Universität Basel

Generalsekretariat

Glossary of terms

on the Website of the Data Protection Officer

Please note that the definitions in the glossary are not legally binding. The glossary is intended to provide a better understanding of the terms used in the context of data protection.

15. Dezember 2022 / lic. iur. Danielle Kaufmann (Data Protection Officer, University of Basel)

Term	Definition
Administrative assistance	Administrative assistance means the support provided by an authority to another authority requesting it. In the context of administrative assistance, there is usually a certain exchange of information on both sides. This exchange constitutes a processing of data, relevant under data protection law (cf. § 3 para. 5, 6 IDG-BS); consequently, there is a need for a legal basis.
Anonymisation	Anonymisation of data is the process of irrevocably removing the reference to a person, meaning the removal of all information that makes a person identifiable. Accordingly, data is anonymous if it is no longer possible to assign the data to a specific person or only with disproportionate effort.
Anonymous/anonymised data	Anonymised data is characterised by the irrevocable removal of the personal reference. However, the process of anonymisation usually requires the processing of personal data, which is why the provisions of data protection law must be taken into account beforehand. This is not the case, however, if data is collected anonymously from the very start, i.e. a reference to a person cannot be established from the beginning or can only be established with disproportionate effort.
Capacity for judgement	According to Art. 16 of the Swiss Civil Code, every person is capable of judgement if he or she can act rationally and this capacity is not restricted due to infancy, mental disability, mental disorder, intoxication or similar conditions. The capacity to judge must be assessed for each individual case. With regard to children, it is important to note that there is no statutory age limit.
CISO	*Chief Information Security Officer*; The person with overall responsibility for information security in an organisation.
Collection of data	Cf. Processing
Commissioned Data Processing	Commissioned data processing or data processing by third parties means that the processing of data is transferred to an external party (natural or legal person, public authority, etc.). Such processing applies, for example, to classic outsourcing, data storage in a cloud or the use of certain software, e.g. for survey purposes. Although processing is transferred from the data-controller to a third party (data-processor), the controller always remains responsible for the data-processing. For this reason, the controller must carefully

	select, clearly instruct and sign a data processing agreement with the external data-processor (cf. § 7 IDG-BS).
Consent (Informed)	Informed consent serves to protect the data subject from unlawful processing of data. Effective consent must fulfil a wide range of formal and substantive requirements and must always be given voluntarily. It can also be revoked at any time.
Controller	Cf. *Commissioned Data Processing*
Correctness (of the data)	Personal data must be correct and, insofar as the purpose of use requires, complete (cf. § 11 IDG-BS); the person responsible must actively ensure that this is the case. Incorrect data must be corrected or otherwise be deleted.
Data Protection	Data protection is the protection of private individuals against infringements of their privacy through improper collection, processing, storage and disclosure of their personal data.
Data protection impact assessment	The data protection impact assessment is an element of preventive data protection. It represents a structured risk analysis with regard to a planned data processing. Its aim is to identify any risks associated with that processing at the earliest stage in order to avoid them.
Data Protection Officer (DPO)	The data protection officer supervises the processing of personal data within an organisation, provides advice and training, carries out internal audits and is the central contact person for the supervisory authority as well as for staff, reserachers and students with regard to data protection issues.
Data protection review	Similar to the new IT services (cf. datasheet), it is also possible to check whether the data protection regulations have been complied with in relation to a research project or any other kind of planned data collection (e.g. in the context of bachelor's, master's and/or seminar theses).
Datasheet	Before a new IT service can be implemented at the university (e.g. transcription software), it must be assessed and approved from a data protection and information security perspective. This review approves or rejects the service for certain classes of data. The first step in the process of approving a new service is the submission of the datasheet by the person making the request (cf. template on the *Intranet*).
Disclosure of (personal) data	A data disclosure is always also a data processing. The disclosure of (special) personal data is permitted to a public body if a legal basis obliges or authorises it to do so, or if this is necessary for the fulfilment of a legally defined task. Only in individual cases does the express consent of the persons concerned legitimise the disclosure (§ 20 ff. IDG-BS). A distinction must be made between ordinary disclosure and the "disclosure of personal data for a non-personal purpose" (cf. Section 22 IDG-BS) as well as the "cross-border disclosure of personal data" (cf. Section 23 IDG-BS).
DPO-BS	(Unofficial) abbreviation for the Data Protection Officer of the Canton of Basel-Stadt.
Encryption	Technical encryption (also ciphering or cryptography) refers to the conversion of readable data (so-called plaintext) into ciphertext; the plaintext can only be recovered with the help of the key.

EU-GDPR	EU General Data Protection Regulation (Directive 95/46/EC)
Factual data	Information that does not relate in any way, directly or indirectly, to a person (e.g. amounts of money, flight movements, water temperatures). Data protection law is generally not applicable to processing of such data. Important: Through additional information or technical processing, factual data and anonymised data can (again) become personal data.
FADP	Federal Act on Data Protection (SR. 235.1)
Health data	Vgl. *personal data (special)*
IDG-BS	Information and Data Protection Act of the Canton of Basel-Stadt (IDG) (SG 153.260)
Information	Information is any record relating to the fulfilment of a public task, regardless of its form of presentation and information carrier (cf. § 3 para. 2 IDG-BS).
Information-Security	Information security is intended to ensure a variety of protection goals (in particular confidentiality, integrity and availability of data). Accordingly, public bodies must protect their data by means of appropriate organisational and technical measures (cf. § 8 IDG-BS). The measures depend on the type of data, the purpose of use and the state of technology.
Lawfulness	In line with the principle of "no action by a public body without a legal basis", the principle of legality states that all actions of the university must be based on a legal basis (cf. § 9 IDG-BS).
Personal data (special)	Personal data includes all information relating to a specific person or a person who can be identified through this information (cf. § 3 para. 3 IDG-BS). This includes, e.g., name, date of birth, e-mail address, telephone and mobile number, AHV number, matriculation number, bank data, IP address (with exceptions), gender, photograph or special characterising features (e.g. the only woman in team XY) etc. In addition to ordinary personal data, there is special personal data (cf. §3 para. 4 IDG-BS). Due to their significance, the way they are processed and/or because they are suitable for creating a profile of the person concerned, there is an increased risk to the fundamental rights of the persons concerned. This includes, for example, data on children and other vulnerable persons (refugees, ethnic minorities, etc.) as well as information on a person's health.
Pre-check (New: pre-consultation)	If the processing of personal data poses a particularly high risk to the rights of the data subjects due to the nature of the processing or the type of data, the planned processing must be submitted in advance to the DPO of the Canton of Basel-Stadt for a pre-check (cf. § 13 IDG-BS). This is necessary, for example, if >10,000 persons are affected by the processing or new technologies are used (e.g. AI).
Privacy by default	Means data protection through default settings; i.e. software and hardware products should be preset by default to be data protection-friendly for their users (e.g. no tedious refusal of cookies via opt-out).

Privacy by design	Means data protection through technology design. I.e. that suitable technical and organisational measures (so-called TOMs) for the protection of data should be integrated into software and hardware products right from the start (cf. § 8 para. 1 IDG-BS).
Privacy policy	Anyone who operates a website collects and processes personal data of visitors to the website. Therefore, a website always needs a privacy policy that provides information about what, for what, for how long and by whom personal data is processed; what measures the organisation takes to protect the privacy of the users; what rights the data subjects have etc. The more complex the data collection, the more detailed the privacy statement should be. In any case, it must be created individually for the respective website. Please note that specific terms of use may also have to be drawn up for the website in question.
Processing	The term includes any handling of personal data, regardless of the means and procedures used, but in particular the collection, storage, usage, disclosure, as well as archiving and the deletion (cf. § 3 para. 5, 6 IDG-BS).
Processing on behalf of	Cf. *Commissioned Data Processing*
Processor	Vgl. *Processing on behalf of*
Proportionality	The principle of proportionality stipulates that only suitable personal data and only as much personal data as necessary must be processed in order to achieve the pre-defined purpose (cf. § 9 para. 3 IDG-BS). At all times the rights of the persons concerned must be respected.
Protective measures	Personal data must be protected by appropriate organisational and technical measures (cf. § 8 IDG-BS). The measures taken depend on the type of data, the purpose of use and the current technology.
Pseudonymous/Pseudonymised data	In contrast to anonymous data, the reference to a person is not irrevocably removed in the case of pseudonymous data. Due to the fact that re-identification of the data subject is possible (e.g. using a code), the provisions of data protection law apply unchanged.
Public body	Public bodies are the organisational units of the canton and the communes that fulfil a public task; the organisational units of legal entities under cantonal and communal public law that fulfil a public task (e.g. the University of Basel as an institution under public law); private entities insofar as they are entrusted with the fulfilment of public tasks by the canton or communes.
Purpose and und limitation	A specific purpose must be defined at the beginning of each processing of personal data. This purpose must be communicated transparently to the persons concerned (cf. principle of transparency). The processed data may then only be processed for this defined purpose (cf. § 12 IDG-BS). In the event of any other use not communicated at the beginning (e.g. subsequent use for a new project), the consent of the persons concerned must be obtained again.
Research Datamanagement	Research data management refers to all organisational and technical measures and procedures for handling the data that occur in the course of a research process.

Rights of data subjects	With regard to data protection, the law grants the data subjects a wide range of rights. From the right of access to one's own information and (personal) data (cf. § 25 f. IDG-BS), to the protection of that data (cf. § 27 IDG-BS), or also blocking of disclosure (§ 28 IDG-BS). A new feature is the possibility of a complaint to the data protection officer (§ 28a nIDG-BS).
Terms and conditions (of use)	The terms and conditions of use of a website set a clear framework for the use of the website in general and/or certain contents or functions and, in particular, define which rights and obligations exist for the users.
Transparency	According to the principle of transparency, any data processing must be recognisable to the persons concerned - i.e. the person must be informed transparently who, how, for what and how long etc. processes the data. In addition, the public body must organise the handling of data in such a way that it can provide information quickly, comprehensively and factually (cf. § 4 para. 1 IDG-BS).