Pestalozzi Update February 2017

Revision project of the Data Protection Act – new obligations and the implications for companies

The preliminary draft of the complete revision of the Swiss Federal Act on Data Protection (FADP) was submitted to the Swiss parliament for consultation in December 2016. The goal of this revision is among others to strengthen data protection provisions to reflect evolving technological and social circumstances. In this respect, a key objective is to align Swiss data protection laws with European legislation in order to facilitate continued transborder dataflows.

- **The revision project of the Data Protection Law imposes greater responsibilities and obligations on companies.**
- **Companies are required to process the personal data of individuals in a more transparent manner and to adequately fulfil their duty to provide information to individuals so they can exercise their rights under the law.**
- **Stiff penalties can be imposed for data protection infringements.**

This revision is intended to create greater transparency in the processing of personal data and to give the individuals concerned more control over their data. To meet the objectives of the revised law, companies will be obliged to take steps to prevent potential data breaches whenever personal data is processed. In return, companies will no longer be required to declare data files for registration.

1. Alignment with EU legislation

Within the scope of the Schengen Association Agreement, Switzerland has committed to adopting the new **EU Directive 2016/680** covering data protection. Furthermore, Switzerland intends to ratify the ETS 108 (European Treaty Series [Sammlung der Europäischen Verträge (SEV)]) "for the Protection of Individuals with regard to Automatic Processing of Personal Data", on which the Council of Europe has begun deliberations on its revision.

The need for alignment and equivalence between Swiss and EU legislation in this area of the law is of critical importance to the Swiss economy, particularly as this will secure and improve Switzerland's ability to remain competitive: In fact, it is this alignment which forms the basis for EU recognition of Switzerland as a non-member state with acceptable data protection standards, and it is only in this way that simplified transborder data flows shall remain feasible in the future. In addition, a high level of data protection that meets international standards will also promote the development of new industries in the digital society.

2. Key changes affecting companies

Any company that processes personal data is bound by the provisions of the FADP and in the future by its revision. Therefore, **all companies operating in Switzerland** are affected by the amendments proposed in the preliminary draft. Companies which specify the purpose of personal data processing and which determine the means and the scope of such processing, are defined as being a **"controller"** under the revised Data Protection Act (Art. 3(h) VE-DSG [Preliminary Draft, Data

Protection Act], which corresponds to Art. 3(8) EU Directive 2016/680).

In future, data pertaining to legal persons will not be subject to protection anymore (article 1 of the preliminary draft of the FADP (**PD-FADP**). In this way, the transfer of data pertaining to legal persons to foreign states will be facilitated (in many cases, these states do not include legislative provisions for the protection of data relating to legal persons). **Company-related data will no longer be protected under the revised FADP.** However, comprehensive protection of such data will continue to be enshrined in the provisions of other legislation (article 28 et seq. of the Swiss Civil Code (ZGB; Zivilgesetzbuch), the Unfair Competition Act (UWG; Gesetz gegen unlauteren Wettbewerb), the Federal Copyright and Related Proprietary Rights Act (URG; Bundesgesetz über das Urheberrecht und verwandte Schutzrechte), etc.). Additionally, personality profiles are no longer protected as this was viewed as being a special feature to Swiss law; only **profiling**, i.e. any form of automated personal data processing, will be covered by the revised FADP (article 3(f) PD-FADP) and will request a prior informed consent (articles 4 para. 6 und 23 para. 2 lit. d PD-FADP).

The intention is to improve and increase **transparency** in the way companies manage personal data processing. In this regard, the **active duty to inform** data subjects about the collection of their data (not only for sensible personal data) will be expanded to cover all types of data processing (article 13 PD-FADP) and must comprise all relevant information that enables data subjects to exercise their rights under the law. However, companies are permitted to comply with this duty to provide information by issuing general declarations (such as in their General Terms and Conditions or on other easily available and comprehensible way) rather than on an individual basis. Data subjects must also receive **information regarding any decisions taken on the basis of automated data processing** (article 15 PD-FADP). In such cases, they must be given the opportunity to make their views known. Companies are obliged to provide further information if data subjects exercise their extended **right to information** in accordance with article 20 PD-FADP, or if personal data is transmitted to third parties (article 19(b) PD-FADP).

In particular, the revised DSG creates new **processing and reporting obligations** for companies: companies are obliged to conduct audits of data handling for all data processing activities, and, in cases where an increased risk for the rights of the data subject is identified, they must report their planned preventive measures to the Federal Data Protection and Information Commissioner (FDPIC). Furthermore, any **data breaches** pursuant to article 17 PD-FADP must be reported to the FDPIC without delay and to the concerned data subjects if necessary for their protection or the FDPIC requests it. In conducting data processing audits, companies may seek guidance from the recommendations for best practices published by the FDPIC (article 8-9 PD-FADP).

As a consequence, **self-regulation** and **responsible behaviour** by companies will play a key role. Compliance with data protection requirements must be reinforced by the introduction of appropriate **data protection-friendly technology or in the default privacy settings** of company systems, already as early as the planning phase of data processing activities, so that the risk of personal data breaches can be minimised or prevented (article 18 PD-FADP). It should become a standard operating procedure to prioritise data solutions which maximise data privacy (as a **privacy by design** solution). This means that going forward, companies can only collect and process smaller data quantities. In addition, companies will be required to **document their entire data processing activitie**s (article 19 PD-FADP).

With regard to the **transfer of personal data to other countries**, the current regulations will basically remain in place. Personal data may not be disclosed abroad if the privacy of the data subject would thereby be seriously threatened. This is particularly the case if the country in question does not have the necessary legislation to guarantee a sufficient level of protection (article 5 PD-FADP). Data transfer agreements (based on the sample agreement issued by the Council of Europe), treaties under international law (such as the new Privacy Shield Treaty for data transfers between the USA and Switzerland), as well as binding internal company data protection regulations which have been previously approved by the FDPIC or a foreign data protection agency, are deemed to guarantee sufficient protection (article 5(3) PD-FADP). Notwithstanding the above requirements, the disclosure of data to other countries is insofar permissible, if such data is essential to establish, exercise or enforce legal claims before an administrative authority, such as a tax office (article 6(1)(c) PD-FADP).

The FDPIC is charged with supervising the implementation of self-regulation by companies and has been assigned an expanded role with broader powers

(article 41 et seq. PD-FADP). It may enact **codes of conduct,** which can be used by companies as a basis to create its own internal data protection policies (article 8 PD-FADP). Also, the FDPIC may open an investigation into a company, either in its own right or following the filing of a complaint, to assess the legality of that company's data processing activities. Subsequent to this investigation it may issue binding directives to the companies concerned. This enables better supervision of the implementation of, and compliance with, data protection requirements.

3. Stiffer penalties and sanctions

To ensure strict compliance with the revised obligations and provisions of the FADP by the responsible parties, the catalogue of punishable offences has been aligned with the revised responsibilities and the penalties have been stiffened. The **maximum fine** will increase from CHF 10,000 to CHF 500,000 (article 50 et seq. PD-FADP).A further revision is the obligation now incumbent upon the FDPIC to report any criminal offence within the meaning of article 50 et seq. PD-FADP to the criminal prosecution authorities.**Legal persons can be directly subject to criminal prosecution** in accordance with article 53 PD-FADP.

4. Recommendations

The protection of privacy in the course of data processing is now clearly strengthened by this revision. Although the revision is still in the parliamentary consulting process, stiff resistance to the proposals is unlikely. It is critical that the Swiss model remains aligned with the new EU Directive 2016/680.

Companies are facing new challenges and responsibilities. The need to demonstrate concrete action should not be underestimated. Starting today, companies need to pay more attention to data protection and regulatory issues. Indeed, they need to audit their existing internal procedures for handling personal data and set the necessary standards to prepare them for the implementation of the revised Data Protection Act. Companies currently without a compliance infrastructure and binding internall data protection policies should develop them accordingly.

Checklist for companies	
1	Is the processing of personal data carried out in good faith and in accordance with the stated purpose, and does it follow the principle of proportionality?
2	When processing personal data, do we sufficiently meet our duty to provide information?
3	Do we utilise technology and default privacy settings which maximise the protection of personal data?
4	Do we have sufficient safeguards in place when transferring data to foreign countries?
5	Do we have compliance infrastructure and internal data protection policies in place which enable us to audit and enforce our data processing procedures?

We would be pleased to work together with you to develop the steps required to ensure your company complies with the revised Data Protection Act.

For further information, kindly visit our website or contact the following persons:

Dr. Lorenza Ferrari Hofer
Partner
Head IP&TMT Group
lorenza.ferrari@pestalozzilaw.com
+41 44 217 92 57

Michèle Burnier
Partner

michele.burnier@pestalozzilaw.com
+41 22 999 96 31

Pestalozzi Attorneys at law

Zürich - Löwenstrasse 1 | 8001 Zürich | Schweiz | T +41 44 217 91 11
Genf - Cours de Rive 13 | 1204 Genf | Schweiz | T +41 22 999 96 00

www.pestalozzilaw.com