VISCHER Privacy Score (for the private sector)

provided by **privacyscore.ch**

Template Version 15.5.2023 | ***English Content*** | *Questions, feedback, errors: dataprivacy@vischer.com*

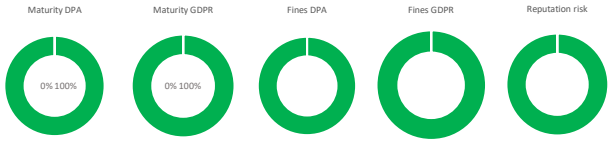
Scope: This tool allows any private sector company to easily assess the maturity of its data protection governance, whether the entire company or individual areas and departments. It does not replace the assessment by an expert. Nor does it check the data protection conformity of individual data processing activities. However, the questionnaire provides information on how well the company has the necessary processes, responsibilities, regulations and other measures in place to comply with the Swiss Data Protection Act (Swiss DPA) and the EU General Data Protection Regulation (GDPR). At the same time, the tool recommends which steps can be taken to additionally increase the maturity of the data protection governance. The resulting maturity score can be compared with those of other companies; the scores - including the VISCHER Privacy Score (this is only displayed if you have selected the "Privacy Score" program) - are calculated when the answers are recorded in step 3. Please note: All references to the Swiss DPA refer to the revised Swiss DPA, which will come into force on 1 September 2023. A glossary of terms used can be found at the bottom of the table. About the language: The questions and answers are available in both German and English. You can switch at the top. Once you have done so, you will need to redo your selections of the scope of the audit, the audit programme and the applicable data protection law. Any answers

Our Survival-Guide for the Swiss DPA for SME (free download)

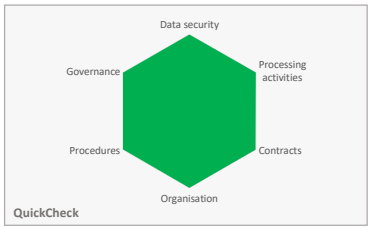
Step 1: The Organization		
Company:	GIT SA	
Seat (Place, Country):	Switzerland	
Industry sector (as per NACE):	J. INFORMATION AND COMMUNICATION	(Link to Eurostat NACE list)
Size of operation:	18172	(in number of employees, not FTE; the number has no relevance in the calculation of the score or the questions)
Locations, offices:	Geneva	

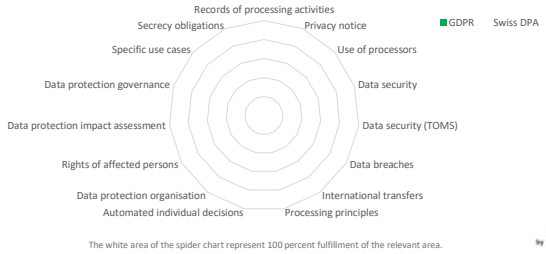
Step 2: The Audit Program		
Scope of audit:	Single Entity	(the scope will impact the available audit programs; therefore, it has to be chosen first)
Description:		
Inclusions, exclusions:		(state here what may be in or out of scope of your audit)
Audit program:	Assessment Small Enterprise (Quickcheck)	(the requirements in step 3 are chosen based on this; therefore, this must be chosen now and should not be changed anymore)
Data protection law:	Swiss DPA+GDPR	(the requirements in step 3 are chosen based on this; therefore, this must be chosen now and should not be changed anymore)
Assessor:	Mickaël Strazzeri	
Date of assessment:	11/09/2023	
Contact details:	it@git.ch	

Assessed: 100%



Here you can be find how these these assessments where calculated (i.e. which of the audited requirements received how many maturity or risk points)





The white area of the spider chart represent 100 percent fulfillment of the relevant area.

by VISCHER

The documents you should create, check or obtain:

Documents for training employees re data protection and information security (ET)

(This list will be automatically generated when completing step 3; the column "Documents" below will tell you which document is recommend for which requirement)

Step 3: Verification — **Time required to complete: 0 Min.**

Instructions: Please go through each of the requirements for each of the topics and select the appropriate answer in the "Status" column (if this form has been completed online, the appropriate answers have already been inserted). A recommendation will automatically be displayed if and what needs to be done to comply with the data protection requirement at issue. If necessary, have Excel automatically adjust the height of each line so that the entire text is visible (this has to be done manually). Furthermore, depending on the audit program chosen, the documents required for each requirement are shown; in this case, they are summarised above with the corresponding abbreviations. The two columns on the right indicate whether a requirement is necessary or not according to the Swiss DPA or the GDPR. At the end of each line, it is stated how many maturity points (max. 5) or risk points (max. 3) per requirement the response given by you contributes to the overall scores and assessments. Caution: If the subject of the scope, the audit programme or the applicable law or language is subsequently adjusted, the information already recorded will no longer match.

Please only select the answer that fits best

##	Topic	Requirement	Status		DPA	GDPR	Maturity DPA	Maturity GDPR	(not used)	Fines DPA	Fines GDPR	Reputation risk
1	**Governance**	For every data processing activity (i.e. every activity in the organisation where personal data is processed), there is someone who is responsible for data protection compliance. This should not be the person responsible for data protection in general.	Yes, we have.	Is this always clear and also documented in policy?	Good	Good	5	5	0	0	0	0
2		We have someone who takes care of data protection compliance. The person watches over those who are responsible for individual data processing activities (but is not responsible for them) and advises them.	Yes, we have.	-	Good	Good	5	5	0	0	0	0
3		We have someone we can contact with questions about data protection who will answer them for us.	Yes, we have someone internally.	-	Good	Good	5	5	0	0	0	0
4		We have someone who looks after information security with us and regularly maintains our IT systems and assesss them for security.	Yes, we have hired a specialist to do it.	-	Good	Good	5	5	0	0	0	0
5		We are subject to the GDPR and our business requires the processing of sensitive personal data or otherwise particularly delicate processing of personal data, which is why we have appointed a Data Protection Officer.	Yes, we have.	-	n/a	Must	5	5	0	0	0	0
6	**Processing activities**	We are aware of what is expected of us in terms of our handling of personal data. We are of the opinion that we do nothing that could be considered unfair or indecent against this background.	Yes, we can confirm that we do not do anything with personal data that could be critical in this respect.	Please note that what is legally compliant is not necessarily perceived as correct. Perceived data protection is just as important today. To do this, understand what expectations are specifically placed on your company.	Must	Must	5	5	0	0	0	0
7		We know how long we are allowed to keep which documents and data, regularly go through our filing and mailboxes and remove what we no longer need. This is especially true for sensitive personal data (such as personnel files).	Yes, we know that and we do.	-	Must	Must	5	5	0	0	0	0

8		We have a privacy notice on our website that describes what personal data we collect on a scheduled basis. Someone has assessed that it contains the necessary information. We keep it up to date.	Yes, that is true.	-			Must	Must	5	5	0	0	0	0
9		We only collect personal data that we really need and for which we have a good business reason; we do not collect personal data on a stock basis.	Yes, we pay attention to data minimization and only ask for the personal data that we really need for our business.	-			Must	Must	5	5	0	0	0	0
10		If we want to repurpose existing personal data for something new (e.g. for sending a newsletter or a new project), we tell the affected persons in advance or clarify whether this would also be permitted without informing them (e.g. internal evaluation that has nothing to do with the affected persons).	Yes, that's what we do or will do.	-			Must	Must	5	5	0	0	0	0
11		We all know that non-public personal data about employees, customers and other persons must be treated confidentially. Internally, too, we apply the need-to-know principle and sensitive documents (e.g. personnel files) are locked away or sensitive electronic data are protected by restricted access rights.	Yes.	-			Must	Must	5	5	0	0	0	0
12		If we notice that personal data we have used is incorrect or incomplete, we correct it; if we are not sure, we write it down.	Yes.	-			Must	Must	5	5	0	0	0	0
13		Our staff know that they should not write anything down in our computer applications and other records, which would be embarrassing if we had to show it to people.	Yes.	-			Must	Must	5	5	0	0	0	0
14		We only send electronic promotional mailings to existing customers or people who have requested it. You can unsubscribe at any time.	Yes, we stick to that.	Good! Here is a checklist for your information: https://bit.ly/3ZaeP5j			Must	Must	5	5	0	0	0	0
15		There is no tracking on our website and third parties do not collect any personal data about our users on it, or the users have given their legally compliant consent.	Yes, that is so.	Good! Here is a checklist for your information: https://bit.ly/3YaDfub			Good	Must	5	5	0	0	0	0
16	**Data security**	We have activated all security functions on our computers, including anti-malware scanner, browser protection and firewall.	Yes.	-			Must	Must	5	5	0	0	0	0
17		Our notebooks are set up so that all information on them is encrypted.	Yes.	-			Must	Must	5	5	0	0	0	0
18		We have configured our computers and other devices to update themselves automatically.	Yes.	-			Must	Must	5	5	0	0	0	0
19		All our programmes and computers with personal data can only be used by our employees with a personal password.	Yes.	-			Must	Must	5	5	0	0	0	0
20		For external access, we have activated multi-factor authentication (MFA) as far as possible.	Yes.	Note: For administrator accounts, you should also activate the MFA for internal access.			Must	Must	5	5	0	0	0	0
21		We regularly back up our personal data and other important information and keep it separate from our computers.	Yes.	If you make a backup in the cloud: Make sure that this is also separated from the computer so that it is not affected by a ransomware attack. The attackers usually also try to destroy the backups.			Must	Must	5	5	0	0	0	0
22		When we dispose of documents, computers or other data carriers containing personal data, we don't just do it in the trash or recycling, we do it securely.	Yes, we take care of that.	-			Must	Must	5	5	0	0	0	0
23	**Contracts**	We have data processing agreements (DPAs) with our service providers if they store or do anything with personal data for us.	Yes, we have.	-			Must	Must	5	5	0	0	0	0
24		Where possible, we have selected service providers within the EEA, UK or Switzerland (rather than those in the US or other countries). Where possible, we also store the data in Europe.	Yes, that is how we proceed.	-			Must	Must	5	5	0	0	0	0
25		If we give or otherwise make personal data available to someone outside the EEA and the UK, we enter into the EU Standard Contractual Clauses (EU SCC) with them or ask a specialist.	Yes, that is how we proceed.	Have you assessed all contracts to see if they already contain the EU SCC of 2021 or later? If not, do so now. The earlier EU SCCs are no longer valid.			Must	Must	5	5	0	0	0	0
26		If we carry out joint processing of personal data with someone, we agree who is responsible for what and record this in writing.	Yes, that is how we proceed.	-			Good	Must	5	5	0	0	0	0
27	**Procedures**	In our company, everyone knows that they must report breaches of data security immediately, i.e. if personal data has been lost, if there has been manipulation of such personal data or if such data has been disclosed to people who are none of their business.	Yes.	-			Must	Must	5	5	0	0	0	0
28		If there is a data breach, we know whether and how to report it or have someone who can help us immediately.	Yes, that is so.	-			Must	Must	5	5	0	0	0	0
29		No one creates a new collection of personal data, feeds personal data into a new software or service, or otherwise starts a new data processing operation without our prior data protection review and and have designated a person who, as owner, is responsible for compliance with data protection.	Yes, that's how it works.	-			Must	Must	5	5	0	0	0	0
30		If we are planning a potentially particularly sensitive data processing operation (e.g. surveillance, processing of a lot of sensitive personal data), we carry out a data protection impact assessment (DPIA).	Yes, we do that.	-			Must	Must	5	5	0	0	0	0
31		If someone asks us about their own personal data (e.g. for information or deletion), we immediately give it to someone who knows what to do with it.	Yes, that's how it works.	-			Must	Must	5	5	0	0	0	0
32		Our board of directors and our management have basic knowledge of data protection and are regularly informed about where we stand in terms of data protection, make the necessary specifications and intervene if things are not going right.	Yes, that's how it works.	-			Must	Must	5	5	0	0	0	0
33	**Organisation**	We know which personal data we process at which points in our company.	Yes, we even recorded that.	-			Must	Must	5	5	0	0	0	0
34		We have instructed our employees on data protection. This also includes confidentiality.	Yes, there is a directive and we have also carried out training.	-			Must	Must	5	5	0	0	0	0
35		We all regularly raise our awareness in the area of information security (e.g. with learning videos).	Yes, we do.	-	ET		Good	Good	5	5	0	0	0	0
36		We have created a record of our personal data processing activities. We keep it up to date.	We are only subject to the Swiss DPA, have fewer than 250 employees and do not have a lot of particularly sensitive personal data, nor do we engage in high-risk profiling.	You do not need a processing register under these conditions.			Must	Must	5	5	0	0	0	0
37		We try to set all IT applications that we have or offer ourselves to be as data protection-friendly as possible by default.	Yes, we pay attention to that.	-			Must	Must	5	5	0	0	0	0
38		In all data collections, we make sure that we can delete the personal data we record in them if this should be requested.	Yes, we pay attention to that.	-			Must	Must	5	5	0	0	0	0

39		We ensure that we do not make unnecessary copies of files and other data collections containing personal data.	Yes, we pay attention to that.		-			Good	Good	5	5	0	0	0	0
40		If a data breach occurs, we document it.	Yes, that's what we do.		-			n/a	Good	0	5	0	0	0	0

Glossary (the abbreviations of the recommended documents can be found at the top of the dashboard before step 3):

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	The contract ("data processing agreement", sometimes also called "data processing addendum") that a controller enters into with its processor in order to comply with data protection law requirements. Among other things, it stipulates that the processor must only act on the documented instructions of the controller, ensure an adequate level of data security, have subprocessors approved and delete the data at the end.
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 a data protection compliant manner, 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, the following 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 ask visitors to their websites for their consent to being tracked or to the use of cookies.
Cookies	Cookies is a technique that has been 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 for 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 affected person has. The Swiss DPA and the GDPR require one 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 affected persons and what measures are to be taken against this. The Swiss DPA and the GDPR require a DPIA to be done in certain cases.
Swiss DPA	Swiss Data Protection Act, 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 communities.
GDPR	The EU and UK General Data Protection Regulation is the equivalent to the Swiss DPA and govern data protection in the EEA. The UK had already adopted the GDPR before the Brexit, and continues to rely on it.
EDR, XDR	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 made 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, their implementation and 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.

Maturity (5=max.):

0	1	2	3	4	5

Risk (3=max.):

0	1	2	3

The VISCHER Privacy Score was written by David Rosenthal (drosenthal@vischer.com) with the help of David Koelliker and Lucian Hunger as well as Alessandro Loperfido-Lawrence. Many thanks to everyone else for their support and feedback.