BÄR & KARRER

BRIEFING MARCH 2023

REVISED SWISS DATA PROTECTION ACT: NOT READY YET? HERE'S YOUR GUIDE.

As widely known, the revised Swiss Federal Data Protection Act („revFADP") will enter into force on 1 September 2023, and there will be no grace period. As a result, if you or your organisation process personal data in Switzerland, you have five months to implement the new requirements in your organisation.

Swiss organisations are at different stages of implementing the new requirements. If your organisation has done little to nothing to date, this briefing will guide you on what you really should do now.

PERFORM DATA MAPPING & GAP ANALYSIS

As a starting point, you should review all your data processing activities and, if necessary, perform a comprehensive **data mapping** exercise with your teams or departments and carry out a **gap analysis**.

Data mapping reveals your organisation's **data flows**, including the sources, storage and destinations of personal data. It is a critical component of data protection compliance because it helps your organisation to understand how personal data is collected, processed, and stored and to identify potential privacy risks.

Conducting a gap analysis helps your organisation to assess your level of data protection compliance and to **identify any gaps for remediation** (e.g., missing documents, processes, training etc.) prior to 1 September 2023 when the revFADP enters into force.

Once you have mapped your data flows and carried out a gap analysis, prioritise the steps you need to take according to your highest exposure or risks. In the following, we have listed important action items according to the level of exposure and risks.

REVIEW DATA PROTECTION ORGANISATION

You should review and, where necessary, adjust your general **data protection governance**, such as roles and responsibilities regarding data protection within your organisation, structures, policies and processes.

INFORM DATA SUBJECTS

As the responsible organisation, you will now be required to actively inform your clients, employees and other individuals of **all** processing of their personal data when you collect their data.

You have to inform them **appropriately** about the collection of personal data; 'appropriately' means that information should be provided in a **precise, transparent, comprehensive** and **easily accessible form**.

The information you need to provide is **less comprehensive** than in the EU (identity of controller, purpose of processing, recipients of data and categories of data). However, contrary to the EU, you must provide a **list of recipient countries and, where necessary, guarantees** if you transfer data abroad.

In view of the extended duty to inform, you should **review** and, where necessary, **adapt** your **privacy policies, privacy notices, employee handbooks, general terms and conditions** and other means you use to inform individuals of your processing activities.

Exceptions apply, among others, if the individual already has the information (no need to reinform individuals), the information would defeat the purpose of processing (e.g., in connection with ongoing legal proceedings or internal investigations) or the controller is a private person and bound by a legal obligation to secrecy.

REVIEW OUTSOURCING AND CROSS-BORDER DATA TRANSFERS

Under the revFADP, your organisation can be fined if you do not comply with the requirements for outsourcing data processing activities or cross-border data transfers.
If you outsource certain data processing activities to third parties (so-called „processors") within or outside your group, you should review whether you have signed the necessary agreements (so-called **„data processing agreements"**), the third party has implemented **appropriate data security measures** and you have obtained **consent, if necessary**, due to statutory or contractual confidentiality obligations. The data processing agreement should also provide a mechanism for your prior (general with objection right or individual) **approval of sub-processors**.

If you transfer data abroad (within your group or to a third party), you should **review the recipients of the data and whether they are located in a country which is on the list of countries** that provide an **adequate level of data protection**. You will find such list in the annex of the revised Swiss Federal Data Protection Ordinance (**„revOFADP"**). These include, for example, all EU member states, the United Kingdom, Israel and to a certain extent Canada.

Should you transfer data to a country which is not included in the list (e.g., USA, China and India), you need to ensure that you have **sufficient safeguards** for such transfer in place, such as the revised EU standard contractual clauses amended to comply with Swiss law (**„SCCs"**) or binding corporate rules (**„BCRs"**) for group-internal transfers.

However, you cannot simply sign the SCCs. You must generally conduct a **data transfer impact assessment (DTIA)** to ensure the requirements of the SCCs can be met and if not, what supplementary measures to implement.

In individual cases, you can also rely on the explicit consent of the affected individual or contractual necessity to share personal data with recipients in countries such as the USA, China and India.

ASSESS DATA SECURITY MEASURES

You should assess whether your organisation's current **data security measures (in particular those of a technical nature)** are still **sufficient and comply with the requirements set out in the revOFADP** (e.g., access control, user control, system security, disclosure control).

To determine the appropriate level of protection, the kind of **data, purpose, scope and means of processed data** should be taken into account.

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

ENSURE REPORTING OF DATA BREACHES

Under the revFADP, you as the responsible organisation must notify the **Federal Data Protection and Information Commissioner („FDPIC") as soon as possible** of a data breach that is likely to result in a **high risk** to the person whose data has been breached. This may be the case but is not limited to if there is a high risk of identity theft, if a large volume of data or sensitive data has been compromised, if children's data is affected, etc.

You must also inform the **affected individual** if this is necessary for his or her protection, e.g., if credit cards need to be blocked, passwords need to be changed or banks need to be informed, or if the FDPIC so requests. Contrary hereto,

under the GDPR, the affected individual must be informed if the breach is likely to result in a high risk to such individual or if the competent DPA so requests.

Exceptions to the duty to notify the individual (but not the FDPIC) apply, among others, if prevailing interests of third parties or a statutory duty of secrecy prohibit a reporting, if a reporting is impossible or requires disproportionate efforts, or if the affected individuals are informed by a public announcement.

Therefore, your organisation needs to **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**.

You should also review whether you are subject to other notification obligations for security incidents, e.g., under financial regulatory law or due to contractual obligations. These obligations should also be included in your data breach response plan.

REVIEW YOUR PROCESSES TO ANSWER DATA SUBJECT REQUESTS

In addition to the already existing data protection rights such as the **right to information/access, the right to correction and the right to deletion of data**, the revFADP introduces the **right to data portability**. Under this right, individuals can request to receive their data in a commonly used and machine-readable format from your organisation, so that they can transmit it to a different company or otherwise use the data. This right only applies in certain cases.

This new right gives your organisation the opportunity to **review and update your processes to answer requests you receive from individuals**. You should ensure that when you receive a request to access, correct or delete data or a data portability request: (i) you **confirm the receipt** of the request, (ii) you have **defined internal responsibilities** to answer such requests, (iii) your processes are set up in a way to ensure you can generally **answer access and data portability rights within the 30-day time limit** given by law.

ESTABLISH A DATA PROCESSING REGISTER

Under the revFADP, you are obliged to **establish and maintain a comprehensive data processing register** covering all your processing activities.

Such register needs to describe the purpose of the processing, the categories of the data subjects, the processed personal data and the recipients, in case of cross-border transfers, the recipient countries and guarantees; and if possible, it should also cover the storage period or the criteria to determine the storage period, as well as the data security measures.

Exceptions apply if your organisation employs **fewer than 250 employees**, and the processing entails a low risk of infringing the personality of the individuals.

OTHER STEPS

Other changes that the revFADP will bring such as the obligation to carry out data protection impact assessments (risk analyses) for high-risk processing activities as well as the implementation of further policies (e.g., archiving policy, access management policy etc.), processes and training for employees can then be actioned at a later stage.

Please also refer to our past briefings Update: The Revised Federal Act on Data Protection – Get Ready Now and The New Swiss Data Protection Law – Implementing Provisions Adopted. These describe the changes under the revFADP in further detail and provide an in-depth insight of the requirements entering in to force on 1 September 2023.

AUTHORS

Dr. Christian Kunz
Partner /
Data Protection Expert
T: +41 58 261 52 66
christian.kunz@baerkarrer.ch

Christian Kunz is an expert in data, data protection, cybersecurity, and technology law. He advises clients on the development and implementation of data strategies and data protection-related processes, the use and monetization of data, (cloud) outsourcings, international data transfers, data disclosure requests, and data breach incident management and recovery. He also advises on data-driven business models and platform solutions (XaaS, cloud services, IoT) and advanced technology projects.

Dr. Rehana Harasgama
Senior Associate /
Data Protection Expert
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. She also advises clients on developing data-driven products and services as well as data access, ownership and monetisation within their business.

FURTHER CONTACTS

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

Dr. Jonas Bornhauser
Counsel
T: +41 58 261 54 13
jonas.bornhauser@baerkarrer.ch

Martina Athanas
Counsel
T: +41 58 261 54 24
martina.athanas@baerkarrer.ch

Dr. Christine Schweikard
Associate
T: +41 58 261 53 46
christine.schweikard@baerkarrer.ch