ATTORNEYS AT LAW

SCHELLENBERG WITTMER

MARCH 2017

Newsletter

Authors:
Roland Mathys
Samuel Klaus

DATA PROTECTION / DATA PRIVACY

Highlights of the Revision of the Data Protection Act

The revised Swiss Data Protection Act builds on certain aspects of the EU General Data Protection Regulation in order to ensure that the EU will consider Switzerland as providing for an adequate level of data protection. To this aim, the preliminary draft sets out new regulation regarding the Controllers and Processors as well as the Data Subjects. This newsletter sheds some light on the planned changes from the point of view of these three target groups.

1 STATUS OF THE REVISION

The preparations for the revision of the Swiss Data Protection Act (**DPA**) have started back in 2010. At the end of 2016, the preliminary draft of the revised DPA has been published (**PD-DPA**). The consultation period will end on 4 April 2017. Since quite a number of responses are to be expected, the consolidated results in the form of the final draft of the revised DPA with the accompanying dispatch to the Federal Parliament will most likely not be available before the end of 2017. The revised DPA could then enter into force at the earliest between mid-2018 and the beginning of 2019.

The PD-DPA takes into account, *inter alia*, the requirements of the EU General Data Protection Regulation (**EU-GDPR**) and the revised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data by the Council of Europe (ETS 108), in order to ensure that the EU will continue to consider Switzerland as providing for an adequate level of data protection. In addition, the PD-DPA contains a number of changes to strengthen data protection in comparison with the current DPA. Even though not all proposed provisions of the preliminary draft might find their way into the final draft, an early assessment is recommendable, in particular for enterprises whose business models will be affected by the proposed changes.

In this newsletter, we present the highlights of the revision of the DPA from the point of view of the **Data Controller**, the **Data Processor**, and the **Data Subject**.

2 DATA CONTROLLER

The current term of 'controller of a data file' will be replaced by the term **Controller** (*Verantwortlicher*). The Controller is subject to new information obligations as well as precautionary obligations. These are backed up by criminal sanctions which are more stringent than those in the current law – but by far not as severe as the fines imposed under the EU-GDPR.

2.1 NEW INFORMATION OBLIGATIONS

When collecting personal data, the Controller will be subject to **more extensive information obligations** than under the current law. In particular, he will need to inform the Data Subjects about the identity and contact details of any Processor if the data processing is carried out by a third party. Furthermore, in case of unauthorized data processing or loss of data (data breaches), the Controller will have to inform the Federal Data Protection and Information Commissioner (**FDPIC**) as well as the affected Data Subjects, if so required for their protection (e.g. in case of loss of credit card data, log in information, etc.).

2.2 NEW PRECAUTIONARY OBLIGATIONS

If a specific data processing presumably leads to an increased risk for the Data Subject, then the Controller has to conduct a **Privacy Impact Assessment (PIA)** before such processing. The result of the PIA as well as all data processing will need to be documented. This comprehensive **documentation obligation** will replace the requirement in the current law to register certain data collections (data files). Further-more, the result of the PIA as well as the measures taken to mitigate the related risks have to be notified to the FDPIC who may, within three months, raise objections against the measures taken.

> "The preliminary draft provides for Privacy by Design and Privacy by Default – and backs them up with criminal sanctions."

Just as under the current law, the Controller needs to ensure the **data security**. However, under the revised law, he might be subject to a fine if he neglects to implement the necessary measures. He will also be subject to a fine if he fails to implement the newly introduced principles of **Privacy by Design** (data protection by technological means) and **Privacy by Default** (data protection friendly default settings). Privacy by Design requires preventive technical and organizational measures (e.g. anonymization); Privacy by Default prescribes appropriate default settings to ensure that only such data is processed as required for the intended purpose and only to the extent as necessary therefor.

On the other hand, the revised DPA provides for certain simplifications for the Controller in the form of the newly introduced instrument of Best Practices: If a Controller abides by **Best Practices**, the law stipulates that he will be deemed to be in compliance with the data protection regulations specified thereby. Best Practices can either be drafted by the FDPIC or by private parties, but will have to be approved by the FDPIC in the latter case.

2.3 STRICT CRIMINAL SANCTIONS

The PD-DPA extends the **scope of criminal sanctions**: The information obligation, the duty to provide information on request by the data subject, as well as the documentation obligation are all subject to fines. If a Controller disobeys an order of the FDPIC, transfers data abroad without adequate safeguards, unlawfully delegates data processing to a processor, or neglects to implement appropriate data security measures, he will also be subject to a fine. Furthermore, the failure to perform a PIA as well as the default to implement Privacy by Design and Privacy by Default may also trigger criminal sanctions.

The PD-DPA provides for **fines up to CHF 500'000 in case of intent respectively CHF 250'000 in case of negligence**. These amounts are high compared to the *status quo* - but still rather low in comparison to the EU-GDPR. As a noteworthy difference to, e.g. the sanctions in antitrust law, these fines are not administrative sanctions levied against a corporation, but rather criminal sanctions against the individual (e.g. the employee of such corporation). It remains to be seen whether this concept is appropriate and effective.

3 PROCESSOR

While the current law just speaks of 'third parties processing personal data for the Controller' and contains few provisions regarding such third parties, the PD-DPA defines such third parties as **Processors** and makes them subject to various obligations - as well as to the related criminal sanctions.

3.1 EXTENSIVE NEW OBLIGATIONS

Many of the new obligations set out in the PD-DPA will **directly apply to the Processor** as well, either cumulatively or alternatively to the Controller. For example, the Processor will have to ensure data security in the same manner as the Controller, will have to document the data processing, and will have to implement the principles of Privacy by Design and Privacy by Default. Regarding the PIA, the Processor is only obligated alternatively to the Controller – but is subject to the same criminal sanctions.

The Processor is under an obligation to notify data protection violations (unauthorized data processing, **data breaches**) to the Controller, in order to enable the Controller to fulfill his notification obligation vis-à-vis the FDPIC and – potentially – the Data Subjects.

3.2 SUBPROCESSING ONLY WITH APPROVAL

The Processor may only subcontract the data processing (or a part thereof) to a third party (sub-processor) upon the **prior written approval of the Controller**. A general consent by the Controller may suffice, but in such case the Processor will need to inform the Controller before any changes in order to enable the Controller to object thereto. This is intended to ensure that the Controller himself is in a position to fulfill his information obligation vis-à-vis the Data Subjects.

3.3 SUBJECT TO CRIMINAL SANCTIONS

The Processor will be subject to the same strict criminal sanctions as the Controller, including **fines of up to CHF 500'000 in case of intent respectively CHF 250'000 in case of negligence**.

"The Processor will be subject to new obligations – as well as to the corresponding criminal sanctions."

4 DATA SUBJECT

The PD-DPA also contains certain changes affecting the **Data Subject** whose data are being processed. On the one hand, under the PD-DPA only data pertaining to individuals shall be protected, while on the other hand the scope of sensitive data shall be extended and the right to information shall be strengthened.

4.1 APPLICATION LIMITED TO INDIVIDUALS

The current law protects both data pertaining to **individuals** (natural persons) as wells as data pertaining to legal entities (legal persons). Under the PD-DPA, the data protection provisions shall only apply to data pertaining to individuals. While data pertaining to legal entities would lose its protection under the PD-DPA, this change should still be welcomed since data transfers abroad would become much easier: Since the majority of foreign data protection regimes does not provide for the protection of personal data pertaining to legal entities, the intended change would greatly facilitate data transfers abroad.

4.2 SENSITIVE DATA

The term of sensitive data will be extended to **genetic data** (such as e.g. a DNA profile) and **biometric data** able to unambiguously identify a person. Biometric data comprises e.g. facial recognition pictures, iris scans, or finger prints (e.g. such as are used to unlock smartphones).

4.3 TRANSPARENCY / INFORMATION RIGHT

The revision of the DPA also serves to raise transparency regarding data processing. To that end, the **transparency obligations** respectively the information obligations of the Controller are strengthened on the one hand (cf. above section 2.1). On the other hand, the **right to information** of the Data Subjects is expanded and the law defines more clearly which additional information the Controller will have to disclose to the Data Subject as a minimum standard.

Failure to comply with the duty to disclose the requested information is subject to **criminal sanctions**: If the Controller intentionally provides false or incomplete information, he will be subject to a fine of up to CHF 500'000.

A special provision will address how **data pertaining to the deceased** shall be handled. In particular, their relatives will have a right to access the data and may request its deletion.

5 CONCLUSION

While the new provisions in the PD-DPA affect all the involved parties, the **Controller** will be affected most, as he will face a number of new obligations and run the risk of incurring severe fines in case of non-compliance.

Whereas the Processor is subject to only a few obligations under the current law, many of the new provisions focus on the **Processor**. The PD-DPA contains a significant number of obligations which will apply directly to the Processor, either cumulatively or alternatively to the Controller. Furthermore, the Processor will be subject to the same criminal sanctions as the Controller.

But also the **Data Subjects** are affected by the PD-DPA: On the one hand, legal entities will lose the protection of the DPA. On the other hand, the transparency and information rights of the Data Subjects will be strengthened.

Presumably, not all new provisions in the PD-DPA will actually find their way into the revised law. In a first step, the results of the consultation process will be consolidated into a final draft addressed to the Parliament. In a second step, a thorough debate in the Parliament has to be expected, closely watched by a public that is getting more and more interested in, and concerned about, data protection issues.

The **EU-GDPR will have effect as of 25 May 2018**, affecting – directly or indirectly – Swiss companies as well. However, **it is not to be expected that the revised Swiss Data Protection Act will take effect as well by then already**. Nonetheless, it is advisable for Swiss companies to watch the development closely and to adapt their internal data protection processes as early as possible to the emerging changes. This way, a repeated adaptation of the compliance structures might be avoided – first to the requirements set out by the EU-GDPR, and shortly thereafter to those of the revised Swiss DPA.

"Swiss companies should watch the development closely – to avoid repeated adaptations of their compliance structure to the EU-GDPR on the one hand and to the revised Swiss DPA on the other hand."

Contacts

The content of this Newsletter does not constitute legal or tax advice and may not be relied upon as such. Should you seek advice with regard to your specific circumstances, please contact your Schellenberg Wittmer liaison or any of the following persons:

In Zurich:

Roland Mathys
Partner
roland.mathys@swlegal.ch

Samuel Klaus
Associate
samuel.klaus@swlegal.ch

In Geneva:

Vincent Carron
Partner
vincent.carron@swlegal.ch

Catherine Weniger
Counsel
catherine.weniger@swlegal.ch

SCHELLENBERG WITTMER LTD / Attorneys at Law

ZURICH / Löwenstrasse 19 / P. O. Box 2201 / 8021 Zurich / Switzerland / T +41 44 215 5252
GENEVA / 15bis, rue des Alpes / P. O. Box 2088 / 1211 Geneva 1 / Switzerland / T +41 22 707 8000
SINGAPORE / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapore 049909 / www.swlegal.sg

www.swlegal.ch