LEGAL DATA MANAGEMENT WITHIN A GROUP

Personal data is increasingly an indispensable basis for the value adding activities of companies. Within a group, personal data is exchanged for various purposes, with data protection requirements applying. Legal data management ideally sets standards for how the entire group of companies processes personal data but this is often difficult to implement in practice. An affected group company should not wait for a possible group decision, but should actively promote legal data management at company level.

Delia Fehr-Bosshard, LL.M., Attorney at Law

Data protection requirements are increasing

Above all, the increasing digitization of business processes and service provision makes data an increasingly important raw material for companies. Personal data takes on a special role, i.e. information that can be assigned to a determinable person. Each company regularly processes personal data at least as a side effect (e.g., employee data). As a rule, the procurement, processing, storage and / or transfer of this personal data triggers the applicability of data protection regulations. Increasing legal requirements for data protection and data security - e.g. in the EU with the General Data Protection Regulation (GDPR)[1] – mean companies face ever greater legal challenges.

In Switzerland, we are (again) at the beginning of the total revision of the Data Protection Act (DPA)[2]. In January 2018, the National Council's Science, Education and Culture Committee decided to split the revision and tackle the total revision of the DPA "without time pressure"[3]. However, Swiss-based companies and group companies are also affected by the EU's revision, in particular in the processing of personal data of data subjects who are in the EU, when data processing is linked to the supply of goods or services to, or with the behavioral observation of, these persons in the EU.[4] The GDPR becomes effective on May 25, 2018.

Data protection ordinances such as the GDPR and the Swiss DPA contain, in part, detailed information obligations for the companies collecting and processing personal data,

---

1 Regulation EU 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of data and repealing Directive 95/46 / EC (General Data Protection Regulation), available in German at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

2 Federal Act on Data Protection, SR 235.1, available in German under https://www.admin.ch/opc/de/classified-compilation/19920153/index.html.

3 Media release of the National Council's Science, Education and Culture Commission of 12 January 2018, available in German under https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059.

4 Art. 3 para. 2 GDPR.

information rights of the data subjects, processing principles, requirements for the lawfulness of data processing and documentation obligations. Companies may need to conduct data protection impact assessments ahead of new data uses to estimate the potential risks to data subjects. In the development of new offers, products and services they must, as far as possible, make (technical) arrangements and select default settings, so that by default only a minimum of data is collected (so-called "Privacy by design" and "Privacy by default").

Under the GDPR, the risk of sanctioning increases massively: In addition to measures ranging from the imposition of concrete adjustments of processing practices up to bans,[5] the GDPR stipulates, in particular, fines of up to 4% of the total worldwide annual turnover of the company in the previous financial year or EUR 20,000'000.[6]

Legal data management is indispensable

The optimal management of data thus becomes a key success factor: Data management includes all measures, in particular of a conceptual, technical and organizational nature, with which the use of the resource (personal) data is controlled. However, data management does not just mean ensuring that the required and desired data on employees and customers is available in high quality and quantity, but also that this data is maintained and protected. The person who holds the personal data has not only the benefits, but also the duties, e.g. in EU terminology, as a "controller" with decision-making authority over that personal data.[7] Good legal data management enables the best possible, efficient utilization of personal data for their own business processes, while complying with the legal requirements for data protection and security.

(Legal) Data management is already a challenge for a medium-sized, independent company. The human resources department of a Swiss SME (e.g. with full-time and part-time employees, permanent and temporary employees, apprentices, long-term employees and retired former employees) has, even just in their personnel files, a large amount of personal data (e.g. birth dates of employees and family members, addresses, insurance benefits, salaries, bonuses, advances, pensions, illnesses, employment references, assessments, promotions, etc.). In addition to various internal users (e.g. HR managers, trainers, IT officers, direct supervisors), the employer also shares this personal data with external service providers (e.g. outsourced accounting service providers, auditors) and independent third parties (e.g, compensation funds, pension funds, occupational health insurance).

While dealing with these risks is already challenging for the individual company, the complexity increases abruptly in a group structure. Each individual group company is potentially the procurer and recipient of personal data (e.g. employer, supplier). The individual company processes personal data in its own interests (e.g. payroll accounting, order processing) and forwards these for its own purposes inside and outside the group (e.g. services of a central personnel department for the group company, central invoicing for orders). The Group companies also provide each other with personal data of their employees, suppliers and customers for the purposes of the receiving group companies or in the interests of the group as a whole (e.g. a group-wide career portal, personnel

---

5 Art. 58 para. 2 GDPR.

6 Art. 83 para. 5 GDPR.

7 C.f. the definition in Art. 4 (7) GDPR.

appraisal, customer brokerage for group companies, customer management systems). This disclosure of personal data within the Group, to parent, subsidiary or sister companies is also considered as disclosure to third parties and thus subject to the data protection requirements.

The data transfers are often covered by a contractual purpose and so allowed under the GDPR itself. In the case of data disclosure to a third party abroad, there are additional requirements if the target country does not offer so-called "adequate" level of protection. Each of these data transfers also entails a risk to the data security of the commissioning company: When the external payroll service provider manages its own IT systems and unauthorized third parties obtain access, this not only damages the employees concerned, but possibly also the employer, e.g. when account details for the salary payment are revealed. Reputational risks due to careless handling of data also increase as the public's attention for topics such as data security and privacy increases. Making it all the more important that companies have comprehensive legal management of their data processing practice.

Development of legal data management

The individual group company or the entire group can better ensure compliance with duty of care requirements by means of uniform data management. A single group company can also serve as a role model within the group and promote privacy and security. The following steps are useful for determining the necessary standards and measures for improved data management:

- **Inventory, e.g. with data mapping**: Data mapping creates a layout of the processed personal data and the existing data streams of the entire corporate group. The goal is to identify the existing processing procedures and data flows as well as their basic principles and the company's own control mechanisms. This includes, in detail, the identification of categories of personal data (e.g. address data, payroll data, health data, order data, payment history, etc.) and their purpose (e.g., payroll, recruiting, targeted advertising, credit decisions). Based on this, the handling of personal data is evaluated: e.g. What data does the company collect, about who, for what purpose, what information is provided to the data subject, on what basis, with which standard contracts, contractual clauses, etc.? To whom does the company pass on this data? How long does it retain the personal data, when does it delete or anonymize the data by default? It is also important to identify which personal data (e.g. salary data, order behavior) and in which areas (e.g. personnel, marketing) are indispensable for day-to-day business. Furthermore, the affected data should be subdivided according to sensitivity: health data of the employees is e.g. more sensitive than publicly available address data. Suitable for information gathering purposes are documents on existing standards, data protection regulations, contracts, etc. but also interviews and workshops. Data mapping can quickly become very time consuming. If a Group Executive Board is unwilling to cover this expense, it is still advisable for a single group company to record the incoming and outgoing flows of personal data from its individual point of view.
- **Identification of the need for action by means of gap analysis:** The actually practiced conditions must be checked for compliance with the legal requirements for information, consent, basis for data processing, data security,

etc. This should show up any gaps which pose a risk for the company and that need to be closed. These are to be further categorized in a risk-based approach based on the reputation and sanction risk and the urgency: Which practices of the group company are not compliant with the GDPR or the applicable data protection law (such as the DPA) and for what reasons? On what basis does the company rely on the processing of personal data? For which data processing and forwarding is there an insufficient basis? Where are the biggest risks? If there is no Group Executive Committee decision, the gaps must be determined from the point of view of the individual company.

- **Measures:** Based on the identified deficits and risks, the individual group company can derive the action needed to close the identified gaps in a risk-adequate manner. Changes to be made include, above all, technical rules (especially in the area of IT, e.g. technical access restrictions, two-factor authentication, standard pseudonymisation or anonymisation etc.) and organizational adjustments (e.g. definition of standard procedures and documents for information and consent, definition of responsibilities for information requests etc.). In order to determine the technical and organizational measures to be taken, the timing of the implementation and any budget restrictions must be clarified in detail in this phase. At this level, there is another opportunity to get more group companies or even group Management on board to work out a group-wide plan of action. The measures must be approved by the management of each company involved.
- **Implementation:** With regard to the coming into effect of the GDPR in May 2018, many companies are already in the implementation phase. Even if the ideal case involves a group-wide uniform enforcement of the measures, this is often illusory in practice. In order to fulfill its duty of care as a company, a phased implementation of the most urgent measures at the level of the local group company may be preferable to waiting for a global group decision. The implementation also includes operational change. Regularly, however, the focus is on the training and instruction of the employees.

"Data Awareness" is central to data management

When implementing measures, the "human factor" plays a key role: The Federal Data Protection and Information Commissioner (FDPIC) recommends "in-depth information and sensitization of employees in connection with technical-organizational preventive measures"[8] in order to avoid a negligent breach of data protection. What at first glance appears to be a very general statement, strikes at the very heart of a company's duty of care in the area of data protection: technical and organizational measures are essential to ensure adequate protection of personal data at company level. The "human" factor, however, is and remains the real "uncertainty". In the area of data security, it is regularly human error, carelessness or ignorance that is the actual causes of data leaks. The company can only effectively fulfill its duty of care obligations if it raises the awareness of each individual employee for the importance of personal data and its security, through

[8] FDPIC, Accountability, available in German at https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/verantwortlichkeit.html (last visited on 28 February 2018).

information, education, training and binding instructions. Employees (from the temporary help to the top management) are the primary targets of these measures. However, "data awareness" also requires uniform standards when communicating with other group companies. As a rule, a group company can better enforce and justify its guidelines for the intra-group and external transfer of personal data if it conducts careful data management internally at the level of its own company and not only complies with data protection requirements on paper but actively lives by them. The more consistent and reliable the legal data management at the level of the individual company, the more likely it is that other group companies will follow the good example. When group-wide standards are actually lived by, they in turn simplify compliance with data protection requirements and have, as a side effect, a positive effect on the reputation of the entire group.

VISCHER AG
www.vischer.com
Schuetzengasse 1 8021 Zurich Switzerland Tel +41 58 211 34 00
Aeschenvorstadt 4 4010 Basel Switzerland Tel +41 58 211 33 00