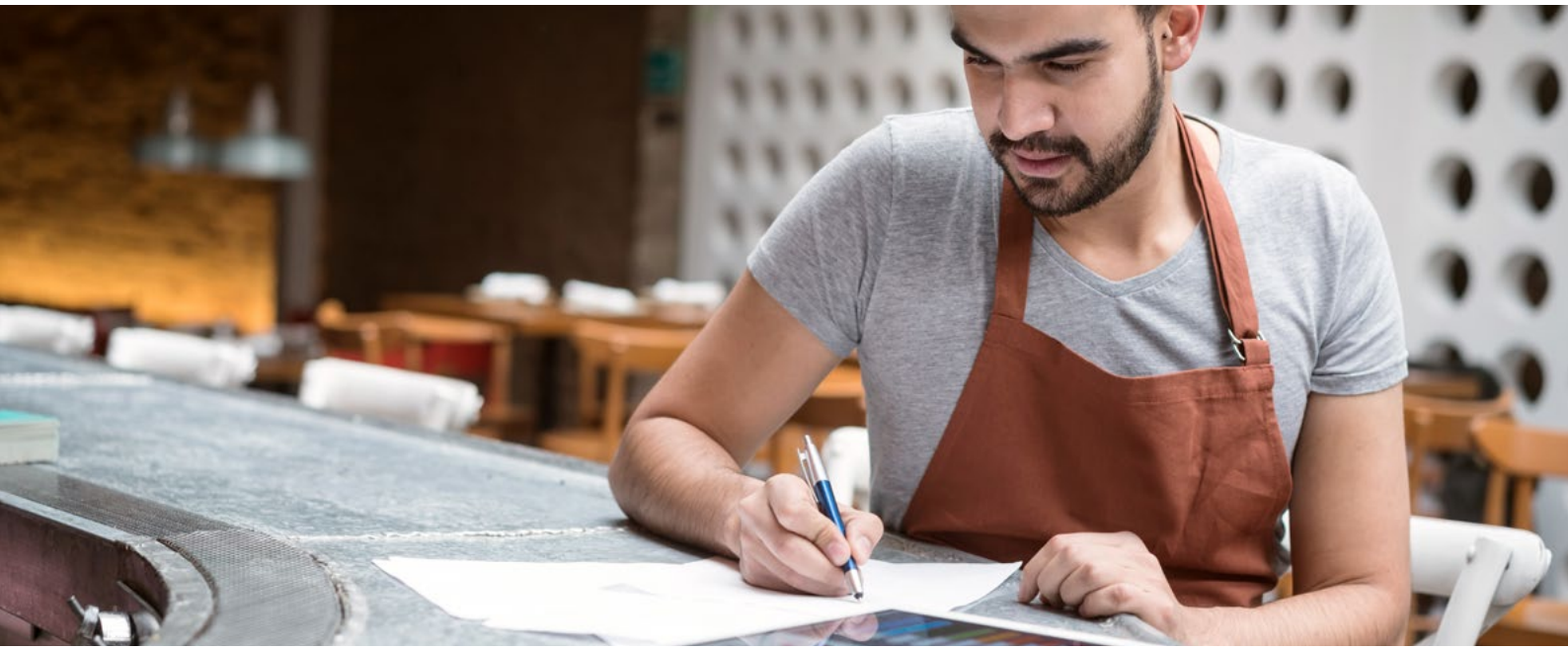
Developments in data protection law

In addition to the goal of harmonising data protection, the EU General Data Protection Regulation (GDPR), directly applicable in the EU since 25 May 2018, is to serve to introduce a standard of data protection in the EU that meets state-of-the-art requirements of the internet age. As an EEA Member State, **Liechtenstein** adopted the GDPR in July 2018. In this connection the Liechtenstein Data Protection Act was revised and entered into force on 1 January 2019. The **Swiss** Data Protection Act is currently also being revised, and generally reflects the main thrust of the GDPR. It is not anticipated to be enacted until 2020.



What are the main points of emphasis of the GDPR?
Essentially, as a result in particular of corporate accountability, increased supervision and a greater threat of penalties, (more) consistent implementation is anticipated. The main cornerstones of the GDPR are as follows:

- Directly binding within the EU, although adjustments (flexibility clauses) to country-specific circumstances are possible
- Mandatory, continuous documentation obligations
- Greater powers for supervisory authorities
- Mandatory reporting of data protection incidents, if at all possible within 72 hours
- Rights of persons affected, including right to the deletion of data and right to complain to supervisory authorities
- Obligation for certain companies to appoint data protection officers or nominate a representative in the EU
- Non-compliance carries the threat of high penalties (fines up to EUR 20 million or up to 4% of the previous year's global turnover)

Are you affected?

As a result of the adoption of the GDPR within the EEA, the GDPR is directly applicable for all companies in **Liechtenstein**.

Although the GDPR applies within the EU, in no way are all Swiss companies excluded from its scope. The reason for this is the so-called extraterritorial scope of the GDPR. In general terms, the GDPR applies to Swiss enterprises offering goods or services to people within the EU, even if they do not have an establishment in the EU. The same applies in the event that Swiss enterprises observe the behaviour of people within the EU and process data in this connection or evaluate the user behaviour of people within the EU while they are on the internet (profiling).

What should you do?

The requirements defined by the GDPR affect all areas of an enterprise. Necessary measures must be implemented particularly in the core areas of legal, organization, process and IP:

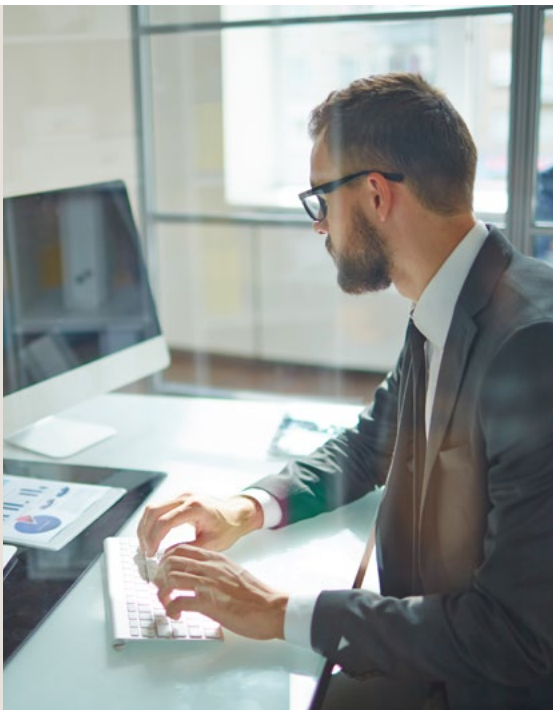
- **Legal**
  Data protection provisions cover all internal business areas. This creates many interfaces which must be included in a net of controls:
  - The processing methods of their data must be explained to visitors to your company's website in like manner to your company's employees.
  - Standard contracts are to be checked as, for example, your company's own general conditions of business, confidentiality obligations, and contracts with suppliers and service providers (in the latter case, particularly if they are to be classified as order processors).
  - It is also essential that data protection to be taken into consideration in your corporate culture and in the awareness of employees, and that appropriate in-house guidelines exist. Data protection is from now on a standard compliance topic. One element amongst others is an awareness of internal and external possibilities of access to the personal data processed by your company.
  - Another essential feature is a conscious approach to transborder data transmissions.
- **Organization**
  An essential part of data protection in your enterprise is the data protection organization in conjunction with a data protection management system (DPMS). These elements enable roles, tasks and powers to be defined and the areas of legal, organization, process and IT to be transparently mapped and managed.
- **Process**
  By introducing data protection processes, a system is put in place to recurrently monitor compliance with data protection. In case of any deviations, predefined measures are implemented to meet requirements. If monitoring reveals potential for improvement, this should be addressed.
- **IT**
  Responsibility for general data protection is assumed centrally by IT. All the users of the system are centrally managed. In addition, documented, technical (and organizational) minimum standards relating to the company's own technical infrastructure create trust.

Outlook

On the issue of data protection, one tends to start considering technical IT solutions. However, experience has shown that in order to implement the GDPR, around 90% of the work is of a legal, organization and procedural kind, and not of a technical nature. The time spent on this issue is often considerable and should not be underestimated.

Companies should also be aware that data protection is a recurrent topic and requires ongoing activity. Auditing, maintenance and adaptation of implemented processes is a long-term project.

Liechtenstein companies which have not yet considered the GDPR are urgently recommended to attend to this issue as soon as possible. The same applies to **Swiss** companies which are already affected by the scope of the GDPR. Irrespective of the ongoing revision of the Swiss Data Protection Act, all other Swiss companies would be well advised to now seriously consider the implementation.



Contact

Olivier F. Künzler
Partner
Head of Legal Services
Grant Thornton AG
T +41 43 960 71 71
E olivier.kuenzler@ch.gt.com

Grant Thornton