ZURICH
Brandschenkestrasse 24
CH-8027 Zurich

GENEVA
Route de Chêne 30
CH-1211 Geneva 6

LAUSANNE
Avenue de Rhodanie 40C
CH-1007 Lausanne

Revision of Swiss Data Protection Act and Ordinance finalized, entering into force on 1 September 2023

On 31 August 2022, the Swiss Federal Council decided that the revised Data Protection Act ("revDPA") shall enter into force on 1 September 2023 and adopted the corresponding revised implementing Ordinance ("revDPO"), thereby concluding a revision process that started in September 2017. The revision responds to technological advancements, aligns Swiss data protection law with today's international data protection standards, including the GDPR, and shall allow Switzerland to uphold its status as a country adequately protecting personal data from an EU perspective.

Published: 18 November 2022
Updated: 24 July 2023

AUTHORS	Guy Vermeil	Partner, Head of Technology and Outsourcing
	Fedor Poskriakov	Deputy Managing Partner, Head of Fintech
	Lukas Morscher	Partner, Head of Technology and Outsourcing
	Jürg Simon	Partner, Co-Head of Intellectual Property
	Leo Rusterholz	Associate
	Nadja Guberan-Flühler	Associate
EXPERTISE	Data Protection and Privacy TMT	

Key aspects of revDPA for the private sector:

- End to protection of legal entities' data: Under the revDPA, legal entities' personal data will no longer be protected, thereby following the main international data protection standards, including the GDPR;
- Strengthened individual rights: Data subjects benefit from enhanced information rights, including as to data exports.

They also get a right to data portability (i.e. a right to receive their own personal data in a commonly used electronic format, subject to certain prerequisites).

In case of automated decision-making, affected data subjects can generally require that the automated decision be reviewed by a natural person;

- Extended governance & documentation rules: Controllers and processors have to keep data processing records (whereby SMEs with less than 250 employees may benefit from an exemption).

Controllers must perform a data protection impact assessment with respect to contemplated data processing activities entailing high risks for data subjects' personality and fundamental rights and, in some cases, notify the Federal Data Protection and Information Commissioner ("FDPIC").

Data breaches must be notified to the FDPIC when they are likely to create high risks for data subjects' personality and fundamental rights, and to the data subjects when necessary for their protection or when the FDPIC so requests. Controllers domiciled abroad that offer goods and services in Switzerland or monitor the behavior of data subjects in Switzerland must appoint a representative in Switzerland, if they process data regularly and on a large scale and the processing entails high risks for the data subjects' personality;

- Expanded powers of the FDPIC: The FDPIC is granted the competence to issue binding administrative decisions (including requiring controllers or processors to modify, suspend or terminate their processing activities or to delete or destroy personal data). Contrary to his EU counterparts, the FDPIC (still) does not have the competence to issue fines;
- Introduction of severe fines: Fines for willful breaches of certain provisions of the revDPA are increased to CHF 250,000 (from previously CHF 10,000). Cantonal law enforcement authorities (rather than the FDPIC) are competent to prosecute such breaches. In principle, fines are imposed on the responsible individual, not on the legal entity acting as controller or processor.

Adoption of final revDPO

The revDPO implements and specifies the requirements of the revDPA. The draft revDPO submitted to public consultation had been heavily criticized by legal commentators and interest groups for being unclear and, in some cases, imposing obligations without a well-defined basis in the revDPA. Based on such feedback, the final revDPO has been redrafted and provides for some alleviations compared to the initial draft.

Key aspects of the revDPO for the private sector include the following:

- Data security: Controllers and processors must determine the necessary level of protection and implement suitable technical and organizational measures (to be reviewed and adapted, as required) in a risk-based approach, whereby they must consider the types of processed data, purpose type, extent and circumstances of processing, risks to personality and fundamental rights, current state of the art and implementation costs.
- Data logging: Controllers and processors must keep logs when processing sensitive data on a large scale by automated means or carrying out high-risk profiling, despite significant criticism towards this new obligation during the public consultation (as there is no respective basis in the revDPA).

The related duties have only been slightly alleviated compared to the initial draft, such that the minimum log retention period is 1 year (instead of 2 years as initially envisaged);

- Processing Regulations: Controllers and processors must issue (and regularly update) processing regulations for automated data processing, if they process sensitive data on a large scale or carry out high-risk profiling. The regulations must include information on the internal organization, data processing and control procedures and measures to ensure data security;
- Sub-processing: The controller's authorization of sub-processing (required pursuant to the revDPA) may be specific or general. In case of a general authorization, the processor must inform the controller of contemplated changes in its sub-processors and the controller may object thereto;
- Data exports: In addition to the safeguards set out in the revDPA, data exports may rely on an approved code of conduct or certification ensuring suitable data protection abroad.

The revDPO appends the list of countries providing for adequate data protection legislation for cross-border transfer purposes. The initial list corresponds to the existing list published by the FDPIC (and includes all EEA member states, the UK and further selected countries). If data export to countries not providing for adequate data protection legislation is based on standard contractual clauses ("SCC"), the exporter must implement appropriate measures to ensure that the recipient complies with such SCC;

- Information and access right modalities: The controller must inform the data subject about the obtaining of personal data in a precise, transparent, intelligible, and easily accessible manner. To exercise an access right, data subjects must generally make a written request (including by electronic means). The requested information must be provided in an intelligible manner and generally in writing (including by electronic means) or in the form in which the data are available. The controller must take appropriate measures to identify the requesting data subject, which must comply with such measures.

Information and access right modalities have been streamlined compared to the initial draft. In particular, the relevant obligations are imposed on controllers only (and not also on processors), and controllers do not systematically need to inform all data subjects when correcting or erasing their data or limiting the processing.

Next steps

Controllers and processors subject to the revDPA should, in particular:

- review privacy notices/policies and customer/supplier agreements for compliance with the extended information duties;
- establish processes to address requests related to the exercise of individual rights, to carry out data protection impact assessments (as required) and to respond to (and promptly notify) data breaches;
- keep and update records of data processing activities, data logs and processing regulations, each as required;
- review and amend data processing agreements and existing bases for data exports, each as necessary; and
- assess whether they must appoint a representative in Switzerland.

Given the similarities between the revDPA and the GDPR, companies that are already GDPR-compliant will only need to take targeted steps to meet the requirements of the revDPA and

revDPO. Significant compliance efforts will be required from companies that are not yet GDPR-compliant. Controllers and processors have time until 1 September 2023 to implement all necessary steps as there will be no transition period.

Please do not hesitate to contact us in case of any questions.

Legal Note: The information contained in this Smart Insight newsletter is of general nature and does not constitute legal advice.

CONTACTS		
	Guy Vermeil	Partner, Head of Technology and Outsourcing, Geneva guy.vermeil@lenzstaehelin.com Tel: +41 58 450 70 00
	Fedor Poskriakov	Deputy Managing Partner, Head of Fintech, Geneva fedor.poskriakov@lenzstaehelin.com Tel: +41 58 450 70 00
	Lukas Morscher	Partner, Head of Technology and Outsourcing, Zurich lukas.morscher@lenzstaehelin.com Tel: +41 58 450 80 00
	Jürg Simon	Partner, Co-Head of Intellectual Property, Zurich juerg.simon@lenzstaehelin.com Tel: +41 58 450 80 00
	Leo Rusterholz	Associate, Zurich leo.rusterholz@lenzstaehelin.com Tel: +41 58 450 80 00
	Nadja Guberan-Flühler	Associate, Zurich nadja.guberan@lenzstaehelin.com Tel: +41 58 450 80 00