Regulatory Alert 3/2021
Revised Swiss Data Protection Act

Geneva, 19.01.2021

1. References

1.1 Legislation

On 25 September 2020, the Swiss Parliament adopted the revision of the Swiss Data Protection Act (in the following: revDPA).

> Revised Federal Act on Data Protection, available at: https://www.parlament.ch/centers/eparl/curia/2017/20170059/Schluzssabstimmungstext%203%20NS%20D.pdf (in German) and https://www.admin.ch/opc/fr/federal-gazette/2020/7397.pdf (in French)

The Federal Council will decide on the entry into force of the revDPA at a later stage; it is however expected to come into force not earlier than 2022.

1.2 Reference texts

> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2017 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or GDPR)
> Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (amended Convention 108) of 10 October 2018
> FINMA Circular 2018/3, Outsourcing – banks and insurers
> BRP Alert EU 9/2020 & Alert US 1/2020 on the CJEU decision on the validity of standard contractual clauses and the EU-US Privacy Shield, 14.08.2020
> BRP Alerte Réglementaire 14/2020 (Communication FINMA 05_2020 sur les cyberattaques)
> BRP News 15/2018 (Transmission au DoJ de la Leaver List)

2. Context

After three years of parliamentary consultations, the revised Swiss Data Protection Act was adopted by the two chambers of the Parliament on 25 September 2020. The revision of the Act, which dated from 1992, aims at bringing the law in line with technological developments and the evolution of international data protection standards, in particular the EU GDPR (in view of the required adequacy decision from the European Commission for data transfers to third countries) and the Council of Europe's amended Convention 108 (whose ratification the Swiss Parliament recently approved). However, it bears mentioning that the revDPA is not a simple copy-paste of the GDPR. Rather, it keeps distinctive features of the old DPA (currently still in force).

3. Content

The following sections present a summary of what will change under the revised Data Protection Act and what will not change. The summary of the key changes also incorporates a short analysis of how the changes relate to the legal situation under the GDPR.

3.3 Key changes

> No more protection of legal entities' data: Contrary to the old DPA, the data of legal entities are no longer protected under the revDPA (Art. 1). This is in line with the GDPR.

> Extraterritorial application: The revDPA introduces an explicit provision on the territorial scope of application of the revDPA. According to Art. 3 revDPA, the revDPA is applicable to "situations which have an impact in Switzerland, even if they originate abroad" ("*Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst wurden*"). This formulation codifies the already applicable approach towards the (extra-) territorial application of the old DPA. It is commonly accepted that the term "impact" relates to a potential or real interference with the personality rights of a concerned person in Switzerland, while the impact must be of sufficient weight, excluding purely isolated cases.

> Introduction of new definitions: Art. 5 revDPA introduces new concepts, like the concepts of "profiling", "high-risk profiling" and "processor" Furthermore, the new law extends the definition of "sensitive data" which covers now also biometrical data for identifying a person. Voice and facial client's recognition data will therefore fall within the scope of the law, which was not the case before (PFPDT Rapport d'activité 2019/2020, p. 40, BRP AR 23/2020). Last but not least, the concept of "controller of a data file (maître du fichier)" has been replaced by the concept of "data controller".

> Greater information duties of data controllers: The information duties have been considerably increased for private data controllers in Art. 19 revDPA. While under the old DPA, an information duty towards the data subject only existed in case the data controller collected sensitive personal data or in case of personality profiles, the revDPA will impose information duties for the collection of *all* personal data, unless an exception applies (Art. 20 revDPA). Among the different exceptions, it is worth mentioning the first two ones: a) the person already has the corresponding information (e.g. the person has already given its consent through the acceptance of general terms of business (Message du Conseil Fédéral (CF), FF 2017 p. 6670); b) the processing of personal data is provided for by law (e.g. AML regulation (Message du CF, FF 2017 p. 6671). The required minimum content of the information duty is in general less extensive than the content of the information duty under the GDPR; however, in case the personal data will be transferred abroad, the countries of destination must be named, as well as the data protection safeguards applicable or the existence of an exception covering the transfer of the personal data abroad. The revDPA provides for a longer list of exceptions from the information duty than the GDPR.

> New data subject's rights: Data subject's rights are regulated more comprehensively in the revDPA, even though not all rights available to data subjects are new. This is in particular the case for the right to rectification and right to erasure ("right to be forgotten"), which already existed under the old DPA, explicitly or implicitly (in the case of the right to erasure as expression of the principle of proportionality).
  - However, new is the right of the data subject to be informed by the data controller in the case of automated decision-making having legal effects or significantly affecting the data subject (Art. 21 revDPA). This could be the case of decisions which have a tax impact for the client (Message du CF, FF 2017 p. 6674 by analogy). In this case, the affected data subject must be informed and, upon request, given the possibility to express his/her point of view and have the automated decision reviewed by a person. This is less strict than under the GDPR, where automated decision-making is allowed only under strict conditions and is accompanied by strict information duties.
  - New in the revDPA is also the right to data portability (i.e. the right of the data subject to receive his/her personal data, which the data subject provided to the data controller, in a commonly used electronic format and to request that the data controller transfer this personal data to another data controller unless this constitutes a disproportionate effort), which is largely in line with the corresponding right to under the GDPR. This right could have an important impact for financial intermediaries because the client could decide to transfer his/her personal data (client's file) to another services provider.

> Controller and processor: New in the revDPA is also the key terminology of "controller" and "processor", which has been "imported" from the GDPR. In this sense, a controller is any private person or federal organ that, on its own or together with others, determines the purpose and the means of data processing, while a processor is any private person or federal organ that processes personal data on behalf of a controller. However, this change in terminology does not entail any substantive changes to the legal situation prevailing under the old DPA. Any controller mandating a data processor must, as before, ensure that the data processor processes data only in a way as the controller would be allowed to do and that no statutory or contractual duties of secrecy prohibit the transfer of personal data (Art. 9 revDPA). This is less restrictive than under the GDPR, where any processing on behalf of a controller must be governed by a contractual agreement or legal act that contains a list of minimum requirements. For banks and other financial entities, these requirements do not constitute an issue since financial regulation on outsourcing is more restrictive.

> Extended governance rules: New or extended governance rules in the revDPA include:
  - The duty of both data controller and data processor to keep a register of their data processing activities (Art. 12 revDPA). This duty will replace the duty under the old DPA to keep registers of data procession activities which, under certain circumstances, had to be notified to the Federal Data Protection and Information Commissioner ("FDPIC"). Exceptions from the duty to keep a data processing register will apply to companies with less than 250 employees where the data processing presents only a low risk for data subjects' personality. This register must not to be

confused with the inventory of outsourced functions required by § 14 of FINMA-Circ. 2018/3 Outsourcing – banks and insurers. The registers required by the revDPA applies with or without delegation. The bank that has outsourced data processing should thus ensure that its registers conform to the requirements of both the revDPA and FINMA-Circular.

- The possibility to appoint a data protection adviser ("Datenschutzberater") (Art. 10 revDPA). Contrary to the GDPR, there is no obligation for private controllers to appoint a data protection adviser. However, if a data controller appoints such data protection adviser, it must ensure that the data protection adviser has the necessary means and independence to exercise its position, notify the data protection adviser to the FDPIC and include its contact details in the privacy notice.
- Duty to notify data breaches (Art. 24 revDPA): The revDPA introduces a new duty to notify data breaches to the FDPIC in case the data breach is likely to lead to a high risk for the personality or the fundamental rights of the concerned data subject. A data breach is understood as any breach of data security with the consequence of personal data being lost, deleted, destroyed or altered in an unintentional or unlawful manner or being disclosed to or made accessible to unauthorized persons. Contrary to the GDPR, there is no *de minimis* rule in the revDPA, meaning that even in case only one person is affected, the duty to notify the FDPIC may exist as long as there is a high risk for the person's personality or fundamental rights. Also contrary to the GDPR (where a data breach must normally be notified to the supervisory authority within 72 hours after becoming aware of the data breach), there is no deadline for the notification of a data breach, but such notification to the FDPIC must occur "as soon as possible" and include at least the kind of data breach involved, its consequences and the measures taken or foreseen. Banks must be aware that in case of data leak as a consequence of a cyberattack, the notification of the FDPIC does not replace the obligation to inform FINMA based on FINMA Communication 05/2020 (BRP AR 14/2020).
- Designation of a Swiss representative (Art. 14, 15 revDPA): The revDPA now also requires a private data controller seated or domiciled abroad to designate a representative in Switzerland if the data processing occurs in relation to the offering of goods or services to persons in Switzerland, the data processing is extensive, occurs regularly and creates a high risk for the personality of the concerned persons. These conditions being cumulative, not many foreign entities processing data of persons in Switzerland should be concerned by this new obligation (contrary to a similar obligation under the GDPR for non-EU data controllers to designate a EU representative, which applies under less restrictive conditions). However, should the obligation to designate a Swiss representative exist, the name and contact details of the Swiss representative must be notified to the FDPIC and included in the privacy notice, and the Swiss representative must keep the data processing records foreseen in Art. 12 revDPA.
- Certification: Under Art. 13 revDPA, data controllers and data processors may submit their systems, products and services for evaluation by recognised independent certification organisations (e.g. certification ISO 27001). This extension of the certification to services (Art. 11 of the old DPA only foresees certification of IT

solutions and procedures) has important practical consequences, since it will allow the concerned controllers/processors to avoid the obligation to conduct data protection impact analyses (Art. 22 revDPA).

> Strengthened role of the FDPIC (Art. 49 ff. revDPA): The FDPIC is no longer limited to emitting recommendations, but may now (as any other supervisory authority) start investigations (both on its own motion and upon complaint) into alleged violations of the revDPA. To this aim, it may, if the concerned private person or federal organ fails to comply:

- Request access to all information, documents, data processing records and personal data necessary for the investigation,
- Request access to premises and installations,
- Interview witnesses, or
- Request expert opinions or inspections.

If the FDPIC determines a breach of data protection provisions, it may order a variety of measures, in accordance with administrative procedure law (VwVfG).

> More severe sanctions (Art. 60 ff. revDPA): The revDPA introduces a longer catalogue of punishable intentional penal offences (such as failure to comply with orders and duties related to information or cooperation, violation of conditions under which a transfer of personal data abroad is allowed, etc.) as well as higher fines, which may go up to CHF 250'000 (though this is little compared to possible GDPR fines). Contrary to the GDPR, these fines may only be imposed on individual persons, unless the fine does not exceed CHF 50'000, the breach is committed within a business and the investigation of the responsible person(s) would be disproportionate, in which case the legal entity may be sentenced to pay the fine. The situation of the legal entity is the same as that for financial institutions in case of violation of penal offences contained in market laws (Art. 49 FINMASA). The competency for the prosecution and enforcement of the penal provisions lies with the cantonal authorities.

> General duty of confidentiality (Art. 62 revDPA): Worth mentioning is also the introduction of a new and more general professional duty of confidentiality, which differs from the duty of confidentiality in the old DPA that was limited to certain professionally necessary sensitive data and personality profiles. According to the new general duty of confidentiality, the intentional disclosure of confidential personal data obtained during, and necessary for, the exercise of one's professional activity is punishable by fine of up to CHF 250'000. This offence also includes apprentices and support staff and extends to after the termination of the professional activity or apprenticeship. The notion of confidentiality is to be understood in the same manner as in Art. 321 Swiss Criminal Code (SCC) (breach of professional confidentiality) (Message du CF, FF p. 6717). With respect to the offence of breaching banking secrecy (Art. 47 Banking Act), it is worth mentioning that the offence contained in the revDPA only criminalizes the *intentional* breach of the duty of confidentiality, while Art. 47 Banking Act also punishes the negligent breach of the duty of confidentiality. The question of the competition between Art. 62 revDPA and Art. 321 SCC on one hand, and Art. 47 Banking Act on other side has not been addressed.

3.4 What did not change

> No paradigm shift with respect to the general permissibility of data processing by private persons: Like the old DPA, the conceptual approach of the revDPA continues to be built on the premise that data processing in principle does not require consent nor another justification or legal basis, unlike under the GDPR, where data processing is only lawful if covered by a legal basis. A justification (consent, overriding private or public interests or legal basis) is only necessary under the revDPA if the processing principles (Art. 6 and 8 revDPA) are not respected, the concerned person has explicitly disagreed with the data processing or sensitive personal data are disclosed to third parties (Art. 30 (2) revDPA).

> Disclosure of personal data abroad (Art. 16 ff. revDPA): The cross-border transfer regime remains largely unchanged. Note that the revDPA uses the term "disclosure" instead of "transfer" as in the GDPR; this should however not entail any substantive difference. As before, personal data may be communicated abroad if the legislation of the recipient country offers an adequate level of data protection. This may be based on an adequacy decision taken by the Swiss Federal Council (no longer by the FDPIC, as under the old DPA) or, in the absence of such adequacy decision, based on other tools guaranteeing an adequate level of data protection, such as a public international law treaty, standard contractual clauses authorized or recognized by the FDPIC, binding corporate rules etc. Note that the Swiss-US Privacy Shield may no longer be relied upon as a legal basis to transfer personal data from Switzerland to the US after the FDPIC determined, as a consequence of the CJEU decision on the EU-US Privacy Shield, that the Swiss-US Privacy Shield did no longer present the necessary guarantees for an adequate level of data protection (see our BRP Alert EU 9/2020 & Alert US 1/2020 on the CJEU decision on the validity of standard contractual clauses and the EU-US Privacy Shield, 14.08.2020). Exceptions listed in Art. 17 revDPA correspond in general terms to the exemptions listed in the current Art. 6 DPA. However, some differences exist. We only mention the exception available if the communication of personal data is necessary to defend oneself in courts or before foreign authorities (the current Art. 6 does not foresee the case of defense in front of authorities). The new version is intentionally more permissive (Message du CF, FF 2017 p. 6661). We believe that this change is a consequence of the restrictive decisions of the Swiss Supreme Court prohibiting banks to transfer clients' data to the Department of Justice (DoJ) in the context of the US Program (e.g. BRP AR 15/2018). With this amendment, the transmission to the DoJ would be possible.

3.5 Changes in other laws

With the adoption of the revDPA, Parliament amended about 100 other laws. We limit ourselves to presenting here the most significant changes impacting financial institutions.

> The most significant change concerns Art. 23 FINMASA. The amended article introduces two important rights for FINMA with respect to data processing:
  - FINMA is allowed not only to process itself personal data but may now also delegate the processing to third parties. In its message, the Federal Council stated that "the data processing may be outsourced to specialized agents", which can be delegated persons submitted to the duty of secrecy based on Art. 14, or even to persons not submitted to this obligation (Message du CF, FF 2017 p. 6765).

- FINMA will now also be allowed to undertake profiling. As explained by the Federal Council, FINMA should be permitted to undertake profiling in order to discover potentially unlawful behaviour (such as insider trading or market abuse) among the significant amount of data it receives from supervised institutions and third parties. This amendment is significant because it could completely change the way FINMA supervises persons. The regulator could move from a passive supervision approach (reaction in case of reception of a negative information) to an active supervisory approach (dynamic detection of possible abusive behaviours).

> The second change we would like to highlight is the introduction of a new Art. 179*decies* SCC. This criminal offence is intended to punish persons who usurp the identity of someone else ("identity theft/fraud") by using that person's name, picture, personal or professional data, IP address, account number, user name etc. While this new offence is particularly relevant and timely in view of the developments of e-commerce, e-banking and social media, it is not limited to identity theft or fraud committed on the web or on social media platforms (Message du CF, FF p. 6741f.)

4. Comment

Although the new law introduces many additional obligations and rights, the most significant change concerns the modification of the nature of the law itself. Until now, the DPA has been a predominantly civil law act. With the in-depth change of the role of the FDPIC which can now initiate administrative enquiries and decide measures, the revDPA has become a predominantly administrative law act. This change is also perceivable in the treatment of a request to stop the transmission of data abroad if it is considered that the transmission would violate Art. 16 and 17 revDPA. Until now, the request had to be submitted to a civil court (many cases occurred in the last years related to the US Program, e.g. BRP News 12/2017). Art. 51 revDTA now gives this competence to the FDPIC and submits the procedure to the administrative procedure law (Art. 52 revDTA).

All in all, it can be said that Switzerland has made a decisive step towards the modernisation of its data protection law and the strengthening of individuals' data protection. In the eyes of some data protection experts, the Parliament has overall succeeded in bringing the Swiss data protection framework closer to the European framework – an important condition for securing a (hopefully) continued adequacy decision of the European Commission – all the while not engaging in a pure copy-paste of the GDPR and taking at times more measured approaches towards certain concepts and obligations. At the same time, there are some "Swiss finishes" in the revised Act, and some of the approaches taken (e.g. with respect to the data protection adviser) are missed opportunities. Then again, the imposition of personal (criminal) responsibility of individuals seems exceedingly harsh (in particular since not only members of management are likely to be covered by this liability) and raises the question how many employees will be willing to assume such a personal liability risk.

What is clear is that the importance of data protection will continue to increase, and companies doing business in Switzerland and processing personal data in this context can no longer afford to adopt a cavalier attitude towards data protection. The good news is that those companies

that are already GDPR-compliant will find it rather easy to adapt their privacy policies and procedures to the revised DPA for when the latter enters into force. For any company that is not yet GDPR-compliant (but whose data processing operations might be covered by the GDPR), this could be a good moment to consider "shifting gears" to privacy policies and procedures that have the potential to be both GDPR and revDPA-compliant.

5. Practical implication

Legal and compliance functions of Swiss entities should be aware of the upcoming legal changes and inform their management accordingly so that all necessary steps can be taken for their privacy policies and processes to be brought into compliance with the revDPA once the latter enters into force (not before 2022).

In particular, they should undertake the following steps (see also Annex below):

- Review privacy policies and notices for compliance with the revDPA for data concerning prospects/clients and employees;
- Establish the necessary internal processes to address data subjects' requests in accordance with the increased information duties;
- Keep register of data processing activities;
- Review outsourcing data processing agreements for their conformity with the revDPA and amend agreements as necessary;
- Ensure security of personal data and data breach notification processes in compliance with revDPA;
- Ensure transfers of personal data out of Switzerland are made in compliance with the revDPA.

Swiss bank and other financial intermediaries that have EU clients and have not yet established GDPR-compliant processes may also wish to consider to "kill two birds with one stone" and take the necessary steps to render their data processing operations, to the extent possible, both revDPA and GDPR-compliant.

We are at your disposal for any questions you may have.

Best Regards,

BRP Bizzozero & Partners SA

ANNEX

	Obligation	Legal basis	Comment	Deadline
Privacy policies	> Review/update privacy policy, setting out data subjects' rights and controllers/processors' obligations under the revDPA	Art. 19 ff. revDPA		As soon as possible
Agreements with clients	> Include privacy policy or a mention in the agreement where the client may find the privacy policy > Request consent for sharing of personal data with external data processors to avoid breach of banking secrecy (see also outsourcing)	Art. 19 ff. revDPA; Art. 47 Banking Act		By entry into force
Internal processes for responding to data subjects' information requests	> Establish adequate internal processes to address data subjects' requests in compliance with extended information duties > Ensure data portability is possible if requested	Art. 25 ff. revDPA		By entry into force
Outsourcing data processing agreements	> Review outsourcing data processing agreements for their conformity with the revDPA and amend agreements as necessary > Ensure the processor is able to safeguard security of personal data > Agree on information and assistance duties of the data processor in case of data breach	Art. 9 revDPA		By entry into force

Website	> Make updated privacy notice available	Art. 19 ff. revDPA		By entry into force
Internal set-up	> Assess and itemize/register which kind of personal data are processed (including which personal data is considered sensitive) and for which purpose > Ensure personal data is deleted if no longer required > Establish/keep register of data processing operations > Consider appointing a data protection advisor > Designate contact person for communications with the FDPIC and FINMA > Establish incident response plan with roles and responsibilities in case of data breach (see also data security) > Ensure data protection by design and data protection by default > Undertake data protection impact assessments where required by law >	Art. 6 (3) revDPA; Art. 7 revDPA; Art. 8 revDPA; Art. 10 revDPA Art. 12 revDPA; Art. 22 revDPA; FINMA-Circular 2018/3 Outsourcing-Banks and Insurer;		By entry into force
Transfer of personal data abroad	> Review all external data flows > Identify the applicable legal bases for the transfers > Stop the transfer immediately if the bank transfers data to the US and the only legal basis is the	Art. 16 ff revDPA	See BRP Alert EU 9/2020 & Alert US 1/2020 (CJEU decision on the validity of standard contractual	For data transfers to the US: immediately if the transfer is based on the Swiss-US Privacy Shield;

	Swiss-US Privacy Shield		clauses and the EU-US Privacy Shield)	Otherwise: by entry into force
Security of personal data	> Take all necessary appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing > Define access rights to data files > In case of data breach: • Establish communication channels with one dedicated contact point • Make data breach notifications to FDPIC and concerned data subject(s) as required by law • Have business continuation plan in place	Art. 8, 24 revDPA		As soon as possible
Training of staff	> Training of staff for the case of data breach (whether cyberattack or not)	Art. 8 revDPA		As soon as possible
Certification	> Consider certification of IT systems and/or the services	Art. 13 revDPA		By entry into force