BÄR & KARRER

BRIEFING SEPTEMBER 2022

THE NEW SWISS DATA PROTECTION LAW – IMPLEMENTING PROVISIONS ADOPTED

On 31 August 2022, the Federal Council officially adopted the revised Data Protection Ordinance („revDPO") as well as the Ordinance on Data Protection Certifications and confirmed that the Ordinances together with the revised Data Protection Act („revDPA") will enter into force on 1 September 2023. As a result, companies and other persons processing personal data have one year to implement the new requirements in their organisations. There will be no further grace period, and companies should get ready now.

AT A GLANCE

With the newly adopted revDPO, the Federal Council exercised its competence to clarify and specify certain obligations of the revDPA. In particular, the revDPO provides implementing provisions on data security, information and documentation obligations, the rights to access and data portability, the outsourcing of data processing to third parties, cross-border data transfers, the data protection advisor (i.e., data protection officer), data protection impact assessments and the notification of data breaches. In the following, we have summarised the most important provisions for private companies:

DATA SECURITY MEASURES

The provisions concerning the required level of data security specify article 8 revDPA and are generally based on the current provisions of the DPO. The revDPO does not opt for rigid minimal standards but follows an **individual risk-based approach**: The controller and processor need to determine the necessary level of protection, assess the risk and based on their assessment decide which measures should be taken to ensure an adequate level of data security. To determine the required level of protection, the kind of data, purpose, scope and means of processed data should be taken into account. For the risk assessment, the causes of the risk, the main hazards, measures taken or planned to reduce the risk and the likelihood and severity of a breach of data security despite the measures taken or planned should in particular be accounted for.

When determining the technical and organisational measures, **state of the art** and **implementation costs** should also be considered. However, data controllers and processors cannot exempt themselves from the obligation to provide appropriate data security measures on the grounds that this would entail excessive costs; rather, they must in any case be in a position to ensure adequate data security.

INFORMATION AND DOCUMENTATION OBLIGATIONS

The revDPA stipulates the **duty of information for the controller**, subject to certain exceptions. The revDPO specifies how controllers must provide such information: The controllers have an obligation to inform data subjects appropriately about the collection of personal data; ‚appropriately' is specified as meaning that information should be provided in a precise, transparent, comprehensive and easily accessible form. The duty of information addresses the controller alone and not the processor, but the controller is obliged to inform the data subject about the fact that data will be disclosed to a processor and to provide information about the processor.

If an intended data processing activity potentially bears a **high risk for the rights of the person whose data is processed**, the controller may need to perform a **data protection impact assessment (DPIA)** beforehand. The controller must store this assessment for at least two years after termination of the processing.

RIGHTS TO ACCESS AND DATA PORTABILITY

Several provisions concerning the right to access remain unchanged. **Access requests can be made in writing or electronically and, with the consent of the controller, also orally**. The provisions concerning the deadline and exceptions as to when the information does not need to be provided free of charge remain unaltered to a large extent. In the past, a controller could levy a fee if the data subject had received the information in the past twelve months and did not have a legitimate interest in requesting access again. This provision was removed in the revDPO, as – under the revDPA – such requests now constitute a reason to refuse access altogether.

With the revision of the DPA, a **new right of data portability was introduced**. Under certain conditions, individuals have the right to receive their data in a commonly used and machine-readable format so that they can transmit it to a different company or otherwise use the data. The right to data portability only applies to personal data that has been disclosed by the data subject to the controller. Such data is data that the data subject provided to the controller knowingly and willingly as well as data that the controller collected about the individual and his or her behaviour when using a device or service. However, **data deduced by the controller from the provided or observed data does not fall under the right to data portability**. The time limit, form and further modalities of the right to data portability shall be determined in accordance with the provisions on the right to access. The revDPO also clarifies that **„commonly used and machine-readable formats" are formats that enable the personal data to be transferred with a reasonable effort and to be further used by the data subject or another controller**. Examples of these are XML, JSON, or CSV.

CROSS-BORDER DATA TRANSFERS

The rules on cross-border data transfers generally remain the same but the revDPO states that, if standard contractual clauses **(„SCCs")** are used as a basis for cross-border data transfers, the data exporter must make sure that **appropriate measures** are implemented to ensure that the recipient abroad complies with the SCCs. With this provision, the Federal Council has, in our view, **confirmed a risk-based approach** when transferring personal data based on the SCCs to countries which do not provide an adequate level of data protection, such as the US. To define what measures are appropriate, data exporters will generally be required to **conduct a data transfer impact assessment (DTIA)**.

In its annex, the revDPO lists all countries that, according to the Federal Council's assessment, provide an adequate level of data protection. These include all EU member states, the United Kingdom, Israel, to a certain extent Canada, as well as Andorra, Argentina, Faroe Islands, Gibraltar, Guernsey, Iceland, Isle of Man, Israel, Jersey, Monaco, New Zealand and Uruguay.

FURTHER PROVISIONS

Processors who are processing personal data on behalf of a controller **may only use sub-processors if the controller has consented thereto**. The revDPO now provides that such **consent can be given specifically or in general**. If the controller provides a general consent, the processor must inform the controller about every intended change of sub-processors in advance and the controller has the right to object to such changes.

For the **data protection officer**, on the other hand, not much has changed. One new aspect is, that according to article 23 para. 4 revDPA the controller may consult the data protection officer instead of the FDPIC if a data protection assessment reveals a high risk even after implementing mitigating measures for the identified risks.

Private data controllers and data processors who **process sensitive personal data on a large scale by automated means** or who carry out **high-risk profiling** must at least **log** the storage, modification, reading, disclosure, deletion and destruction of the data if the preventive measures taken are not sufficient to guarantee data protection. The logs must be **kept for at least one year separately from the system in which the personal data is processed** and access must be restricted. This logging and storage duty will be challenging in practice and was heavily criticised in the public consultation but remains in place.

Similarly, private controllers and data processors are obliged to issue and regularly update **regulations for automated data processing** if they process particularly sensitive personal data on a large scale by automated means or carry out high-risk profiling. Such regulations must include information on the internal organisation, the data processing and the measures to ensure data protection.

WHAT SHOULD YOUR NEXT STEPS BE?

Companies subject to Swiss data protection law should **review all their data processing** activities (e.g., review and, if need be, carry out a comprehensive data mapping exercise) to identify gaps and any need for adaption in view of the new law which will enter into force on 1 September 2023.

After that, and subject to the outcome of their analysis, we recommend taking the following **key actions**:

- Review and adjust **data protection governance** (e.g., organisational measures, internal policies, responsibilities within the organisations), where necessary.
- Implement a **data processing register** on all processing activities, if required.
- Assess whether all affected **data subjects are informed** about the processing of their data and, if not, implement or adapt a privacy policy or provide for other notification.
- Assess whether you process sensitive personal data on a large scale by automated means or carry out high-risk profiling, in which case you have a **duty to log** the processing of personal data.
- Take appropriate measures to **provide the data in a machine-readable form** to the data subject, if requested and required.
- Ensure that you can generally **respond to access requests within 30 days**.
- Assess whether the **data security measures are still sufficient**, with a particular focus on technical measures.
- Implement a **process and establish clear responsibilities for reporting and handling data breaches** and, if there is a data breach, store the respective documentation for at least two years. Ensure that you can provide the information required to **comply with potential notification obligations**.
- If you **transfer data abroad** (within your group or to a third party), review the list of countries that provide an **adequate level of data protection** in the annex of the revDPO and, should you transfer data to a country which is not included in the list, ensure that you have **sufficient safeguards** for such transfer in place, such as SCCs or binding corporate rules (BCRs) for group-internal transfers, supplemented by additional measures, if required.
- Introduce a process to assess whether and in what cases **data protection impact assessments** are required to be conducted and to store such assessment for two years.
- Implement **regulations for automated data processing** if you process particularly sensitive data on a large scale by automated means or if you carry out high-risk profiling.
- Appoint a **Swiss representative** if you are domiciled outside of Switzerland and the revDPA applies to you.
- Possibly appoint a **data protection advisor** (i.e., data protection officer) and ensure that he or she has the necessary expertise, resources and access and reporting rights and is independent.

AUTHORS

Rehana Harasgama
Senior Associate
T: +41 58 261 54 51
rehana.harasgama@baerkarrer.ch

Rehana Harasgama is an expert in domestic and international data, cybersecurity and data protection law and advises clients on complex data protection and privacy questions, such as major cross-border disclosures, the implementation of privacy-by-design in new business models, the implementation of data breach response plans and the handling of employee personal data.

Christian Kunz
Partner
T: +41 58 261 52 66
christian.kunz@baerkarrer.ch

Christian Kunz advises clients on data, data protection, cybersecurity and technology law, including (cloud) outsourcings, international data transfers, data breach incident management, data-driven business models and platform solutions (XaaS, IoT, digital marketplaces) and advanced technology projects (AI, Big Data, Metaverse, NFT, blockchain / DLT). He also conducts large-scale internal investigations and e-discovery projects.

FURTHER CONTRIBUTORS

Corrado Rampini
Partner
T: +41 58 261 52 83
corrado.rampini@baerkarrer.ch

Fanny Siegwart
Student Trainee
T: +41 58 261 53 84
fanny.siegwart@baerkarrer.ch

Jana Hesske
Student Trainee
T: +41 58 261 53 72
jana.hesske@baerkarrer.ch