VISCHER

GLOSSAR PRIVACYSCORE.CH

Audit Trail	A data security measure in which all relevant steps that a user takes in a computer system (logins, changes, transfers, retrievals, etc.) are logged so that they can be checked on later. These logs should be regularly reviewed manually or automatically.
Processor	They are organisations (usually companies) that carry out data processing activities for and on behalf of a controller and, therefore, do not themselves decide on how this is to be done (i.e. they are bound by instructions). This includes, for example, many IT service and cloud providers. Under both the Swiss DPA and the GDPR, these organisations are referred to as "processor".
DPA	Der Vertrag ("Auftragsverarbeitungsvertrag", manchmal auch "ADV" oder "DPA" genannt), den ein Verantwortlicher mit seinem Auftragsbearbeiter abschliesst, um den datenschutzrechtlichen Anforderungen zu genügen. Er sieht u.a. vor, dass der Auftragsbearbeiter nur auf Weisungen des Verantwortlichen handelt, eine angemessene Datensicherheit sicherstellen und die Daten am Ende wieder löschen muss.
BCR	Binding Corporate Rules, a tool with which groups of companies can regulate the flow of data between the individual companies in compliance with data protection law in such a way that the data may be transferred also to countries without an adequate level of data protection. BCR are in essence group-wide data protection agreements to which all group companies are parties. However, most companies today instead rely on an IGDTA because it is easier to implement and does not require regulatory approval.
Processing principles	These are a number of basic rules that the FADP and the GDPR have laid down for the handling of personal data in accordance with data protection, such as namely the principle of transparency, purpose limitation, proportionality (including data minimisation and limitation of the retention period), data accuracy, data security, fairness of data processing or the principle of good faith, and the lawfulness of data processing.
Special categories of personal data, sensitive personal data	Under the Swiss DPA, these are personal data (i) on religious, ideological, political or trade union views or activities, (ii) on health, privacy or racial or ethnic origin, (iii) genetic data, (iv) biometric data that uniquely identifies a natural person, (v) on administrative and criminal prosecutions or sanctions, and (vi) on social assistance measures. Special requirements apply to them. Under the GDPR, the catalogue of these types of personal data is defined in a similar, but not identical manner: They are personal data revealing (i) racial and ethnic origin, (ii) political opinions, religious or philosophical beliefs, or trade union membership, (iii) genetic data, (iv) biometric data uniquely identifying a natural person, (v) health data, and (vi) data concerning a natural person's sex life or sexual orientation. For practical purposes, one should also include (vii) data on criminal convictions and offences and (viii) related security measures, because they are also regulated more strictly than "normal" personal data. Under the GDPR, if a controller wishes to use or otherwise process such special categories of personal data, additional conditions (such as the express consent of the data subject) apply.
Process	This refers to any dealing, use or handling of personal data, such as the collection, recording, organisation, arrangement, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The Swiss DPA and the GDPR define processing in the same manner.
Records of Processing Activities	The directory of processing activities, or Records of Processing Activities for short. Sometimes the term directory of processing activities is also used. It provides an overview of the individual data processing activities of a company. The FADP and the GDPR prescribe it in certain cases.

BYOD	Bring-you-own-device, the concept used by more and more companies that allow employees to make available and use their private devices for work purposes, e.g. by using their own mobile phone to check their business emails and access their office accounts.
CMP	Consent Management Platform, a software solution that allows companies to obtain from visitors of their websites the consent requirement to track them or to make use of cookies.
Cookies	Cookies is a technique that is used for many years and allows the operator of a website to have its server transmit a digital marker (the "cookie") with a unique number encoded into it to each visitor of the website. If the visitor returns to the website later on, the server can recognise the visitor by reading out the marker and the number contained therein. This allows the server to track the visitor. However, he will not necessary know who the visitor is. The tracking can serve analytical purposes or be used to determine the visitor's interests, which can then be used for more targeted advertising.
DLP	Data loss prevention, a data security measure to prevent unwanted "leakage" or "loss" of company data, e.g. by scanning e-mails to see if they contain business secrets or blocking (or detecting and recording) the use of USB sticks on computers so that employees or third parties cannot steal data.
DMZ	De-militarised zone, a technical term used in connection with firewalls. It describes a digital "forecourt" to a company network in which visitors can stay, but are not allowed inside the company network. If you set up a WLAN and want to make it available to guests, you can configure it in a manner so that the guests can use it but cannot access the rest of the company from there; they have to stay in the DMZ, so to speak, thus protecting the company network.
PN	The privacy notice or data protection statement, which describes what personal data a controller collects, what it does with it and how, and what rights the data subject has. The Swiss DPA and the GDPR require it in many cases.
DPIA	Data protection impact assessment, i.e. the documented assessment of whether a planned project regarding the processing of personal data may have undesirable negative consequences for the data subjects and what measures are taken against this. The Swiss DPA and the GDPR require a DPIA to be done in certain cases.
Swiss DPA	Swiss Data Protection Act, which regulates data protection for the private sector and federal bodies in Switzerland. There are also cantonal and communal data protection laws, but these only apply to public bodies in the cantons and communes.
GDPR	The EU and UK General Data Protection Regulation. It is the equivalent to the Swiss DPA and govern data protection in the EEA. The UK has already adopted the GDPR before the Brexit, and continues to rely on it.
EDR	Endpoint Detection & Reponse (or Extended Detection & Response), a data security measure in which a software is installed on all devices (e.g. notebook) that detects abnormal and therefore suspicious behaviour and raises an alarm or automatically blocks access or a device if a cyber attack or other misuse is suspected.
EU SCC	The Standard Contractual Clauses of the European Commission. This usually refers to the standard contract published and approved by the European Commission as contractual safeguards for transfers of personal data to countries that do not have an adequate level of data protection. The EU SCC can also be used under the Swiss DPA if the appropriate modifications are applied to them.
IGDTA	Intra-Group Data Transfer Agreement, an intra-group contract that regulates all flows of personal data within a group of companies in terms of data protection law.
ISMS	Information Security Management System, a structured approach in a company to properly define the measures to ensure information security, to ensure their implementation and to ensure that they are improved, replaced or supplemented as necessary. An ISMS consists of processes, directives, the assignment of responsibilities, risk assessments and documentation, among other things. An ISMS often follows

	a standard, such as ISO 27001, and in these cases can also be "certified" by a third party. The measures taken (TOMS) are the result, but not part of the ISMS. An ISMS allows a company to ensure an adequate level of data security.
MDM	Mobile Device Management, i.e. usually a software and process that is used to to manage mobile devices connected to the corporate network and to ensure their information security.
MFA, 2FA	Multi-factor authentication or two-factor authentication (2FA), refers to all procedures in which access authorisation is checked not only by a single password or other single secure "factor" (in addition to the user name), but by two or more of them, i.e. by a code transmitted by SMS, by a fingerprint or by using an authenticator app. This is an essential security measure. Without MFA, anyone who is able to steal a user's password can use it to gain access to their account, in the worst case without them noticing. Therefore, the use of MFA is an essential measure for securing data networks.
Personal data	All information that relates to a specific or identifiable individual. It must therefore be possible to identify the person to whom the data relates by reasonable means, whether directly (e.g., by name, a picture or a telephone number) or indirectly (e.g., by an internet search or combining several data sources). The term is defined in the same manner under both the Swiss DPA and the GDPR.
Profiling	Means a fully automated evaluation of a person by a computer, i.e. an automated value judgment (e.g., a prognosis, an assessment) concerning a characteristic (e.g., interest) or behaviour of an individual person based on their personal data.
ROPA	Records of Processing Activities, the inventory of all processing activities.
TIA	Transfer Impact Assessment, the documented analysis of whether, in the case of a transfer of personal data to a foreign country, the authorities in such country (e.g., police, intelligence authorities) could gain access to it and whether this could happen in a way that would be problematic according to European law. The Swiss DPA and the GDPR require that such an analysis is done in certain cases.
TOMS	Technical and organisational measures of security; this is the main term for all the measures an organization undertakes to ensure the security of personal data, both by taking technical steps (e.g., firewalls, encryption) and organizational measures (e.g., instructions, training, contracts). Each organization has its own set of TOMS.
Controller	The organization (usually a company) that essentially determines the purpose for which or how personal data is to be processed (e.g., categories of data, sources, recipients) and is, thus, responsible for compliance with data protection law in this regard. A particular data processing activity may have several controllers who together decide on the processing activity or on certain aspects of it.

March 11, 2023