revDPA – what to do.

for SMEs

Completed: ☑

New as of 01.09.2023

7 Ten commandments for handling personal data under the DPA[1]

1. We **tell** persons in advance what we do with their data and why.
2. We **stick to this** and do not use data for purposes not intended.
3. We practice **data minimization** and "need-to-know".
4. We **delete** data as soon as we no longer need it.
5. We allow people to say **"no"** to us processing their data.
6. We only do what we would find **acceptable** for ourselves.
7. We validate our data for problematic **errors** and omissions.
8. We do not pass along **sensitive data**[2] for purposes of others.
9. We take measures to ensure the data is **secure** with us.
10. We obtain data only **legally** and in particular from legal sources.

Exceptions are possible (only) for overriding reasons. We design any data processing according to these principles!

2 Privacy notice

Any planned processing of personal data that is not required by law is included in a privacy notice created by us. We refer people to the notice (in T&Cs, apps, on forms etc.). It is on our website.

Mandatory content: Who we are (with contact details), the data and the purpose for which it is collected, who we give it to (names not required) and the countries or regions concerned (incl. what we legally rely on[3]).

1 Inventory of processing

We keep an inventory of our activities with which we process personal data (e.g., customer data admin, accounting, online shop, HR admin). It contains the information as listed in Art. 12 revDPA, incl. the processing purposes, categories of persons, data and recipients, and retention periods.[4] This **duty only applies** if we have 250+ employees (headcount) or process sensitive data[2] on a large scale or engage in high-risk profiling.

3 Data processors under control

If we entrust the processing of our data to an IT provider or anyone else, we enter into a "DPA", i.e. a **contract** that allows us to manage and control the company and to approve (or object to) the use of third parties in advance. It also sets out the **security measures** (so-called TOMS). We check these (incl. audit reports, if needed). A DPA in line with Art. 28 GDPR is fine if it also refers to the Swiss DPA. The processor may only do what we are allowed to do (e.g., usually no processing for own purposes). We check any current/new DPA for compliance.

5 When data goes abroad

Problem-free: EEA, UK, adequate countries[5]

All **other states** *inter alia* permitted if:

- Export necessary for the performance of a contract with or for the data subject
- Explicit waiver (data protection is given up)
- Conclusion of the EU "Standard Contractual Clauses"[6] with CH adaptations and no reason to believe that there will be problematic access by authorities (→ carry out a TIA[6,7]).

We check our contracts for this!

6 We grant data subjects their rights

We correctly **identify** the requestor in advance.

We provide a person with **their own personal data** (not documents) and, upon request, certain other information (usually free of charge within 30 days). We avoid giving the impression that all data has been provided by us (as false or incomplete information is punishable). Our first response may be limited to the data usually sought by data subjects. The person must help us in identifying further data. Non-privacy motivated requests are not protected. We protect third party data and our own business secrets.

Any person may request **correction** of their data. If the truth is in dispute, this will be recorded.

Any person can request **deletion** of their data or otherwise want us to stop or change our processing. We can continue if we have an overriding reason to do so.

If a **computer** makes discretionary decisions with significant negative consequences, we tell the people affected and offer human intervention.

Sometimes, we must allow people to **take with them** the data they provided to us during our engagement (so they can use it somewhere else).

We make sure we can fulfill this!

10 Data protection impact assessment (DPIA)

In the case of projects that could be **risky** for data subjects in terms of data processing, we carry out a DPIA. In it, we document the project and the measures to protect the data subjects and check if there is still a high risk of undesirable **negative consequences** for them (if so: seek advice). We keep the DPIA.

8 Privacy by default

Where we have privacy **settings** in apps, on websites, etc., they are **preset** to the **minimum**. All our developers ensure that this is the case.

9 Small professional secrecy

Indicates that willful violation is punishable (up to CHF 250k, upon a complaint)

We keep secret personal data **entrusted** to us that is needed by us for our job or we make it clear in advance that we will not keep it secret.

4 The data is secure, otherwise we report

Technical: Access only "need-to-know" and with personal account, "MFA" where there is external access, audit trails (may be mandatory for sensitive data[2], retain 1 year), pseudonymisation, firewalls, anti-malware software, backups (also offline).

Organisational: Instructions (e.g., use this sheet for this purpose), training, checking the logs, if there is a lot of sensitive data[2], check your measures and create a processing policy.

Duty to report: If confidentiality, integrity or availability of personal data is breached *and* there is a high risk of negative consequences for individuals (not merely a nuisance), then report it to the FDPIC (https://edoeb.admin.ch provides a form) and document it for 2 years; if individuals can protect themselves from consequences, then report it to them as well.

Everyone is responsibile for security!

7 We do not rely on consent

As a matter of principle, we do not rely on consent. If we do, it must be **informed** and **voluntary**. In the case of sensitive data[2] and high-risk profiling it must be explicit.

We have somebody that knows what to do when … (6 7 10 4)

… a person wants to see/obtain their data or have it deleted or corrected or they otherwise have a data protection concern relating to their data:

… we have a new/changed project that concerns data of individuals and, thus, has to be checked for data protection compliance (if needed with a DPIA):

… personal data is lost, falls into the wrong hands, has been tampered with, this may have happened or if there are other security issues:

Each of us reports such incidents to this person immediately!

[1] revDPA: https://datenrecht.ch/gesetzestexte/ndsg-en/
[2] Sensitive personal data: Art. 5(c) revDPA
[3] See privacy notice template: https://dsat.ch
[4] Templates: https://dsat.ch, https://bit.ly/3qrpOIb (DE)
[5] See Appendix I of the DPO (https://bit.ly/3DmSbPm)
[6] See FAQ (with sources): https://bit.ly/3MIb1TE
[7] See TIA: https://bit.ly/3L3mxYO (with ref. to FAQ)

Questions? (FAQ at https://bit.ly/3EOsiIL and more at https://bit.ly/3RCmuFQ)

Internal:

External: (may incur charges)

Key: Handling data | Governance | Data subject's rights | Process | 4 Prio implementation | ☐ Completed Y/N

Criminal sanctions

The revDPA is stricter than the GDPR or requires other, incompatible procedures.

Version 13.9.2022 – Updates: www.rosenthal.ch

Author: David Rosenthal, drosenthal@vischer.com

by VISCHER