SWITZERLAND GLOBAL ENTERPRISE

GDPR – Information Sheet

Background

The European General Data Protection Regulation (GDPR) entered into force on 25 May 2018. Although the GDPR is a European regulation, it also applies to Swiss companies under certain conditions.

The Swiss Data Protection Act (CH-DSG) is also currently under revision and will be brought into line with European law. The CH-DSG is not expected to enter into force until 2019 at the earliest.

This information sheet provides an overview of the applicability of the GDPR to Swiss companies and the need for action. The information sheet is intended as a working aid and does not claim to be exhaustive. It is always necessary to conduct an individual analysis of the company in question.

To whom does the GDPR apply?

The GDPR applies to **any handling of personal data** (including acquisition, storage, deletion, anonymization, transfer, etc.; in short "processing") by Swiss companies, if the company

- **has a regional office in the EU**, such as a branch office, agency, local representative office or subsidiary, provided the latter does not act independently but on behalf of the Swiss parent company, and processes personal data in connection with the regional office (example: a branch in France sells products or services for the head office in Switzerland and uses the name and address of end customers or the buyer's contacts from France);
- **is not established in the EU**: if the company offers goods or services in the EU (example: a company in Switzerland actively distributes goods or services to Germany via a website or a Software as a Service (SaaS) provider in Switzerland has customers in the EU) or observes the behavior of persons in the EU (example: cookies are used on the company's website in Switzerland by means of which one can draw conclusions about the behavior of the website visitors and this data is evaluated).

Which data protection principles must be observed in accordance with the GDPR?

The following data protection principles must be observed and adhered to in all data processing:

- **Principle of lawfulness:**
  Personal data may only be processed lawfully and fairly (including law, contract, consent, legitimate interest).

- **Principle of purpose:**
  Personal data must only be collected for specified, explicit and legitimate purposes and must not be further processed in a way that is incompatible with those purposes.

- **Principle of transparency:**
  The collection of personal data and in particular the purpose of its processing must be identifiable to the data subject. The processor must actively provide information about the processing of personal data. Data subjects have a right to information.

- **Principle of data accuracy:**
  Anyone who processes personal data must ensure that it is factually correct and up-to-date on an ongoing basis.

- **Principle of data minimization and storage limitation:**
  Processing must be appropriate and limited to the extent necessary for the processing purpose.
  The storage duration must be defined so that data is only kept as long as is necessary for the processing purpose (implementation of archiving and deletion processes).

- **Integrity and confidentiality:**
  Personal data must be processed in a manner that ensures adequate security of the personal data (including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by means of appropriate technical and organizational measures).

- **Accountability:**
  The data processor is responsible for ensuring that the above principles are adhered to and must be able to demonstrate this accordingly.

What organizational and operational measures must be taken?

Swiss companies that are subject to the GDPR but do not have a regional European office must appoint a local representative in one of the countries concerned[1]. Under certain conditions[2] , a data protection officer must also be appointed.
Companies subject to the GDPR must meet numerous requirements. First and foremost, it must be ensured that the following (not exhaustive) requirements are met using guidelines, templates and other documentation:

- actions to implement the requirements must be organized and documented (e.g. data protection organization, preparation of data protection regulations and directives, training of employees);
- companies that process personal data are responsible for compliance with the processing principles (accountability) and must maintain a register of processing activities[3];
- data subjects must be informed of predetermined points before the processing of their data begins (in particular information by means of a Privacy Policy);
- the storage period of personal data must be determined in advance and data must be deleted when the purpose of the processing ceases to apply, the retention period has expired and , under certain circumstances and subject to retention obligations, also at the data subject's request ;
- in the event of a data breach, the controller must inform the competent data protection authority without delay and no later than 72 hours after becoming aware of the breach, if the breach poses a risk to the rights and freedoms of data subjects. If there is a high risk, the data subject must also be informed;
- a data protection impact assessment must be carried out prior to risky data processing;
- data subjects have various rights with regard to their personal data (e.g. right of access or deletion), which must normally be fulfilled within one month – this requires corresponding internal processes;
- written data processing agreements must be concluded with service providers that process personal data;

[1] Exceptions to this provision are listed in Art. 27 (2) GDPR.
[2] See Art. 37 GDPR.
[3] There are exceptions to this provision for companies with less than 250 employees, Art. 30 (5) GDPR.

- before transferring personal data to countries outside Europe/EEA or Switzerland, it must be ensured that the country in question has an adequate level of protection. If this is not the case, appropriate measures must be taken (e.g. conclusion of data protection contracts).

What are the consequences of non-compliance?

An infringement of the GDPR could have the following consequences:

- European authorities can impose fines of up to 20 million euro or – if higher – four percent of the guilty company's worldwide annual turnover.
- Contracts often require compliance with applicable law in general or data protection law in particular. In such cases, an infringement can lead to contractual penalties, premature termination, claims for damages and the loss of rights.
- In today's world, infringements can spread very quickly, especially for companies that are well known, handle sensitive data, have violated regulations before or operate in exposed areas. Correspondingly, this poses a reputational risk.

GDPR – Information Sheet 2: S-GE measures – new provisions

Handling data from business cards:

Handling the delivery of business cards:

- when delivered in a collection box (at trade fair/event in EU)
- when delivered directly to the company (given directly to a person)

Note on handling data from business cards:

Data from business cards is personal data. This must be processed lawfully. Processing is lawful in particular if it is based on law, consent or a justified reason (such as the data processor's legitimate interest).

On the one hand, in the context of the processing of personal data from business cards, no established practice has been developed yet, and on the other hand, it always depends on the circumstances of the individual case.

In principle, however, in most cases it can be assumed that the company (recipient of the business cards at trade fairs) can assert a legitimate interest in data processing, and that it does not lie outside trade fair participants' expectations for their business cards to be used by the companies to whom they have distributed them at a trade fair.

Issuing information (either upon receipt of the business card, e.g. on the lead sheet, or on first contact with the relevant person) is therefore sufficient; explicit consent is usually not required. The information could read as follows:

> *We hereby inform you that [company name/business card recipient] stores your personal data in its system on the basis of the received business card. The data is limited to your name, position, email address and telephone number.*
>
> *The data will be stored so that we can stay in contact with you and keep you informed about the latest news. Please let us know if you do not wish to receive any information, invitations or newsletters from us.*
>
> *We will not pass on your data to third parties.*

Consent would have to be obtained for any further use (such as passing on data to third parties). Consent is only valid if it is based on comprehensive information tailored to the specific case. Therefore, a review in each individual case is recommended.

In the event that the data is passed on to third parties, the consent could read as follows. The consent would have to be ticked by the owner of the business card to indicate agreement (either on the lead sheet incl. signature or during initial contact – in any case, however, before the transfer to third parties):

☐ *I agree that [name of company/business card recipient] may pass on my personal data (name, position, email address, address and telephone number) to third parties for marketing purposes in the areas of [please list].*

You can revoke your consent to the above declaration at any time and request the deletion of your personal data. Please contact us at [email address].

What questions should a Swiss SME ask itself?

- **Does a Swiss SME require a data protection officer?**

  According to Art. 37 GDPR, a data protection officer must be appointed if

  a) the **company's core activity** is to carry out processing operations which, by their nature, scope and/or purposes, require extensive **regular and systematic supervision of** data subjects, or
  b) the **company's core activity** is **processing of large amounts of specific data categories** (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data that clearly identifies a natural person, health data or data relating to sex life or sexual orientation of a natural person**)** or personal data relating to criminal convictions and offenses.

  The criteria for assessing whether a data protection officer should be appointed are not clear and require an analysis of an SME's actual activities and related data processing activities.

- **What other requirements must be met for a Swiss SME to avoid sanctions?**

  This question cannot be answered in general since the scope of data protection measures depends on the individual processing of personal data. It is therefore necessary to consider each individual case in each company.

  In any case, you should consider the following data protection requirements:

  - Take note of the following data protection principles when processing data:
    - ✓ Principle of legality and fairness
    - ✓ Principle of purpose:
    - ✓ Principle of transparency:
    - ✓ Principle of data accuracy:
    - ✓ Principle of data minimization and storage limitation
    - ✓ Principle of integrity and confidentiality
    - ✓ Principle of accountability

- Ensure good governance
  - ✓ You need to be familiar with your internal processes and maintain order in data processing so that you can fulfill your obligations to provide information at any time
  - ✓ Work closely with your IT department
  - ✓ Grant access permissions and restrictions
  - ✓ Train your employees and draw up internal instructions
  - ✓ Define responsibilities related to data protection

- Draw up a Privacy Policy
- Check whether you need to appoint a representative in the EU according to Art. 27 GDPR
- Make sure that in the event of a breach of data protection law you are able to observe the 72-hour deadline for reporting to the supervisory authority
- Prepare records of processing activities in accordance with Art. 30 GDPR
- Take the necessary technical and organizational measures designed to comply with data protection principles (privacy by design/privacy by default).
- Check whether you are obliged to appoint a data protection officer.

If you have any further questions, please consult www.s-ge-com/de/exporthelp, contact us directly at exporthelp@s-ge.com or give us call at 0844 811 812.