treureva

ARE YOU READY FOR THE NEW DATA PROTECTION ACT?

The new Data Protection Act and Data Protection Ordinance came into effect on 1 September 2023. There is no transition period. Read on to discover what the law means for you and the action you must take in your company.

First and foremost: the new Data Protection Act applies to all of us, whether a private individual, a one-man operation, an SME or a multi-national conglomerate. It applies to a Jass club just as much as to Swiss federal agencies. It also applies to all sectors and any person or organisation failing to comply with the legislation now runs the risk of huge fines.

The new Federal Data Protection Act (FADP) with its implementing ordinances governs all aspects of the processing of personal data by private individuals, companies and federal agencies. The term „personal data" refers to all data relating to an identified or identifiable natural person. As before, the term „processing" has a broad meaning and, among other things, includes the collection, processing, saving, storage, adaptation or alteration, dissemination, use, archiving, erasure or destruction of data.

In particular, the new Data Protection Act improves the transparency of all types of data processing and significantly strengthens the position of data subjects in respect of their own data. The data protection legislation imposes a large number of (new) obligations on the data controller. We give a list below of the most important changes and the controller's obligations:

Information obligations and data privacy statement

Data subjects must be informed about the extent and purpose of data processing. This usually takes the form of what is called a „data privacy statement". This informs data subjects about which personal data is processed for which purposes, the party or parties to whom the data is transmitted, whether and which data is obtained from third parties, and whether data is sent outside the borders of Switzerland. The data privacy statement can, for example, be posted on a company's website or made available to data subjects by other methods. Although it does not have to be attached to every written communication, such documents should at least make reference to the relevant website. Please note that the new FADP contains additional obligations to provide information. This means that you must check your privacy statements and amend them if necessary. *We will support you in this process and update your privacy statement for you.*

Data privacy / IT infrastructure

Only the persons who actually need the data for processing should have access to this personal data. In this regard, internal guidelines on data processing must be prepared or amended and processes defined. *We would be pleased to assist you in the preparation of these guidelines.*

Technical (e.g. encryption and/or firewalls) and organisational (e.g. IT directives/training courses) measures must be adopted to protect personal data.

Protection against claims and costs (insurance)

Companies will in future be subject to a large number of extended duties of care. If these are breached, protection in the form of suitable insurance policies tailored to meet the new circumstances will quickly gain in importance. *We strongly recommend that you ask your insurance advisor/broker to review the following insurance policies.*

---

1. Your business and professional liability insurance

In most cases, pure financial loss arising from breaches of data protection obligations and the costs of regulatory assessment procedures can now be easily included in the insurance cover.

2. Directors' and officers' liability

The data controller should be mentioned in the policy as a co-insured person.

3. Legal expenses insurance

Comprehensive insurance extends across all possible disciplines such as criminal, administrative and data pro-

criminal, administrative and data protection proceedings as well as investigations, etc. The involvement of public authorities can have extensive cost implications.

4. Cyber insurance

Data privacy and data security are inseparable today. Fines and penalties can be partially imposed on the insurer. Cyber insurance as the ultimate insurance deserves special consideration.

Contracts with service-providers

You probably use service providers for certain parts of your operations (e.g. IT support, accounting software, distribution of newsletters, etc.). It is possible to outsource data processing to order processors under specific conditions. *As the controller, do you already have order processing contracts with third party providers? We would be happy to review and update these. Alternatively we would be pleased to assist you in the drafting of these contracts.*

Reporting in the event of breaches of data privacy

A breach of data privacy occurs if personal data is inadvertently or unlawfully lost, erased, destroyed and altered or if the data is disclosed or made accessible to unauthorised persons. If the breaches are likely to pose a serious risk to the personal or basic rights of the data subject, this must be reported to the Federal Data Protection and Information Commissioner (FDPIC). Data subjects must also be informed if this is necessary for their protection. *We will support you in these processes and, if requested, provide you with a template for your submission to the FDPIC.*

Rights of the data subject

Data subjects whose personal data is processed have the right to receive information about their own data. The FADP grants them the right to receive information from data processors. Information of this nature must be provided free of charge within 30 days. Data subjects also have the right to have incorrect data rectified or to request the erasure of their data. However, the data subject's right to information is not absolute. Thus in statutory exceptional cases (e.g. legal proceedings) there is no obligation to comply with the request for information. *In specific cases we would be pleased to advise you whether it is actually necessary to respond to a request.*

Processing log

Companies with more than 250 employees or companies which process large volumes of sensitive personal data or which undertake high-risk "profiling" are placed under a mandatory obligation to maintain a data processing log.

Article 5 nFADP, para. c1-6 classifies the following data as sensitive personal data:

---

1. Data on religious, ideological, political or trade-union views or activities,
2. Data on health, private life or racial or ethnic origin,
3. Genetic data,
4. Biometric data that unambiguously identifies a natural person,
5. Data on administrative and criminal prosecutions or sanctions,
6. Data on social assistance measures

We recommend that companies maintain a data processing log even if they are not subject to a mandatory obligation to compile such a log. In smaller scale situations it is at least sensible to maintain a data inventory. A log or inventory provides an enhanced and centralised representation of the data processing, increases transparency of the processed data and creates an overview. Among other benefits, they assist in the identification of data breaches. *Contact us for detailed information and a summary of the essential questions when establishing a log or inventory.*

Transmission abroad

Most international cloud and software providers have servers outside Switzerland or servers that can be accessed from abroad. The major international players, in particular, also make storage facilities available in Switzerland. However, storage facilities of this nature must often be pro-actively requested. If data is to be transmitted abroad, the country must have an equivalent level of data protection (which is the case in the EU but not in the USA) or additional measures must be undertaken to guarantee data security. Transmission not only includes actively sending the data, but also remote access.

When data is transmitted to the USA, adequate data protection can be guaranteed by standard contractual clauses as well as by other and/or supplementary security measures. In such cases please take care that you make reference to standard contractual clauses and that these are contained in your General Terms and Conditions of Business or in the order processing contract. If this is not the case, you must ensure that these clauses are incorporated. *We would be pleased to support you in this matter also.*

Data privacy impact assessment

All companies which process personal data must identify and assess the associated risks. Companies can in principle undertake a simple risk assessment for this purpose. When planning new data processing activities which could potentially involve a serious risk for data subjects, the data controller must assess and document the risks as part of a formalised data privacy impact assessment. Serious risks arise in particular when using new technologies or from the nature, extent, circumstances and purpose of the processing (for example if large volumes of sensitive personal data are processed or if artificial intelligence is used). The data privacy impact assessment contains a description of the intended processing, an assessment of the risks to the personal or basic rights of the data subjects as well as measures to protect their personal and basic rights. *Do you need help? Contact us.*

Data controller and contact

Nominating a person to take care of data privacy in the company, organisation or even in a club is recommended. This data controller would have to acquire a basic knowledge of data privacy legislation and serve as the contact person in the organisation for questions about data privacy. This person can acquire this knowledge from public sources or training courses and can also call on external support. *We would be pleased to support you in this matter too.*

Erasure of data

Personal data may only be processed for as long as is necessary to perform the service, guarantee the contractual and statutory retention periods or safeguard overriding business interests (e.g. to safeguard legal claims). Data that is no longer needed must be erased. "Erase" means that the data cannot be restored without disproportionate effort and/or expense. The process for erasure must also be formalised, meaning that internal rules must be drafted about who is responsible for checking the retention periods, the frequency with which the checks are to be undertaken and who erases the data.

The Treureva Group experts will support you in the implementation of the new data privacy legislation. ***Contact us.***

Oliver Habke
+41 58 255 73 00
datenschutz@treureva.ch

About the Treureva Group

The Treureva Group is a leading, independent service provider located in the heart of Zurich. Founded in 1982, the Group is wholly self-owned. The group includes Treureva, GHM Partners, Integralis and AVANTA.

With our inter-disciplinary team of over 100 experts we can provide you with comprehensive advice. Just like our orange chair, we can operate anywhere and are there where you need us. Not surprisingly, our credo is "Making our clients more successful".

We are a member of EXPERTsuisse and the international association PrimeGlobal; we are also the only Swiss member of the German Auditors' Association (Wirtschaftprüferverbund BAN e.V.).

Our employees have in-depth knowledge of national and international accounting standards as well as the legal aspects of commercial and specialist regulatory systems and requirements. As ongoing advanced training is one of the foundation stones of our corporate philosophy we can guarantee the highest level of quality for our clients. We have experienced and long-serving staff and can guarantee ongoing service from your contact persons.

treureva AVANTA BROKER SWISS QUALITY BROKER integralis