2011	13,200,000	web	hacked	[184]
NHS	2011	8,300,000	healthcare	lost / stolen media	[185]
Nintendo	2013	240,000	gaming	hacked	[186]
Nival Networks	2016	1,500,000	gaming	hacked	[187]

Entity	Year	Records	Organization type	Method	Sources
Norwegian Tax Administration	2008	3,950,000	government	accidentally published	[188]
Ofcom	2016	unknown	telecom	inside job	[189]
US Office of Personnel Management	2015	21,500,000	government	hacked	[190][191]
Office of the Texas Attorney General	2012	6,500,000	government	accidentally published	[192]
Ohio State University	2010	760,000	academic	hacked	[28]
Orbitz	2018	880,000	web	hacked	[193]
Oregon Department of Transportation	2011	unknown	government	poor security	[28]
OVH	2013	undisclosed	web	hacked	[194]
Patreon	2015	2.3 million	web	hacked	[195]
Popsugar	2018	123,857	fashion	hacked	[196]
Premera	2015	11,000,000	healthcare	hacked	[197]
Puerto Rico Department of Health	2010	515,000	healthcare	hacked	[85]
Quora	2018	100,000,000	Question & Answer	hacked	[198]
Rambler.ru	2012	98,167,935	web	hacked	[199][200]
RBS Worldpay	2008	1,500,000	financial	hacked	[201]
Reddit	2018	unknown	web	hacked	[202][203]
Restaurant Depot	2011	200,000	retail	hacked	[28]
RockYou!	2009	32,000,000	web, gaming	hacked	[204]
Rosen Hotels	2016	unknown	hotel	hacked	[205]
San Francisco Public Utilities Commission	2011	180,000	government	hacked	[206]
Scottrade	2015	4,600,000	financial	hacked	[207]
Scribd	2013	500,000	web	hacked	[208][209]
Seacoast Radiology, PA	2010	231,400	healthcare	hacked	[85][210]
Sega	2011	1,290,755	gaming	hacked	[211]
Service Personnel and Veterans Agency (UK)	2008	50,500	government	lost / stolen media	[212]
SingHealth	2018	1,500,000	government, database	hacked	[213]
Slack	2015	500,000	tech	poor security	[214]
SnapChat	2013	4,700,000	web, tech	hacked	[215]
Sony Online Entertainment	2011	24,600,000	gaming	hacked	[216][217]
Sony Pictures	2011	1,000,000	web	hacked	[218]
Sony Pictures	2014	100 terabytes	media	hacked	[219]
Sony PlayStation Network	2011	77,000,000	gaming	hacked	[220]
South Africa police	2013	16,000	government	hacked	[221]
South Carolina Government	2012	6,400,000	healthcare	inside job	[85][222]
South Shore Hospital, Massachusetts	2010	800,000	healthcare	lost / stolen media	[28]
Southern California Medical-Legal Consultants	2011	300,000	healthcare	hacked	[28]
Spartanburg Regional Healthcare System	2011	400,000	healthcare	lost / stolen computer	[85][223]
Stanford University	2008	72,000	academic	lost / stolen computer	[28][224]
Starbucks	2008	97,000	retail	lost / stolen computer	[28]
Starwood Hotels including Westin Hotels and Sheraton Hotels	2015	54 locations	hotel	hacked	[225][226]
State of Texas	2011	3,500,000	government		[227]

Entity	Year	Records	Organization type	Method	Sources
				accidentally published	
Steam	2011	35,000,000	web	hacked	[228]
Stratfor	2011	935,000	military	accidentally published	[229]
Supervalu	2014	200 stores	retail	hacked	[230]
Sutter Medical Center	2011	4,243,434	healthcare	lost / stolen computer	[85][231]
Syrian government (Syria Files)	2012	2,434,899	government	hacked	[232][233]
Taobao	2016	20,000,000	retail	hacked	[234]
Taringa!	2017	28,722,877	web	hacked	[235]
Target Corporation	2014	70,000,000	retail	hacked	[236][237]
TaxSlayer.com	2016	unknown	web	hacked	[238]
TD Ameritrade	2007	6,300,000	financial	hacked	[239]
TD Bank	2012	260,000	financial	hacked	[240][241]
TerraCom & YourTel	2013	170,000	telecoms	accidentally published	[242][243]
Texas Lottery	2007	89,000	government	inside job	[28]
Ticketfly (subsidiary of Eventbrite)	2018	26,151,608	ticket distribution	hacked	[244]
Tianya Club	2011	28,000,000	web	hacked	[245]
TK / TJ Maxx	2007	94,000,000	retail	hacked	[246][247]
T-Mobile, Deutsche Telecom	2006	17,000,000	telecoms	lost / stolen media	[248][249]
Tricare	2011	4,901,432	military, healthcare	lost / stolen computer	[28]
Triple-S Salud, Inc.	2010	398,000	healthcare	lost / stolen media	[85]
Trump Hotels	2014	8 locations	hotel	hacked	[250][251]
Tumblr	2013	65,469,298	web	hacked	[252]
Twitch.tv	2015	unknown	tech	hacked	[253]
Twitter	2013	250,000	web	hacked	[254]
Typeform	2018	unknown	tech	poor security	[49]
Uber	2014	50,000	tech	poor security	[255]
Uber	2017	57,000,000	transport	hacked	[256]
Ubisoft	2013	unknown	gaming	hacked	[257]
Ubuntu	2013	2,000,000	tech	hacked	[258]
UCLA Medical Center, Santa Monica	2015	4,500,000	healthcare	hacked	[259]
UK Home Office	2008	84,000	government	lost / stolen media	[260]
UK Ministry of Defence	2008	1,700,000	government	lost / stolen media	[261]
UK Revenue & Customs	2007	25,000,000	government	lost / stolen media	[262]
Under Armour	2018	150,000,000	Consumer Goods	hacked	[263]
University of California, Berkeley	2009	160,000	academic	hacked	[264]
University of California, Berkeley	2016	80,000	academic	hacked	[265]
University of Maryland, College Park	2014	300,000	academic	hacked	[266]
University of Central Florida	2016	63,000	academic	hacked	[267]
University of Miami	2008	2,100,000	academic	lost / stolen computer	[28]
University of Utah Hospital & Clinics	2008	2,200,000	academic	lost / stolen media	[28]
University of Wisconsin?Milwaukee	2011	73,000	academic	hacked	[28]

Entity	Year	Records	Organization type	Method	Sources
UPS	2014	51 locations	retail	hacked	[268]
U.S. Army	2011	50,000	military	accidentally published	[28]
U.S. Army (classified Iraq War documents)	2010	392,000	government	inside job	[269]
U.S. Department of Defense	2009	72,000	military	lost / stolen media	[28]
U.S. Department of Veteran Affairs	2006	26,500,000	government, military	lost / stolen computer	[270]
U.S. law enforcement (70 different agencies)	2011	123,461	government	accidentally published	[271]
National Archives and Records Administration (U.S. military veterans' records)	2009	76,000,000	military	lost / stolen media	[272]
U.S. government (United States diplomatic cables leak)	2010	260,000	military	inside job	[273]
National Guard of the United States	2009	131,000	military	lost / stolen computer	[28]
Verizon Communications	2016	1,500,000	telecoms	hacked	[274]
Virginia Department of Health	2009	8,257,378	government, healthcare	hacked	[28]
Virginia Prescription Monitoring Program	2009	531,400	healthcare	hacked	[28]
Vodafone	2013	2,000,000	telecoms	inside job	[275]
VTech	2015	5,000,000	retail	hacked	[276]
Walmart	2015	millions	retail	hacked	[68]
Washington Post	2011	1,270,000	media	hacked	[277]
Washington State court system	2013	160,000	government	hacked	[278][279]
Weebly	2016	43,430,316	web	hacked	[280][281][282]
Wendy's	2015	unknown	restaurant	hacked	[283][284]
Wordpress	2018			hacked	[285]
Writerspace.com	2011	62,000	web	hacked	[286]
Xat.com	2015	6,054,459	web	social engineering	[287]
Yahoo	2013	3,000,000,000	web	hacked	[288][289]
Yahoo	2014	500,000,000	web	hacked	[290][291][292][293][294]
Yahoo Japan	2013	22,000,000	tech, web	hacked	[295]
Yahoo! Voices	2012	450,000	web	hacked	[296][297]
Yale University	2010	43,000	academic	accidentally published	[28]
Zappos	2012	24,000,000	web	hacked	[298]

1. ? "21st Century Oncology notifies 2.2 million of hacking, data breach", *CBS12*, March 14, 2016
2. ? "Oh No, Not Again...Chalk Up Yet Another Health Data Breach", *National Law Review*, March 14, 2016
3. ? Template:Cite web
4. ? Template:Cite web
5. ? Template:Cite web
6. ? Template:Cite web
7. ? Template:Cite news
8. ? Template:Cite web
9. ? Template:Cite web
10. ? Template:Cite web
11. ? Template:Cite web
12. ? Template:Cite web
13. ? Template:Cite web
14. ? Template:Cite web

15. ? Template:Cite web
16. ? Template:Cite news
17. ? Template:Cite web
18. ? Template:Cite web
19. ? Template:Cite web
20. ? Template:Cite web
21. ? Template:Cite web
22. ? Template:Cite web
23. ? Template:Cite web
24. ? Template:Cite web
25. ? Template:Cite web
26. ? "91,000 state Medicaid clients warned of data breach", *The Seattle Times*, Feb. 9, 2016
27. ? Template:Cite web
28. ^ Template:Cite web
29. ? Template:Cite web
30. ? Template:Cite web
31. ? Template:Cite web
32. ? Template:Cite web
33. ? "Attacker compromises information of 250K in Bailey's data breach", *SC Magazine*, March 16, 2016
34. ? Template:Cite web
35. ? Template:Cite web
36. ? Template:Cite web
37. ? Template:Cite web
38. ? Template:Cite web
39. ? Template:Cite web
40. ? Template:Cite web
41. ? Template:Cite web
42. ? Template:Cite news
43. ? Template:Cite web
44. ? Template:Cite web
45. ? Template:Cite web
46. ? [1]Template:Dead link
47. ? Template:Cite web
48. ? Template:Cite news
49. ^ Template:Cite web
50. ? Template:Cite web
51. ? "Breached Credit Union Comes Out of its Shell", Krebs on Security, Feb. 25, 2016
52. ^ Template:Cite web
53. ? Template:Cite web
54. ? Template:Cite web
55. ? Template:Cite web
56. ? Template:Cite news
57. ? Template:Cite web
58. ? Template:Cite web
59. ? Template:Cite web
60. ? Template:Cite web
61. ? Template:Cite web
62. ? Template:Cite web
63. ? Template:Cite news
64. ? Template:Cite web
65. ? Template:Cite news
66. ? "Cox Communications Investigates Data Breach Affecting 40K Employees", *Info Security Magazine*, March 7, 2016
67. ? Template:Cite web
68. ^ Template:Cite news
69. ? Template:Cite web
70. ? Template:Cite web
71. ? Template:Cite web
72. ? Template:Cite web
73. ? Template:Cite news
74. ? "Breach Exposes Data From Thousands of DHS Employees", *PC Magazine*, Feb. 8, 2016

75. ? "Hackers Get Employee Records at Justice and Homeland Security Depts.", *New York Times*, Feb. 8, 2016
76. ? Template:Cite web
77. ? Template:Cite news
78. ? Template:Cite web
79. ? Template:Cite web
80. ? Template:Cite news
81. ^ Template:Cite web
82. ^ Template:Cite web
83. ? Template:Cite web
84. ? Template:Cite web
85. ^ Template:Cite web
86. ? Template:Cite web
87. ? Template:Cite web
88. ? Template:Cite web
89. ? "Equifax data breach may affect nearly half the US population", Sept 7, 2017
90. ? "Equifax had patch 2 months before hack and didn't install it, security group says", Sept 14, 2017
91. ? Template:Cite web
92. ? Template:Cite web
93. ? Template:Cite web
94. ? Template:Cite web
95. ? Template:Cite web
96. ? "Massive Data Breach At Experian Exposes Personal Data For 15 Million T-Mobile Customers", *Huffington Post*, Oct. 2, 2015
97. ? "Experian data breach affects 15 million people including T-Mobile customers", *Fortune*, Oct. 1, 2015
98. ? "Security: Data Breach & Old Password Expiration", *Eyewire*, Feb. 23, 2016
99. ? Template:Cite web
100. ? Template:Cite web
101. ? Template:Cite web
102. ? Template:Cite web
103. ? Template:Cite news
104. ? Template:Cite web
105. ? Template:Cite web
106. ? Template:Cite web
107. ? Template:Cite web
108. ? Template:Cite web
109. ? Template:Cite web
110. ? Template:Cite web
111. ? Template:Cite web
112. ? Template:Cite web
113. ? Template:Cite web
114. ? Template:Cite web
115. ? Template:Cite web
116. ? Template:Cite web
117. ? Template:Cite web
118. ? Template:Cite web
119. ? Template:Cite web
120. ? Template:Cite news
121. ? Template:Cite news
122. ? Template:Cite web
123. ? Template:Cite web
124. ? Template:Cite web
125. ? "Gyft Notifies Users of Data Breach", *Low Cards*, Feb. 8, 2016
126. ? "Gyft Notifies Affected Users of Security Incident", *BusinessWire*, Feb. 5, 2016
127. ? Template:Cite web
128. ? Template:Cite web
129. ? Template:Cite web
130. ? Template:Cite web
131. ? Template:Cite web
132. ? Template:Cite news
133. ? Template:Cite web
134. ? Template:Cite web

135. ? Template:Cite web
136. ? Template:Cite web
137. ? Template:Cite web
138. ? Template:Cite web
139. ? Template:Cite web
140. ? Template:Cite web
141. ? Template:Cite web
142. ? "IRS taxpayer data theft seven times larger than originally thought", *CNN*, Feb. 26, 2016
143. ? Template:Cite news
144. ? Template:Cite web
145. ? Template:Cite web
146. ? Template:Cite web
147. ? Template:Cite web
148. ? Template:Cite web
149. ? Template:Cite web
150. ? Template:Cite web
151. ? Template:Cite web
152. ? Template:Cite web
153. ? Template:Cite web
154. ? Template:Cite web
155. ? Template:Cite web
156. ? Template:Cite web
157. ? Template:Cite web
158. ? Template:Cite web
159. ? Template:Cite web
160. ? Template:Cite web
161. ? Template:Cite web
162. ? Template:Cite web
163. ? Template:Cite web
164. ? "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing", *New York Times*, Dec. 11, 2018
165. ? Template:Cite web
166. ? Template:Cite web
167. ? Template:Cite web
168. ? Template:Cite web
169. ? Template:Cite web
170. ? Template:Cite web
171. ? Template:Cite news
172. ? Template:Cite web
173. ? Template:Cite news
174. ? Template:Cite web
175. ? Template:Cite web
176. ? Template:Cite web
177. ? Template:Cite web
178. ? Template:Cite news
179. ? Template:Cite web
180. ? Template:Cite web
181. ? Template:Cite web
182. ? Template:Cite web
183. ? Template:Cite web
184. ? Template:Cite web
185. ? Template:Cite web
186. ? Template:Cite web
187. ? Template:Cite news
188. ? Template:Cite web
189. ? "Ofcom tackles mass data breach of TV company information", *The Guardian*, March 10, 2016
190. ? Template:Cite news
191. ? Template:Cite web
192. ? Template:Cite web
193. ? Template:Cite web
194. ? Template:Cite web

195. ? Template:Cite web
196. ? Template:Cite web
197. ? Template:Cite web
198. ? Template:Cite news
199. ? Template:Cite web
200. ? Template:Cite web
201. ? Template:Cite web
202. ? Template:Cite news
203. ? Template:Cite news
204. ? Template:Cite web
205. ? "Rosen Hotels warns customers of 18-month data breach", *Orlando Sentinel*, March 8, 2016
206. ? Template:Cite web
207. ? Template:Cite web
208. ? Template:Cite web
209. ? [2]Template:Dead link
210. ? Template:Cite web
211. ? Template:Cite web
212. ? Template:Cite news
213. ? Template:Cite news
214. ? Template:Cite web
215. ? Template:Cite web
216. ? Template:Cite web
217. ? Template:Cite web
218. ? Template:Cite web
219. ? Template:Cite web
220. ? Template:Cite web
221. ? Template:Cite web
222. ? Template:Cite web
223. ? Template:Cite web
224. ? Template:Cite web
225. ? Template:Cite web
226. ? Template:Cite web
227. ? Template:Cite web
228. ? Template:Cite web
229. ? Template:Cite web
230. ? Template:Cite web
231. ? Template:Cite web
232. ? Template:Cite news
233. ? Template:Cite news
234. ? Template:Cite web
235. ? Template:Cite news
236. ? Template:Cite web
237. ? Template:Cite web
238. ? Template:Cite web
239. ? Template:Cite web
240. ? Template:Cite web
241. ? Template:Cite web
242. ? Template:Cite web
243. ? Template:Cite web
244. ? Template:Cite web
245. ? Template:Cite web
246. ? Template:Cite web
247. ? Template:Cite web
248. ? http://www.datalossdb.org
249. ? http://www.informationweek.com/security/attacks/t-mobile-lost-17-million-subscribers-per/
250. ? Template:Cite web
251. ? Template:Cite web
252. ? Template:Cite web
253. ? Template:Cite web
254. ? Template:Cite web

255. ? Template:Cite web
256. ? Template:Cite news
257. ? Template:Cite web
258. ? Template:Cite web
259. ? Template:Cite web
260. ? Template:Cite news
261. ? Template:Cite news
262. ? Template:Cite news
263. ? Template:Cite web
264. ? Template:Cite web
265. ? "Data breach affects 80,000 UC Berkeley faculty, students and alumni", Fox News, Feb. 28, 2016
266. ? "University of Maryland computer security breach exposes 300,000 records", Washington Post, Feb. 19, 2014
267. ? Template:Cite web
268. ? Template:Cite news
269. ? Template:Cite web
270. ? Template:Cite web
271. ? Template:Cite web
272. ? Template:Cite web
273. ? Template:Cite web
274. ? "Verizon's Data Breach Fighter Gets Hit With, Well, a Data Breach", *Fortune* magazine, March 24, 2016
275. ? Template:Cite web
276. ? Template:Cite news
277. ? Template:Cite web
278. ? Template:Cite web
279. ? Template:Cite web
280. ? Template:Cite web
281. ? Template:Cite web
282. ? Template:Cite web
283. ? Template:Cite web
284. ? Template:Cite news
285. ? Template:Cite web
286. ? Template:Cite web
287. ? Template:Cite web
288. ? Template:Cite web
289. ? Template:Cite web
290. ? Template:Cite web
291. ? Template:Cite web
292. ? Template:Cite web
293. ? Template:Cite news
294. ? Template:Cite web
295. ? Template:Cite web
296. ? Template:Cite web
297. ? "Yahoo Voices Breach Exposes 453,000 Passwords", *PC Magazine*, July 12, 2012
298. ? Template:Cite web

17 Data Controller

17.1 Definition[edit]

Under Regulation (EU) 2018/1725, as well as under the GDPR, the **Data Controller** is the party that, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

The actual processing may be delegated to another party, called the Data Processor. The controller is responsible for

- the lawfulness of the processing
- for the protection of the data, and
- respecting the rights of the Data Subject.

The controller is also the entity that receives requests from data subjects to exercise their rights.

17.2 Notes[edit]

- In ISO/IEC the term 'PII Controller' is used.

17.3 References[edit]

- EDPS Glossary
- Data Privacy Vocabulary (DPV)

18 Data Minimization

18.1 Definition[edit]

The principle of **Data Minimisation** 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 minimisation principle is expressed in Article 5(1)(c) of the GDPR and Article 4(1)(c) of Regulation (EU) 2018/1725, which provide that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

18.2 References[edit]

- EDPS Glossary

19 Data Mining

19.1 Definition[edit]

Data Mining is the process of analysing data from different perspectives and summarising it into useful new information.

Data mining software is one of a number of tools for interrogating data. It allows users to analyse data from many different dimensions or angles, categorise it, and summarise the relationships identified.

Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery. Obviously, for data mining to be effective it is necessary to analyse large amounts of previously collected data.

19.2 References[edit]

- EDPS Glossary

20 Data Privacy

20.1 Contents

20.2 Definition[edit]

Data Privacy (also *Information Privacy*) denotes the perimeter of information collection and dissemination that is acceptable in a given legal and political environemnt. Related concepts with nuanced differerences in meaning are Information Privacy and Data Protection.

- The concept of data privacy is in-principle tecnhology agnostic. Digital technology has both complicated and accelerated the recognition of data privacy as an important aspect of societal organization.

20.2.1 Data Types[edit]

- Various types of [[Personal Data] often come under privacy concerns
  - Media Consumption patterns (newspapers, radio, television)
  - Online Data (web browsing, email, messaging, search, comments, geolocation)
  - Educational Data
  - Medical Data
  - Commercial Data (purchases, sales, organizational structure)
  - Financial (transactions)

20.2.2 Privacy Laws[edit]

- General Personal Data Protection Law (Brazil)
- Data Protection Directive (European Union)
- California Consumer Privacy Act|California Consumer Privacy Act (CCPA) (California)
- Privacy Act (Canada)
- Privacy Act 1988 (Australia)
- Personal Data Protection Bill 2019|Personal Data Protection Bill 2019 (India)
- China Internet Security Law|China Cyber Security Law (CCSL) (China)
- Data Protection Act, 2012 (Ghana)
- Personal Data Protection Act 2012 (Singapore)
- Republic Act No. 10173: Data Privacy Act of 2012 (Philippines)
- Data protection (privacy) laws in Russia
- Data Protection Act 2018 (United Kingdom)
- Personal Data Protection Law (PDPL) (Bahrain)

20.2.3 Privacy Authorities and Organizations[edit]

- National data protection authority|National data protection authorities in the European Union and the European Free Trade Association
- Office of the Australian Information Commissioner (Australia)
- Privacy Commissioner (New Zealand)
- Commission nationale de l'informatique et des libertés, France
- Federal Commissioner for Data Protection and Freedom of Information (Germany)
- Office of the Privacy Commissioner for Personal Data (Hong Kong)
- Data Protection Commissioner (Republic of Ireland)
- Office of the Data Protection Supervisor (Isle of Man)
- National Privacy Commission (Philippines)

- Personal Data Protection Act 2012 (Singapore)
- Personal Data Protection Office (Turkey) (KVKK, Turkey)
- Federal Data Protection and Information Commissioner (Switzerland)
- Information Commissioner's Office]] (ICO, United Kingdom)
- Confederation of European Data Protection Organisations
- Data Protection Day (28 January)
- International Association of Privacy Professionals (headquartered in USA)
- Privacy International (headquartered in UK)

20.3 Mitigation Mechanisms[edit]

- Regulation
- Education
- Encryption
- Decentralization
- Data Minimization
- Privacy by Design
- Privacy enhancing technologies

20.4 See Also[edit]

- Data Privacy Vocabulary
- Authentication
- Data Retention
- Data Security
- Differential Privacy
- Data Sovereignty
- Data Localization

20.5 References[edit]

- wikipedia:Information privacy

21 Data Privacy Rights

21.1 Definition[edit]

Data Privacy Rights are the 'Individual Rights' or 'Right of a Person' that are recognized by a jurisdiction and its specific Data Protection regime.

- Right of Access
- Right of Information
- Right to Object
- Right to Restriction of Processing

21.2 References[edit]

- EDPS Glossary
- Data Privacy Vocabulary (DPV)

22 Data Privacy Risk

22.1 Definition[edit]

Data Privacy Risk is the Risk that can be associated with one or more different Data Privacy concepts such as purpose, processing, personal data, technical or organisational measures.

23 Data Privacy Vocabulary

23.1 Contents

23.2 Definition[edit]

The **Data Privacy Vocabulary** is a a collection of terms used in Data Privacy context. It integrates (subsets of) terminology from a number of references.

23.3 Structure[edit]

Conceptually the structure of the vocabulary aims to express concretely the real or legal persons involved, the purpose of the data processing and the type of data involved, the legal basis (including consent) that applies and any technical or organization measures that are being taken.

- Entities
- Personal Data Taxonomy
- Data Processing Purposes
- Processing of Personal Data
- Consent
- Legal Basis
- Technical and Organization Measures

23.4 Data Privacy Vocabularies and Controls Community Group[edit]

The Data Privacy Vocabulary (DPV) provides terms (classes and properties) to describe and represent information related to processing of personal data based on established requirements such as for the EU General Data Protection Regulation (GDPR).

The DPV is structured as a top-down hierarchical vocabulary with the core or base concepts of personal data categories, purposes of processing and types of processing, data controller(s) associated, recipients of personal data, legal bases or justifications used, technical and organisational measures and restrictions (e.g. storage locations and storage durations), applicable rights, and the risks involved.

Use case examples of the DPV include:

- annotating privacy policies
- documenting information for specific laws such as GDPR
- producing transparent, machine-readable processing logs (for instance by mapping the DPV to existing database schemas and thereby generating/aggregating machine-readable transparency records directly out of their logging).

NB: DPV It is not a W3C Standard nor is it on the W3C Standards Track

23.5 References[edit]

- Data Privacy Vocabulary (DPV)
- EDPS Glossary

24 Data Processing

24.1 Contents

24.2 Definition[edit]

Data Processing denotes the set of automated or manual operations that an organization may perform on its material digital data flows. It comprises of activities that form part of a Data Processing Taxonomy such as:

- Data Sourcing (also Data Collection)
- Data Storage (persistence of data in databases)
- Data Validation
- Data Migration
- Data Use

24.3 ECB TRIM Requirements[edit]

Data Processing in regulated financial institutions is subject to specific requirements[1] in particular with regard to manual interventions and data transfers:

- *Ensuring that all data transformations are traceable and controlled.* General guidelines and rules should be clearly formalised with regard to manual interventions within the data processing;
- *Ensuring timeliness and Accountability.* All data transfers should be formally agreed upon (for example by means of service-level agreements) by data providers and data users (for both outsourced and in-house processes).

24.4 See Also[edit]

- Processing of Personal Data

24.5 References[edit]

1. ? ECB guide to internal models - Credit Risk, Sep 2018

25 Data Processing Purpose

25.1 Definition[edit]

Data Processing Purpose is the purpose of processing Personal Data

25.2 References[edit]

- Data Privacy Vocabulary (DPV)

26 Data Processing Record

26.1 Definition[edit]

In order to demonstrate compliance with Regulation (EU) No 2018/1725, controllers should maintain a **Data Processing Record** of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility.

Unless it is not appropriate taking into account the size of the Union institution or body, Union institutions and bodies shall keep their records of processing activities in a central register. They shall make the register publicly accessible (Article 31 Regulation (EU) No 2018/1725).

26.2 References[edit]

- EDPS Glossary

27 Data Processing Taxonomy

27.1 Definition[edit]

Data Processing Taxonomy is a scheme for classifying Data Processing activities according to their various characteristics. Such schemes are particularly important in a regulatory contexts.

Data Acquire	to come into possession or control of the data
Data Adapt	to modify the data, often rewritten into a new form for a new use
Data Align	to adjust the data to be in relation to another data
Data Alter	to change the data without changing it into something else
Data Analyse	to study or examine the data in detail
Data Anonymise	to irreversibly alter personal data in such a way that an unique data subject can no longer be identified directly or indirectly or in combination with other data
Data Automated Decision Making	Processing that involves automated decision making
Data Collect	to gather data from someone
Data Combine	to join or merge data
Data Consult	to consult or query data
Data Copy	to produce an exact reprodution of the data
Data Data Source	Source is direct point of data collection; 'origin' would indicate the original/others points of where the data originates from
Data Derive	to create new derivative data from the original data
Data Destruct	to process data in a way it no longer exists or cannot be repaired
Data Disclose	to make data known
Data Disclose by Transmission	to disclose data by means of transmission
Data Disseminate	to spread data throughout
Data Erase	to delete data
Data Evaluation and Scoring	Processing that involves evaluation and scoring of individuals
Data Innovative Use of New Technologies	Processing that involves use of innovative and new technologies
Data Large Scale Processing	Processing that takes place at large scales
Data Make Available	to transform or publish data to be used
Data Matching and Combining	Processing that involves matching and combining of personal data
Data Move	to move data from one location to another including deleting the original copy
Data Obtain	to solicit or gather data from someone
Data Organise	to organize data for arranging or classifying
Data Processing	
Data Profiling	to create a profile that describes or represents a person
Data Pseudo-Anonymise	to replace personal identifiable information by artificial identifiers
Data Record	to make a record (especially media)
Data Remove	to destruct or erase data
Data Restrict	to apply a restriction on the processsing of specific records
Data Retrieve	to retrieve data, often in an automated manner
Data Share	to give data (or a portion of it) to others
Data Store	to keep data for future use
Data Structure	to arrange data according to a structure
Data Systematic Monitoring	Processing that involves systematic monitoring of individuals
Data Transfer	to move data from one place to another

Data Transform	to change the form or nature of data
Data Transmit	to send out data
Data Use	to use data

27.2 See Also[edit]

- Personal Data Taxonomy

27.3 References[edit]

- EDPS Glossary
- Data Privacy Vocabulary (DPV)

28 Data Processor

28.1 Contents

28.2 Definition[edit]

According to Article 3 (12) of Regulation (EU) 2018/1725, a **Data Processor** shall mean a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

The essential element is therefore that the processor only acts "on behalf of the controller" and thus only subject to his instructions.

28.3 Example[edit]

For example, a security company monitoring the entries into an institution's building is not processing personal data of the persons entering a building for its own purpose, but on behalf of the institution concerned.

In some cases, the processor may choose not to process the data himself, but may have recourse to a subcontractor who processes the data on his behalf. In practice, this will depend upon the processor agreement entered into with the controller.

28.4 See Also[edit]

- Data Processor Agreement

28.5 References[edit]

- EDPS Glossary

29 Data Processor Agreement

29.1 Definition[edit]

Transfers of Personal Data from a Data Controller to a Data Processor must be secured by a **Data Processor Agreement**. It must meet certain minimum requirements, as set forth by Article 28 of the General Data Protection Regulation and Article 29 of Regulation (EU) 2018/1725.

The contract must stipulate that the data processor shall act only on instructions from the data controller. The data processor must provide sufficient guarantees in respect of the technical security measures and organisational measure governing the processing to be carried out, and must ensure compliance with such measures.

29.2 References[edit]

- EDPS Glossary

30 Data Protection

30.1 Definition[edit]

Data Protection. Statutory requirements to manage Personal Data in a manner that does not threaten or disadvantage the person to whom it refers.

30.2 See Also[edit]

- Data Privacy

31 Data Protection Authority

31.1 Definition[edit]

A **Data Protection Authority** (DPA) is an independent Authority (body) which is in charge of overseeing legal compliance regarding privacy and data protection laws, more specifically:

- 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;
- hearing complaints lodged by citizens with regard to the protection of their Data Protection rights.

According to Article 51 of the GDPR, 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.), corrective powers (power to order the erasure of data, to impose a fine or a ban on processing, etc.), and authorisation or advisory powers (issuance of opinions, power to accredit certification bodies, etc.).

The EDPS is established as an independent data protection authority at EU level by Article 52 of Regulation (EU) 2018/1725.

National data protection authorities have been established in all European countries, as well as in many other countries worldwide.

31.2 References[edit]

- EDPS Glossary
- List of DPA]

32 Data Protection Coordinator

32.1 Definition[edit]

In addition to the Data Protection Officer foreseen by Regulation (EU) 2018/1725, some EU-institutions have appointed a **Data Protection Coordinator** in order to coordinate all data protection aspects in the relevant DG, Departments or Units.

32.2 References[edit]

- EDPS Glossary

33 Data Protection Day

33.1 Definition[edit]

The Member States of the Council of Europe and the European institutions celebrate **Data Protection Day** each year on 28 January. This date marks the anniversary of the Council of Europe's Convention 108, the first legally binding international instrument related to Data Protection.

33.2 References[edit]

- EDPS Glossary

34 Data Protection Directive

34.1 Definition[edit]

Data Protection Directive is *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;
- the notification of the processing to a supervisory authority.

The Directive also sets out principles for the transfer of personal data to third countries and provides for the establishment of data protection authorities in each EU Member State.

34.2 References[edit]

- EDPS Glossary

35 Data Protection Impact Assessment

35.1 Definition[edit]

Data Protection Impact Assessment is an assessment that must be carrierd by the Data Controller of the impact of the envisaged processing operations on the protection of Personal Data when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

This assessment has to be done prior to the processing and, in particular if using new technologies, has to take into account the nature, scope, context and purposes of the processing.

A single assessment may address a set of similar processing operations that present similar high risks, as stated in the Article 39 of Regulation 2018/1725.

35.2 References[edit]

- EDPS Glossary

36 Data Protection Officer

36.1 Definition[edit]

A **Data Protection Officer** (DPO) is an entity within or authorised by an organisation to monitor internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects and the supervisory authority.

Each European Union Community institution and body shall, in order to comply with Regulation (EU) 2018/1725, have a Data Protection Officer with the following role and responsibilities:

- The DPO should be an expert on data protection law and practices
- Be in a position to operate independently within the organisation
- Ensure the internal application of the Regulation
- That the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operations.
- The DPO shall keep a register of processing operations performed or controlled by the institution or body.

36.2 References[edit]

- EDPS Glossary

37 Data Protection Requirement

37.1 Definition[edit]

Data Protection Requirement. Requirements defining how data about individuals are held.

Covers:

- what information i sheld
- who information can be divulged to
- the individual's rights in respect of that information

37.2 Example[edit]

An example is the EU DA directive and laws, which make the data the property of the individual that data is about. The EU defines Personal Data and Sensitive Personal Data. For credit reference agencies the latter would be covered. More detail about whether they can divulge facts which are not subject to formal judgements etc.

37.3 Disclaimer[edit]

38 Data Quality

38.1 Contents

38.2 Definition[edit]

Data Quality (also *Data Integrity*) refers to the condition of information sets (data) that are to be used as inputs for qualitative or quantitative risk assessment e.g. in the form of Portfolio Information, Algorithms and/or other decision support tools

Regulated institutions are required to have in place a formal Data Quality Management Framework[1]

38.3 Examples[edit]

- In order to support to the development of an internal Credit Scorecard, a firm must have access to historical credit data that meet data quality criteria
- In Data Privacy context data quality[2] refers to a set of principles laid down in Article 5 of the GDPR and Article 4 of Regulation (EU) 2018/1725, namely:
    - Lawfulness, fairness and transparency
    - Purpose limitation
    - Data minimisation
    - Accuracy
    - Storage limitation
    - Integrity and confidentiality

38.4 Issues and Challenges[edit]

- During the Financial Crisis data quality was identified as a contributing cause to poor risk management [3]
- Data quality issues are a significant component of Model Risk, colloquially referred to as the "garbage in, garbage out" principle.

38.5 See Also[edit]

- Wikipedia on Data quality

38.6 References[edit]

1. ? ECB guide to internal models - Credit Risk, Sep 2018
2. ? EDPS Glossary
3. ? BCBS 239: Principles for effective risk data aggregation and risk reporting

39 Data Recipient

39.1 Definition[edit]

A **Data Recipient** of personal data can be used to indicate any entity that receives personal data. This can be a Third Party, Processor (GDPR), or even a Controller.

According to Article 3 (13) of the Regulation (EU) 2018/1725 **Data Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing; "

Notifications of processing operations have to comprise information on the recipients of the personal data. A recipient can be a third party (with the exception of authorities which in the framework of a particular inquiry receive data - in such cases, they shall only be regarded as a third party).

39.2 Example[edit]

An illustrative example may be salary payments of officials of the EU institutions and bodies. The salary slip does not only go to the employee, but also to the institution or body where he or she works, and Eurostat receive the data (compiled).

39.3 References[edit]

- EDPS Glossary

40 Data Retention

40.1 Definition[edit]

Data Retention refers to all obligations on the part of controllers to retain Personal Data for certain purposes.

The Data Retention Directive (Directive 2006/24/EC (pdf)) contains an obligation for providers of electronic communications to retain traffic and location data of communications through telephone, e-mail, etc. The retention takes place for the purpose of the investigation, detection and prosecution of serious crime.

To limit how long you keep personal data is part of Data Minimization. The rule of thumb is "as long as necessary, as short as possible", although sometimes legal rules may impose fixed periods. Data that are no longer retained cannot fall into the wrong hands, nor be abused, meaning that defining and enforcing limited conservation periods helps to protect the people whose data are processed.

40.2 References[edit]

- EDPS Glossary

41 Data Security

41.1 Definition[edit]

Data Security

41.2 References[edit]

- EDPS Glossary

42 Data Subject

42.1 Definition[edit]

The **Data Subject** is the person whose Personal Data are collected, held or processed. The term 'data subject' is specific to the GDPR, but is functionally equivalent to the term 'individual' and the ISO/IEC term 'PII Principle'.

42.2 References[edit]

- EDPS Glossary
- Data Privacy Vocabulary (DPV)

43 Data Transfer

43.1 Definition[edit]

Data Transfers are subject to specific safeguards when the recipient is located in a country outside the EU / European Economic Area (EEA) according to Chapter V of the GDPR and of Regulation (EU) No 2018/1725. See for instance the conditions for the transfer of PNR data or relating to the EU-US Privacy Shield scheme.

43.2 References[edit]

- EDPS Glossary

44 Data Trust Agreement

44.1 Contents

44.2 Definition[edit]

The **Data Trust Agreement** between the Managing Company and Custodian and a third party Data Trustee governs the handling of Private Data

44.3 Details[edit]

The Data Trustee holds the Decoding Key allowing for the decoding of the encrypted information provided to the Issuer to the extent necessary to identify the Transferred Receivable in accordance with the Data Trust Agreement and the Data Trustee shall only release the confidential Decoding Key in certain limited circumstances (denoted the Data Release Events)

44.4 Variations[edit]

None

44.5 Issues and Challenges[edit]

None

44.6 See Also[edit]

None

44.7 Disclaimer[edit]

- This information is provided as is without any representation of correctness, completeness or suitability for any purpose whatsoever. Refer to actual securitisation prospectuses for the definitive terms applicable in each case
- Definitions, detailed descriptions and other content may change at any time as further examples or relevant aspects are introduced

45 Data Trustee

45.1 Contents

45.2 Definition[edit]

The **Data Trustee** is an entity holding Decoding Keys allowing for the decoding of the encrypted information provided to the Issuer to the extent necessary to identify Transferred Receivables in accordance with the Data Trust Agreement circumstances

45.3 Details[edit]

When assets transferred to the securitisation involve personal data subject to privacy laws, the Management Company and/or the Custodian my appoint a Data Trustee so Borrower-related Personal Data are generally encrypted in compliance with banking secrecy rules and data protection requirements.

45.4 Variations[edit]

None

45.5 Issues and Challenges[edit]

None

45.6 See Also[edit]

None

45.7 Disclaimer[edit]

- This information is provided as is without any representation of correctness, completeness or suitability for any purpose whatsoever. Refer to actual securitisation prospectuses for the definitive terms applicable in each case
- Definitions, detailed descriptions and other content may change at any time as further examples or relevant aspects are introduced

46 Data Usage Taxonomy

46.1 Definition[edit]

A **Data Usage Taxonomy** is a classification of distinct purposes (and their characteristics) behind Data Processing activities. Such purposes acquire special significance in the context of Data Privacy and Data Privacy Risk linked to Personal Data.

Academic Research	conduct or assist with research conducted in an academic context e.g. within universities
Access Control	conduct or enforce access control
Advertising	Advertising is a subset of Marketing. Advertising by itself does not indicate 'personalisation' i.e. personalised ads.
Commercial Interest	carry out activities with a commercial interest i.e. of profit or benefit to the Data Controller
Commercial Research	conduct research in a commercial setting e.g. in a company
Communication for Customer Care	communicate with users via email, phone, sms, chat or push messages regarding your requests.
Create Event Recommendations	create and provide personalised recommendations for events
Create Personalized Recommendations	create and provide personalised recommendations
Create Product Recommendations	create product recommendations e.g. suggest similar products
Customer Care	provide assistance for customer complaints and satisfaction
Delivery of Goods	deliver goods and services
Direct Marketing	carry out direct marketing i.e. marketing communicated directly to the individual
Fraud Prevention and Detection	detect and prevent fraud
Identity Verification	verify and authorise identity
Improve Existing Products and Services	improve existing products and services
Improve Internal CRM Processes	improve customer-relationship management (CRM) processes
Increase Service Robustness	improve the robustness and resilience of services
Internal Resource Optimisation	optimise internal resources used by the organisation e.g. resource usage
Legal Compliance	fulfill obligations or requirements towards achieving compliance with law or regulations.
Marketing	carry out marketing i.e. promoting, selling, and distributing a product or service
Non-Commercial Research	conduct research in a non-commercial setting e.g. for a non-profit-organisation (NGO)
Optimisation for Consumer	optimise activities and services for the consumer or user
Optimisation for Controller	optimise activities and services for the Data Controller
Optimise User Interface	optimise interfaces presented to the user
Payment	process users? payment transactions.
Personalised Advertising	provide personalised advertising
Personalised Benefits	personalise benefits received by the user
Registration and Authentication	register, authenticate, and identify in context of a service.
Requested Service Provision	
Research and Development	conduct research and development for new methods, products, or services
Security	ensure and enforce security e.g. of data
Sell Data to Third Parties	sell data or information to third parties
Sell Insights from Data	sell or commercially provide insights obtained from analysis of data
Sell Products to Data Subject	sell products or services
Sell Targetted Advertisements	sell or provide targetted advertisements
Service Optimization	optimise service or activity
Service Personalization	personalise service or activity
Service Provision	provide service or activity
Social Media	market through and on social media.
Analytics	calculate, analyse, and report user behaviour and events for a service or product.

User Interface Personalisation	personalise interfaces presented to the user

46.2 See Also[edit]

- Personal Data Taxonomy
- Data Processing Taxonomy

46.3 References[edit]

- Data Privacy Vocabulary (DPV)

47 E-privacy Directive

47.1 Definition[edit]

The **E-privacy Directive** 2009/136/EC came into force in May 2011, concerns the processing of personal data and the protection of privacy in the electronic communications sector (pdf). It is usually referred to as the "E-privacy Directive" and is an amendment of Directive 2002/58/EC.

The E-privacy Directive covers processing of personal data and the protection of privacy including provisions on:

- the security of networks and services;
- the confidentiality of communications;
- access to stored data;
- processing of traffic and location data;
- calling line identification;
- public subscriber directories; and
- unsolicited commercial communications ("spam").

The main changes to the 2002 Directive include a rule requiring the notification of data breaches (for instance someone whose personal data are lost, modified or accessed unlawfully while being treated by its electronic communications provider should be notified if this breach is likely to affect him/her negatively) and an extension of the Directive to also cover various electronic tags, strengthened enforcement rules, etc.

47.2 References[edit]

- EDPS Glossary

48 EDPS Opinion

48.1 Definition[edit]

The EDPS opinion is an important instrument of the European Data Protection Supervisor, both in the supervisory role and as advisor on proposals for EU legislation.

An opinion is issued on compliance of a processing operation with Regulation (EU) 2018/1725 and to make recommendations to the institution or body concerned. Such opinions are published on the EDPS website (Supervision section).

Opinions on proposals for EU legislation give a full analysis of the proposal from the perspective of data protection and may be discussed in the European Parliament and the Council. Such opinions are published in the C version of the Official Journal of the European Union and on the EDPS website (Consultation section). The EDPS adopts opinions on proposals for EU legislation and also on related instruments (communications, international agreements, comitology tools).

48.2 References[edit]

- EDPS Glossary

49 Eurodac

49.1 Definition[edit]

Council Regulation 2725/2000 of 11 December 2000 (pdf) establishes a system known as "Eurodac", i.e. a fingerprint database that assists the asylum procedure. It mainly helps to determine which Member State is competent for asylum applications (see Council Regulation 407/2002 laying down certain rules to implement Regulation 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention).

The system consists of a central unit, a computerised central database for comparing the fingerprint data of asylum applicants, and means of data transmission between the Member States and the central database. The EDPS is responsible for supervision of the system in cooperation with the competent national data protection authorities.

49.2 References[edit]

- EDPS Glossary

50 European Data Protection Board

50.1 Definition[edit]

The **European Data Protection Board** (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Economic Area (EEA), and promotes cooperation between the EEA?s data protection authorities.

The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The supervisory authorities of the EFTA EEA States are also members with regard to the GDPR related matters and without the right to vote and being elected as chair or deputy chairs. The EDPB is established by the General Data Protection Regulation (GDPR), and is based in Brussels. The European Commission and -with regard to the GDPR related matters- the EFTA Surveillance Authority have the right to participate in the activities and meetings of the Board without voting right.

The EDPB has a Secretariat, which is provided by the EDPS. A Memorandum of Understanding determines the terms of cooperation between the EDPB and the EDPS. In addition to providing the Secretariat of the EDPB, the EDPS is also a full member of the EDPB and contribute actively to the discussions and drafting of documents published by the EDPB. The EDPS participates on a regular basis in the plenary and Expert subgroup meetings of the EDPB.

50.2 See Also[edit]

- European Data Protection Supervisor

50.3 References[edit]

- EDPS Glossary

51 European Data Protection Supervisor

51.1 Definition[edit]

The **European Data Protection Supervisor** (EDPS) is an independent supervisory authority established in accordance with Regulation (EU) No 2018/1725, on the basis of Article 16 TFEU.

The EDPS' 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 the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals;
- advising EU institutions and bodies on all matters relating to the processing of personal information. We are consulted by the EU legislator on proposals for legislation and new policy developments that may affect privacy;
- monitoring new technology that may affect the protection of personal information;
- intervening before the Court of Justice of the EU to provide expert advice on interpreting data protection law;
- cooperating with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information.

51.2 References[edit]

- EDPS Glossary

52 Federated Learning Glossary

52.1 Contents

52.2 Federated Learning Glossary[edit]

A Glossary of Federated Learning terminology. The glossary covers a cross-section of terms that are relevant for *privacy-preserving computatio*n, spanning domains such as cryptography, database architectures and common statistical / machine learning algorithms. It does not aim to be exhaustive in any of those contributing domains.

52.2.1 Categories[edit]

For easier use of the glossary we classify terms according to context in which they arize. NB: The boundaries may not always be crystal clear:

- **Use Case** is a general application domain where some type of federated analysis is used
- **Process** is a required procedure
- **Risk Factor** is any aspect that can compromise / invalidate the premise of federated analysis (not necessarily malicious)
- **Property** is any rigorously defined aspect of a federated system that measures or guarantees e.g. privacy or security features
- **Algorithm** in this context are federated algorithms for data analysis, NOT the low level computation primitives (see Protocol)
- **Protocol** is any concretely defined pattern of information exchange (that is specifically useful in a federated context)
- **Architecture** is a scheme or organizational pattern of organizations, computational or storage devices etc. that defines a particular type of federation
- **Agent** is any entity within an overal architecture

52.2.2 Glossary[edit]

Term	Acronym	Meaning and Context	Category	Links / References
Federated Learning	FL	A machine learning paradigm that trains an algorithm across multiple devices or servers holding local data samples, without exchanging them. A centralised model is trained by locally computing updates and merging them to the centralised model without sharing data.	Use Case	Wikipedia
Privacy by Design		Privacy by design aims at building privacy and Data Protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with Data Privacy and data protection principles	Architecture	
Privacy Preserving Technology	PET	A coherent system of information and communication technology (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system	Architecture	
Privacy-Preserving Computation	PPC	Any general IT architecture that allows performing computations on networked computing devices while preserving some aspect of Data Privacy	Use Case	
Privacy-Preserving Data Mining	PPDM	The extraction of relevant knowledge from large amount of data (Big Data), while protecting at the same time sensitive information.	Use Case	
Secure Multi-Party Computation	MPC	A subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. SMC guarantees that none of the parties share anything with	Protocol	Wikipedia

Term	Acronym	Meaning and Context	Category	Links / References
		each other or with any third party, it can not prevent an adversary from learning some individual information		
Federated Database System	FDBS	A type of meta-database management system (DBMS), which transparently maps multiple autonomous database systems into a single federated database	Architecture	Wikipedia
Differential Privacy		?-differential privacy. A mathematical definition for the privacy loss associated with any data release drawn from a statistical database. It measures, e.g., to what extent the parameters or predictions of a model reveal information about any individual points in the training dataset. It ensures that the addition or removal does not substantially affect the outcome of any analysis.	Property	Wikipedia
Data Federation		Also Data Sharing. It is the general process of aggregating / sharing data that exist in distributed data sources	Process	Wikipedia
k-anonymity		A release of data is said to have the k-anonymity property if the information for each person contained in the release cannot be distinguished from at least k ? 1 individuals whose information also appear in the release	Property	Wikipedia
Data Anonymization		The process of removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous	Process	Wikipedia
Data Re-Identification		Also de-anonymization. Is the risk rising from the possibility of matching anonymous data with publicly available information, or auxiliary data, to discover information that was deemed private	Risk Factor	Wikipedia
Homomorphic Encryption	HE	A form of encryption allowing one to perform calculations on encrypted data without decrypting it first. Homomorphic encryption is a public key system, where any party can encrypt its data with a known public key and perform calculations with data encrypted by others with the same public key. Arbitrarily complicated functions of the data can be computed this way (?Fully Homomorphic Encryption?) though at greater computational cost.	Protocol	Wikipedia
Private Set Intersection		A secure multiparty computation cryptographic technique (MPC) that allows two parties holding sets to compare encrypted versions of these sets in order to compute the intersection. Neither party reveals anything to the counterparty except for the elements in the intersection.	Protocol	Wikipedia
Alice and Bob		Alice and Bob are fictional characters commonly used as placeholders in discussions about cryptographic protocols or systems. They typically represent agents possessing (or seeking) private information	Agent	Wikipedia
Trusted Third Party	TTP	An entity which facilitates interactions between two parties who both trust the third party. Whether a TTP exists or not has major design implications for privacy-preserving computations.	Agent	Wikipedia
Horizontally Partitioned Data		A data distribution design that applies to structured data. In horizontally partitioned data different rows from a common schema are located in distinct databases / devices. For example distinct sub-samples from a population that are stored separately	Architecture	
Vertically Partitioned Data		A data distribution design that applies to structured data. In vertically partitioned data different columns from a common schema are located in distinct databases / devices. For example distinct features characterising a population and stored separately	Architecture	
Private Information Retrieval	PIR	A protocol that allows a user to retrieve an item from a database without revealing which item is retrieved. PIR is a weaker version of 1-out-of-n oblivious transfer, where it is also required that the user should not get information about other database items. Private information retrieval is a functionality for one client and one server.	Protocol	Wikipedia
Oblivious Transfer	OT	A type of protocol in which a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred	Protocol	Wikipedia
Garbled Circuit	GC	A protocol that enables two-party secure computation in which two mistrusting parties can jointly evaluate a function over their private inputs without the presence of a trusted third party.	Protocol	Wikipedia
	PII		Risk Factor	Wikipedia

Term	Acronym	Meaning and Context	Category	Links / References
Personally Identifiable Information		Personal data, also known as personal information or personally identifiable information is any information relating to an identifiable person. It the subject of various regulations (e.g. HIPAA, GDPR)		
Federated Data Analysis		Also Federated Analysis, Federated Data Mining. A general term denoting the analysis of distributed datasets	Use Case	Wikipedia
Client/Server Architecture		An architecture for federated data analysis that shares models, model parameters or other statistical aggregated information rather individual data / information with a central server that is operated by a trusted third party	Architecture	Wikipedia
Decentralized Architecture		A decentralized architecture for federated data analysis does not require a central node (server) to collect aggregate intermediary results from participating entities but rather exchanges information on a a peer-to-peer basis	Architecture	Wikipedia
Zero-Knowledge Proof	ZKP	A protocol by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x.	Protocol	Wikipedia
Federated Data System		Denotes the overall foundation of shared technology architecture that enables federated data analysis. It extends beyond the specific federated database architecture and includes e.g. operational components such security, auditing, authentication and access rights.	Architecture	
Electronic Health Record	EHR	The systematic collection and storage of patient health information in a digital format. Records will include a variety of data formats. Federation of EHR constitutes one of major use cases of federated analysis.	Use Case	Wikipedia
Local Differential Privacy		A model of differential privacy with the added requirement that even if an adversary has access to the personal responses of an individual in a database, that adversary will still be unable to learn too much about the user's personal data. Algorithms with differential privacy necessarily incorporate some amount of randomness or noise, which can be tuned to mask the influence of the user on the output.	Property	Wikipedia
Non-IID Challenge		The challenge that data samples available for federated analysis may not satisfy the non-independent and non-identically distributed (IDD) property that is a precondition for the validity of various algorithms and statistical analyses	Risk Factor	[1]
Trusted Execution Environment	TEE	A secure area of a main processor (Also Secure Enclave). It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. TEEs provide the ability to run code on a remote machine, even if not trusting the machine?s owner/administrator. This is achieved by limiting the capabilities of any party, including the administrator.	Architecture	Wikipedia
Verifiable Computation		A property enabling one party to prove to another party that it has executed the desired behavior on its data faithfully, without compromising the potential secrecy of the data	Property	Wikipedia
Patient Similarity Learning		Patient similarity learning aims to develop computational algorithms for defining and locating clinically similar patients to a query patient under a specific clinical context	Use Case	[2]
Federated Stochastic Gradient Descent	FedSGD	Federated stochastic gradient descent is the direct transposition of the classic algorithm to the federated setting, by using a random fraction C of the nodes and using all the data on a given node. The gradients are averaged by the server proportionally to the number of training samples on each node, and used to make a gradient descent step	Algorithm	[3]
Federated Averaging	FedAvg	Federated averaging (FedAvg) is a generalization of FedSGD, which allows local nodes to perform more than one batch update on local data and exchanges the updated weights rather than the gradients	Algorithm	[4]
Federated Principal Component Analysis	FedPCA	Computing principal components on federated data	Algorithm	[5]

52.3 See Also[edit]

- Jupyter Resources for Privacy-Preserving Computation
- Federation
- Open Source Federation Platforms

52.4 Disclaimers[edit]

- This glossary is not in any way or form attempting to attribute priority for any of the methodologies / algorithms mentioned. Consult the academic literature.

52.5 References[edit]

1. ? The Non-IID Data Quagmire of Decentralized Machine Learning, Kevin Hsieh, Amar Phanishayee, Onur Mutlu, Phillip B. Gibbons
2. ? Privacy-Preserving Patient Similarity Learning in a Federated Environment: Development and Analysis Junghye Lee; Jimeng Sun; Fei Wang; Shuang Wang; Chi-Hyuck Jun; Xiaoqian Jiang
3. ? Privacy Preserving Deep Learning, R. Shokri and V. Shmatikov
4. ? Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-Efficient Learning of Deep Networks from Decentralized Data.
5. ? Federated Principal Component Analysis Andreas Grammenos, Rodrigo Mendoza-Smith, Jon Crowcroft, Cecilia Mascolo

53 GDPR Third Country

53.1 Definition[edit]

A **GDPR Third Country** is a country which is not bound by the General Data Protection Regulation (GDPR) - as opposed to the 28 Member States of the EU and the three European Economic Area (EEA) countries Norway, Liechtenstein and Iceland.

Third countries may be recognised as offering an adequate level of protection for personal data in order to enable transfers of personal data from the EU and EEA Member States to them.

The Commission has so far recognized Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan Jersey, New Zealand, Switzerland, Uruguay and USA (if the recipient belongs to the Privacy Shield), as providing adequate protection.

The effect of such a decision is that personal data can flow from the EU and EEA Member States to that third country (within the limit of the material scope as described by each Decision) without any further requirements.

53.2 References[edit]

- EDPS Glossary

54 Information Security

54.1 Definition[edit]

Information Security. The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.

55 IWGDPT

55.1 Definition[edit]

IWGDPT stands for International Working Group on Data Protection in Telecommunications

55.2 References[edit]

- EDPS Glossary

56 Passenger Name Record

56.1 Definition[edit]

Passenger Name Record (PNR) is the information collected by airlines or travel agencies at the time a passenger makes a reservation, before travelling. It differs from Advanced Passenger Information (API), which is collected later at the time of boarding.

In addition to the name of the passenger, PNR includes all information necessary for the reservation, such as:

- the travel agency responsible for the booking;
- the itinerary (including connections);
- the flights (number, date, time);
- groups of persons registered under the same booking;
- the passenger's contact details (telephone number, address, etc);
- payment/billing information;
- hotel or car booking;
- special service requests (such as seat number, special meal, medical assistance);
- "frequent flyer" information.

Enforcement authorities have shown interest in the collection of PNR data, with a view to fighting terrorism and other forms of crimes. The European Union has concluded agreements with third countries requesting such information, in order to establish minimal data protection safeguards on the use of this information. The Article 29 Working Party and the EDPS have adopted official opinions on these agreements

56.2 References[edit]

- EDPS Glossary

57 Personal Data

57.1 Definition[edit]

Personal Data denotes any Dataset that pertains to a particular Natural Person. The scope of personal data is very wide, covering in-principe all human activity. An informal definition consists of any data directly or indirectly associated or related to an individual. This definition is overlapping with the ISO/IEC definition of Personally Identifiable Information (PII).

In EU context, according to Article 3 (1) of Regulation (EU) 2018/1725: "?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, mental, economic, cultural or social identity of that natural person;".

The name and the social security number are two examples of personal data which relate directly to a person. But the definition also extends further and also encompasses for instance e-mail addresses and the office phone number of an employee. Other examples of personal data can be found in information on physical disabilities, in medical records and in an employee's evaluation.

Personal data which is processed in relation to the work of the data subject remain personal/individual in the sense that they continue to be protected by the relevant data protection legislation, which strives to protect the privacy and integrity of natural persons. As a consequence, data protection legislation does not address the situation of legal persons (apart from the exceptional cases where information on a legal person also relates to a physical person).

57.2 See Also[edit]

- Personal Data Taxonomy
- Sensitive Personal Data
- Data Privacy

58 Personal Data Filing System

58.1 Definition[edit]

According to Article 3 (7) of Regulation (EU) 2018/1725, **Personal Data Filing System** refers to any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

The definition is independent of the size of the filing system, which may vary according to the circumstances. In some cases, such as for instance the case of disciplinary files for a small sized EU-body, the filing system can comprise just a handful of entries.

58.2 References[edit]

- EDPS Glossary

59 Personal Data Taxonomy

59.1 Contents

59.2 Definition[edit]

A **Personal Data Taxonomy** is a classification of Personal Data according to various characteristics. A immediate use of such a taxonomy is to identify Sensitive Personal Data.

59.3 DPV Taxonomy[edit]

- Data internal to the Data Subject (part of their mental models and memories)
  - Preferences
  - Knowledge
  - Beliefs
- External Data
  - Behavioral
  - Demographics
  - Physical
  - Sexual
  - Personally Identifying Information
- Social Environment
  - Family
  - Friends
  - Professional
  - Public Life
  - Communications
- Financial Data
  - Transactional
  - Ownership
  - Financial Accounts
- Digtal Tracking Data
  - Location
  - Device Telemetry
  - Contact

Data	Description	Category	Subcategory
Accent	Information about linguistic and speech accents.		
Account Identifier	Information about financial account identifier.		
Acquantaince	Information about acquaintainces in a social network.		
Age	Information about age		
Apartment Owned	Information about apartment(s) owned and its history		
Association	Information about associations in a social network with other individuals, groups, or entities e.g. friend of a friend		
Attitude	Information about attitude.		
Authenticating	Information about authentication and information used for authenticating		
Authentication History	Information about prior authentication and its outcomes such as login attempts or location.		
Bank Account	Information about bank accounts.		
Behavioral	Information about behavior or activity		

Data	Description	Category	Subcategory
Biometric	Information about biometrics and biometric characteristics.		
Blood Type	Information about blood type.		
Browser Fingerprint	Information about the web browser which is used as a 'fingerprint'		
Browsing Behavior	Information about browsing behavior.		
BrowsingBehaviour			
Browsing Referral	Information about web browsing referrer or referral, which can be based on location, targeted referrals, direct, organic search, social media or actions, campaigns.		
Call Log	Information about the calls that an individual has made.		
Car Owned	Information about cars ownership and ownership history.		
Character	Information about character in the public sphere		
Communication	Information communicated from or to an individual		
Communications Metadata	Information about communication metadata in the public sphere		
Connection	Information about and including connections in a social network		
Contact	Information about contacts or used for contacting e.g. email address or phone number		
Country	Information about country e.g. residence, travel.		
Credit	Information about reputation with regards to money		
Credit Capacity	Information about credit capacity.		
Credit Card Number	Information about credit card number		
Credit Record	Information about credit record.		
Credit Score	Information about credit score.		
Credit Standing	Information about credit standing.		
Credit Worthiness	Information about credit worthiness.		
Criminal	Information about criminal activity e.g. criminal convictions or jail time		
Criminal Charge	Information about criminal charges.		
Criminal Conviction	Information about criminal convictions.		
Criminal Pardon	Information about criminal pardons.		
DNA Code	Information about DNA.		
Demeanor	Information about demeanor.		
Demographic	Information about demography and demographic characteristics		
Derived Personal Data	Derived data is data that is obtained or derived from other data.		
Device Applications	Information about applications or application-like software on a device.		
Device Based	Information about devices		
Device Operating System	Information about the operating system (OS) or system software that manages hardware or software resources.		
Device Software	Information about software on or related to a device.		
Dialect	Information about linguistic dialects.		
Disability	Information about disabilities.		
Disciplinary Action	Information about disciplinary actions and its history		
Dislike	Information about dislikes or preferences regarding repulsions.		
Divorce	Information about divorce(s).		
Drug Test Result	Information about drug test results.		
Email Address	Information about Email address.		
Email Content	Information about the contents of Emails sent or received		
Employment History	Information about employment history		
Ethnic Origin	Information about ethnic origin		
Ethnicity	Information about ethnic origins and lineage		

Data	Description	Category	Subcategory
External	Information about external characteristics that can be observed		
Family	Information about family and relationships		
Family Health History	Information about family health history.		
Family Structure	Information about family and familial structure.		
Favorite	Information about favorites		
Favorite Color	Information about favorite color.		
Favorite Food	Information about favorite food.		
Favorite Music	Information about favorite music.		
Fetish	Information an individual's sexual fetishes		
Financial	Information about finance including monetary characteristics and transactions		
Financial Account	Information about financial accounts.		
Financial Account Number	Information about financial account number		
Fingerprint	Information about fingerprint used for biometric purposes.		
Friend	Information about friends in a social network, including aspects of friendships such as years together or nature of friendship.		
GPS Coordinate	Information about location expressed using Global Position System coordinates (GPS)		
Gender	Information about gender		
General Reputation	Information about reputation in the public sphere		
Geographic	Information about location or based on geography (e.g. home address)		
Group Membership	Information about groups and memberships included or associated with a social network		
Hair Color	Information about hair color		
Health	Information about health.		
Health History	Information about health history.		
Health Record	Information about health record.		
Height	Information about physical height		
Historical	Information about historical data related to or relevant regarding history or past events		
House Owned	Information about house(s) owned and ownership history.		
IP Address	Information about the Internet protocol (IP) address of a device		
Identifying	Information that uniquely or semi-uniquely identifies an individual or a group		
Income	Information about financial income e.g. for individual or household or family		
Income Bracket	Information about income bracket.		
Individual Health History	Information about information health history.		
Intention	Information about intentions		
Interaction	Information about interactions in the public sphere		
Interest	Information about interests		
Internal	Informatoin about internal characteristics that cannot be seen or observed		
Job	Information about professional jobs		
Knowledge and Beliefs	Information about knowledge and beliefs		
Language	Information about language and lingual history.		
Life History	Information about personal history regarding events or activities - including their occurrences that might be directly related or have had an influence (e.g. World War, 9/11)		
Like	Information about likes or preferences regarding attractions.		
LinkClicked	Information about the links that an individual has clicked.		
Loan Record	Information about loans, whether applied, provided or rejected, and its history		
Location	Information about location		
MAC Address	Information about the Media Access Control (MAC) address of a device		

Data	Description	Category	Subcategory
Marital Status	Information about marital status and history		
Marriage	Information about marriage(s).		
MedicalHealth	Information about health, medical conditions or health care		
Mental Health	Information about mental health.		
Name	Information about names associated or used as given name or nickname.		
Official ID	Information about an official identifier or identification document		
Offspring	Information about offspring(s).		
Opinion	Information about opinions		
Ownership	Information about ownership and history, including renting, borrowing, possessions.		
PIN Code	Information about Personal identification number (PIN), which is usually used in the process of authenticating the individual as an user accessing a system.		
Parent	Information about parent(s).		
Password	Information about password used in the process of authenticating the individual as an user accessing a system.		
Payment Card	Information about payment card such as Credit Card, Debit Card.		
Payment Card Expiry	Information about payment card expiry such as a date.		
Payment Card Number	Information about payment card number.		
PersonalDataCategory			
Personal Possession	Information about personal possessions.		
Personality	Information about personality (e.g., categorization in terms of the Big Five personality traits)		
Philosophical Belief	Information about philosophical beliefs.		
Physical Address	Information about physical address.		
PhysicalCharacteristic	Information about physical characteristics		
Physical Health	Information about physical health.		
Physical Trait	Information about defining traits or features regarding the body.		
Picture	Information about visual representation or image e.g. profile photo.		
Piercing	Information about piercings		
Political Affiliation	Information about political affiliation and history		
Preference	Information about preferences or interests		
Prescription	Information about medical and pharmaceutical prescriptions		
Privacy Preference	Information about privacy preferences		
Proclivitie	Information about proclivities in a sexual context		
Professional	Information about educational or professional career		
Professional Certification	Information about professional certifications		
Professional Evaluation	Information about professional evaluations		
Professional Interview	Information about professional interviews		
Public Life	Information about public life		
Purchase	Information about purchases such as items bought e.g. grocery or clothing		
Purchases and Spending Habit	Information about analysis of purchases made and money spent expressed as a habit e.g. monthly shopping trends		
Race	Information about race or racial history.		
Reference	Information about references in the professional context		
Relationship	Information about relationships and relationship history.		
Religion	Information about religion, religious inclinations, and religious history.		
Religious Belief	Information about religion and religious beliefs.		
Retina	Information about retina and the retinal patterns.		
Room Number	Information about location expressed as Room number or similar numbering systems		

Data	Description	Category	Subcategory
Salary	Information about salary		
Sale	Information about sales e.g. selling of goods or services		
School	Information about school such as name of school, conduct, or grades obtained.		
Secret Text	Information about secret text used in the process of authenticating the individual as an user accessing a system, e.g., when recovering a lost password.		
Service Consumption Behavior	Information about the consumption of a service, e.g. time and duration of consumption.		
Sexual	Information about sexuality and sexual history		
Sexual History	Information about sexual history		
Sexual Preference	Information about sexual preferences		
Sibling	Information about sibling(s).		
Skin Tone	Information about skin tone		
Social	Information about social aspects such as family, public life, or professional networks.		
Social Media Communication	Information about social media communication, including the communication itself and metadata.		
Social Network	Information about friends or connections expressed as a social network		
Social Status	Information about social status		
Special Category Personal Data	trade union membership, which is explicitly included in the taxative listing in GDPR Art. 9 (1), is not covered yet.		
TV Viewing Behavior	Information about TV viewing behavior, such as timestamps of channel change, duration of viewership, content consumed		
Tattoo	Information about tattoos		
Tax	Information about financial tax e.g. tax records or tax due		
Telephone Number	Information about telephone number.		
Thought	Information about thoughts		
Tracking	Information used to track an individual or group e.g. location or email		
Transaction	Information about financial transactions e.g. bank transfers		
Transactional	Information about a purchasing, spending or income		
UID	Information about unique identifiers.		
Username	Information about usernames.		
Voice Communication Recording	Information about vocal recorded communication (e.g. telephony, VoIP)		
Voice Mail	Information about voice mail messages.		
Weight	Information about physical weight		
Work History	Information about work history in a professional context		

59.4 See Also[edit]

- Data Processing Taxonomy

59.5 References[edit]

- Data Privacy Vocabulary (DPV)[[Category:Taxonomy]

60 Personally Identifiable Information

60.1 Definition[edit]

Personally Identifiable Information means information identifiable to any person, including, but not limited to:

- information that relates to a person's name
- social security numbers
- driver license numbers
- other identifying numbers
- and any financial identifiers
- health records
- financial records
- educational records
- business
- use or receipt of governmental services or other activities
- addresses
- telephone numbers
- computing device identifiers

60.2 See Also[edit]

- Personal Data

61 Privacy

61.1 Definition[edit]

Privacy is the ability of an individual to be left alone, out of public view, and in control of information about oneself.

One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy").

The concept of privacy therefore overlaps, but does not coincide, with the concept of Data Protection.

The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12) as well as in the European Convention of Human Rights (Article 8).

61.2 See Also[edit]

- Data Privacy

61.3 References[edit]

- EDPS Glossary

62 Privacy Enhancement Measures

62.1 Definition[edit]

Privacy Enhancement Measures refers to all policies, organizational arrangements, technology solutions and other measures that an organization may undertake to enhance Data Privacy.

Access Control Method	Methods which restrict access to a place or resource
Anonymization	Altering personal data irreversibly such that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party
Authentication Protocols	Protocols involving validation of identity i.e. authentication of a person or information
Authorisation Procedure	non-technical authorisation procedures: How is it described on an organisational level, who gets access to the data
Certification	Certification mechanisms, seals, and marks for the purpose of demonstrating compliance
Certification and Seal	Certifications, seals, and marks indicating compliance to regulations or practices
Code of Conduct	A set of rules or procedures outlining the norms and practices for conducting activities
Consultation	Consultation is a process of receiving feedback, advice, or opinion from an external agency
Consultation with Authority	Consultation with an authority or authoritative entity
Contract	Contractual terms governing data handling within the data controller
Data Protection Impact Assessment (DPIA)	Top class: Impact Assessment, and DPIA is sub-class
De-Identification	Conversion of identifiable personal data (PII) to un-identifiable personal data
Design Standard	A set of rules or guidelines outlining criterias for design
Encryption in Rest	Encryption of data when being stored (persistent encryption)
Encryption in Transfer	Encryption of data in transit e.g. when being transferred from one location to another, including sharing
GuidelinesPrinciple	Guidelines or Principles regarding processing and operational measures
Impact Assessment	Calculating or determining the likelihood of impact of an existing or proposed process, which can involve risks or detriments.
Legal Agreement	A legally binding agreement
Non-Disclosure Agreement (NDA)	Non-disclosure Agreements e.g. preserving confidentiality of information
Organisational Measure	Organisational measures required/followed when processing data of the declared category
Privacy Impact Assessment	Carrying out an impact assessment regarding privacy risks
Privacy by Default	Practices regarding selecting appropriate data protection and privacy measures as the 'default' in an activity or service
Privacy by Design	Practices regarding incorporating data protection and privacy in the design of information and services
Pseudo-Anonymization	PseudoAnonmyization or 'pseudonymisation? means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
Pseudonymisation and Encryption	Technical measures consisting of pseudoanonymization and encryption
Regularity of Re-certification	Policy regarding repetition or renewal of existing certification(s)
Risk Management Procedure	Data Protection Impact Assessments as per GDPR art 35, other Privacy Impact Assessments, threat severity assessment https://www.cnil.fr/en/privacy-impact-assessment-pia
Risk Mitigation Measure	Measures intended to mitigate, minimise, or prevent risk.
Seal	A seal or a mark indicating proof of certification to some certification or standard
Single Sign On	Use of credentials or processes that enable using one set of credentials to authenticate multiple contexts.
Staff Training	Practices and policies regarding training of staff members
Storage Deletion	Deletion or Erasure of data including any deletion guarantees
Storage Duration	Duration or temporal entity denoting limitation on storage of personal data

Storage Location	Location or geospatial scope where the data is stored
Storage Restoration	Regularity and temporal span of data restoration/backup mechanisms that guarantee that data is preserved
Storage Restriction	Restrictions required or followed regarding storage of data
Technical Measure	Technical measures required/followed when processing data of the declared category

62.2 References[edit]

- Data Privacy Vocabulary (DPV)

63 Privacy Enhancing Technology

63.1 Definition[edit]

Privacy Enhancing Technology (PET) refers to a coherent system of information and communication technologies that protect Data Privacy by eliminating or reducing Personal Data or by preventing unnecessary and/or undesired processing of personal data, all 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.

PETs can be stand-alone tools requiring positive action by consumers (who must purchase and install them in their computers) or be built into the very architecture of information systems.

PETs are part of a broader set of Privacy Enhancement Measures that address and support enhanced data privacy through **organizational** arrangements and measures that have a less explicit or important technological element.

63.2 References[edit]

- EDPS Glossary

64 Processing of Personal Data

64.1 Definition[edit]

Processing of Personal Data can consist of Personal Data being processed for a purpose, involving entities, using technical and organisational measures, subject to applicable [[Data Privacy Risk]], in the context of concrete Data Privacy Rights, and Legal Basis.

According to Article 3 (3) of Regulation (EU) 2018/1725, **Processing of Personal Data** refers to 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.

Personal data may be processed in many activities which relate to the professional life of a data subject. Examples from within the EU institutions and bodies include: the procedures relating to staff appraisals and to the billing of an office phone number, lists of participants at a meeting, the handling of disciplinary and medical files, as well as compiling and making available on-line a list of officials and their respective field of responsibilities.

Personal data relating to other natural persons than staff may also be processed. Such examples may concern visitors, contractors, petitioners, etc.

64.2 See Also[edit]

- Data Processor

64.3 References[edit]

- EDPS Glossary

65 Race

65.1 Definition[edit]

Race. A category based on a Natural Person's physical characteristics, such as bone structure and skin, hair, or eye color

65.2 See Also[edit]

- Sensitive Personal Data

65.3 Disclaimer[edit]

66 Radio Frequency Identification

66.1 Definition[edit]

Radio Frequency Identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.

An RFID tag is an object that can be applied to or incorporated into a product, an animal or a person for the purpose of identification or remote tracking through the use of radio waves.

The EDPS released an EDPS Opinion on the issue in December 2007, in which it underlines that RFID systems could play a key role in the development of the European information society, but also that the wide acceptance of RFID technologies should be facilitated by the benefits of consistent Data Protection safeguards.

66.2 References[edit]

- EDPS Glossary

67 Right of Access

67.1 Definition[edit]

The **Right of Access** is the right for any Data Subject to obtain from the Data Controller of a processing operation

- the confirmation that data related to him/her are being processed
- the purpose(s) for which they are processed,
- as well as the logic involved in any automated decision process concerning him or her.

This right also allows the data subject to receive communication in an intelligible form of the data undergoing processing and of information regarding the processing.

This right can be exercised without constraint, at any time within 1 month from the receipt of the request, and is free of charge (Article 14 of Regulation (EU) 2018/1725).

67.2 See Also[edit]

- Right of Information

67.3 References[edit]

- EDPS Glossary

68 Right of Information

68.1 Definition[edit]

The **Right of Information** refers to the information which shall be provided to a Data Subject whether or not the data have been obtained from the data subject.

Everyone has the right to know that their personal data are processed and for which purpose. The right to be informed is essential because it determines the exercise of other rights.

The information which must be provided relates to the identity of the controller, the purpose(s) of the processing, the recipients, as well as the existence of the right of access to data and the right to rectify the data.

The right of information for the person concerned is limited in some cases, such as for public safety considerations or for the prevention, investigation, identification and prosecution of criminal offences, including the fight against money laundering.

In the context of Data Processing operations within the EC institutions (see Articles 15 and 16 of Regulation (EU) 2018/1725), this right is often fulfilled by a privacy statement.

68.2 See Also[edit]

- Right to Object

68.3 References[edit]

- EDPS Glossary

69 Right to Object

69.1 Definition[edit]

According to Regulation (EU) 2018/1725 a Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (a) of Article 5(1), including profiling based on that provision.

The Data Controller shall no longer process the Personal Data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."

This right has to be brought to the attention of the data subject at the time of the first communication at the latest and shall be presented in a clear way separately from any other information (see Article 23 sub (2) of Regulation (EU) 2018/1725)

The data subject may use automated means by technical specifications in order to exercise their right to object in the context of the use of information society services, without prejudice to Articles 36 and 37 (see Article 23 sub (3) of Regulation (EU) 2018/1725).

According to Article 23 sub (4) of Regulation (EU) 2018/1725 "Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."

69.2 See Also[edit]

- Right to Restriction of Processing

69.3 References[edit]

- EDPS Glossary

70 Right to Restriction of Processing

70.1 Definition[edit]

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future..

As provided by Article 20 of Regulation (EU) 2018/1725, the data subject shall have the right to obtain from the controller the restriction of processing where:

- their accuracy is contested by the data subject, enabling though the controller to verify the accuracy, including the completeness of the data;
- or the processing is unlawful and the data subject opposes their erasure and demands their restriction of processing instead.
- or the controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof;
- or the data subject has objected to processing to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Personal data restricted can only be processed with the data subject's consent, for purposes of proof, or or for the protection of the rights of a third party, or for reasons of important public interest of the Union or of a Member State.

70.2 References[edit]

- EDPS Glossary

71 Safe Harbor Principle

71.1 Definition[edit]

Safe Harbor Principles are a set of privacy and data protection principles that, together with a set of frequently asked questions (FAQs) providing guidance for the implementation of the principles, have been considered by the European Commission to provide an adequate level of protection.

These principles were issued by the Government of the United States on 21 July 2000.

US organisations can claim that they comply with this framework. They should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) - under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce - or to the jurisdiction of another statutory body that will ensure compliance with the principles implemented in accordance with the FAQs.

71.2 References[edit]

- EDPS Glossary

72 Schengen Information System

72.1 Definition[edit]

The **Schengen Information Syste**m (SIS) is a large-scale IT system linked to the abolition of internal border controls of the Schengen territory (most of the EU territory plus a few other countries).

The SIS will be replaced by SIS II in order to allow the connection of more countries and to provide new functionalities (see EDPS Opinion on the establishment of SIS II (pdf).

The SIS contains information on objects (stolen cars, identity documents, etc.), as well as on persons. Personal information may be recorded in the SIS on:

- third states nationals who are banned from entry to Schengen territory;
- people wanted in relation with criminal proceedings or people under police surveillance;
- missing people who should be placed under protection, in particular minors.

72.2 References[edit]

- EDPS Glossary

73 Security Breach

73.1 Definition[edit]

A **Security Breach** occurs where a stated organisational policy or legal requirement regarding Information Security has been violated. However, every incident which suggests that the confidentiality, integrity or availability of the information has been compromised can be considered a security incident.

Every security breach will always be initiated by a security incident which, only if confirmed, may become a breach.

73.2 References[edit]

- EDPS Glossary

74 Sensitive Personal Data

74.1 Definition[edit]

Sensitive Personal Data. Special categories of Personal Data include data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural's sex life or sexual orientation" (Article 10 of Regulation (EU) 2018/1725; Article 9 of the GDPR)

The Data Processing of such information is in principle prohibited, except in specific circumstances. It is possible to process sensitive data for instance if the processing is necessary for the purpose of medical diagnosis, or with specific safeguards in the field of employment law, or with explicit consent of the data subject.

75 Third Party

75.1 Definition[edit]

According to Article 3 (14) of Regulation (EU) 2018/1725 **Third Party** shall mean "a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor are authorised to process the data."

In the context of the EU institutions and bodies, a third party may be a public authority or private party which temporarily needs to process the personal data of an official. This may be the case, for instance, if an official, who moves to his workplace to start work and who is temporarily entitled to VAT-exemption, buys a car. In that case, the car company, the insurance company, the Ministry of Finance and the authority responsible for the car register would be third parties.

75.2 References[edit]

- EDPS Glossary

76 Traffic Data

76.1 Definition[edit]

Traffic Data are data processed for the purpose of the conveyance of a communication on an electronic communications network.

According to the means of communication used, the data needed to convey the communication will vary, but may typically include contact details, time and location data.

Although such traffic data are to be distinguished from content data, both are quite sensitive as they give insight in confidential communications. These data therefore enjoy special protection in Articles 5 and 6 of the E-privacy Directive 2009/136/EC

76.2 References[edit]

- EDPS Glossary

77 Visa Information System

77.1 Definition[edit]

The **Visa Information System** (VIS) is a large scale IT system which will contain information, including photographs and fingerprint data about visa applicants. The EDPS issued an opinion on the establishment of the VIS in 2005 and another one about the access of law enforcement authorities to the VIS in 2006.

The information will be collected by consulates in the different Member States and then transferred to a central database, VIS, where it will be accessible by all Member States. In principle, the rolling out of the VIS should start in 2009.

One of the main purposes of the database is to fight ?visa shopping?. Citizens from more than 120 countries need visas to enter the EU. In the current situation, an applicant who has been rejected by one country?s consulate could continue applying to other consulates. Once VIS is in place, this will not be possible. Information on previous applications and reasons for rejection will be available through the new system. The inclusion of fingerprint and photograph information is intended to allow border checks to verify whether the person presenting the visa is in fact the person to whom it was issued.

The data protection supervision will be the responsibility of the EDPS at the level of the Central Unit and of the Member States? data protection authorities at national level. The EDPS and data protection authorities will jointly ensure coordination of that supervision.

77.2 See Also[edit]

- Passenger Name Record

77.3 References[edit]

- EDPS Glossary

78 Vulnerable Data Subject

78.1 Definition[edit]

Vulnerable Data Subject is a Data Subject which should be considered 'vulnerable' (particularly exposed to Data Privacy Risk) and therefore would require additional measures and safeguards.

78.2 References[edit]

- Data Privacy Vocabulary (DPV)