Documentation of data processing activities under the revised Swiss Federal Act on Data Protection

- The revised Swiss Federal Act on Data Protection ("**RDPA**") will govern the processing of personal data by private companies in Switzerland as well as those established abroad whose personal data processing activities have an effect in Switzerland.
- Companies will need to identify their processing activities and maintain a record of processing activities ("**ROPA**"). Companies with less than 250 employees and carrying out processing activities with limited risks will be exempted from this requirement.
- If the processing of personal data by a company entails an elevated risk of infringing privacy or fundamental rights, a data protection impact assessment ("**DPIA**") will need to be conducted.
- The RDPA provides a new set of criminal sanctions, e.g. a personal fine of up to CHF 250,000.
- The RDPA does not provide for a transitional period. Companies will need to comply with its new requirements as of the date of the entry into force of the RDPA.

1 INTRODUCTION

After lengthy discussions over several years, the RDPA was finally adopted by the National Council and the Council of States on 25 September 2020. Due to the on-going revision of the implementing ordinances, the date of entry into force of the RDPA remains open (possibly mid-2022, at the earliest). The RDPA will govern the processing of personal data by private companies in Switzerland as well as those established abroad whose personal data processing activities have an effect in Switzerland.

The goal of the RPDA was mainly to modernize a legislation dated from 1992 and align data protection with the General Data Protection Regulation of the European Union ("**GDPR**"). Processing of personal data by companies (i.e. the data controllers) continue to not require a justification. Only when privacy rights are harmed must companies assert a justification so that the processing is not qualified as unlawful. Personal data of legal entities will no longer be covered by the RDPA and they face new obligations (broadened duty to provide information, duty to report personal data breaches, duty for controllers abroad to designate a Swiss representative

etc.), new rights for data subjects (right to data portability) as well as stricter sanctions (personal fine of up to CHF 250,000). In comparison with the GDPR, the RDPA is more flexible in some respects (e.g. optional designation of a data protection officer for companies) while stricter in others (e.g. duty to inform data subjects of data processing extends to the list of countries to which personal data is transferred to).

More specifically, companies will need to identify their processing activities and maintain inventories of the same (**Section 2**). Companies with less than 250 employees and carrying out processing activities with limited risks of privacy infringements will be exempt from this requirement.

If the processing of personal data by a company entails an elevated risk of infringing privacy or fundamental rights, said company will have to conduct a DPIA[1] on its high-risk data processing activities per Art. 22 RDPA (**Section 3**).

2 DOCUMENTATION OF DATA PROCESSING ACTIVITIES

Data controllers/data processors will have to identify their processing activities and maintain a ROPA.[2]

This documentation process should be carried out as appropriate and based upon the company's size, nature of its business, and the regions/countries where its activities are conducted. This process is an on-going task as data processing risk factors vary over time and are contingent on the types of data that a company may process and the locations where such processes occur.

Per the minimum requirements provided by Art. 12(2) RDPA, a ROPA must include: (i) the name and contact details of the data controller/data processor; (ii) the type of personal data that is processed; (iii) the categories of data subjects that are concerned by the company's processing of personal data; (iv) the type of recipients to which the personal data is transferred; (v) if applicable, the countries in which such recipients are located

[1] Terminology used under Art. 35 of the GDPR.

[2] Terminology used under Art. 30 of the GDPR.

and the means by which cross-border transfers are secured; (vi) the security precautions taken by the company to safeguard the personal data; (vii) the period during which the personal data shall be stored (or the criteria used to determine such period); and (viii) the scope and purposes upon which the processing of the personal data is based.

Best practices would warrant also documenting the risks or incidents related to data processing as well as the decisions and measures implemented by the company for remedying the same as such records will allow the company to demonstrate its compliance with the RDPA and best practices.

3 DATA PROTECTION IMPACT ASSESSMENT

A company's DPIA should consider the company's complexity and the jurisdictions in which it operates. Should a company process personal data in jurisdictions where legislation may not guarantee adequate protection from a data protection standpoint,[3] the DPIA will require a comprehensive mapping and categorisation (i.e. listing, prioritisation and definition) of the potential risks related to such jurisdictions.

Furthermore, the data protection risks that may result from the activities of the entities the company controls directly or indirectly, as well as the activities of the subcontractors or suppliers with which they have an established commercial relationship must be taken into account.

An assessment of each data processing activity against the RDPA's data protection principles must be performed. Art. 6 RDPA provides data protection principles that companies are obliged to comply with when processing personal data, namely that the processing of personal data must be lawful (Art. 6(1) RDPA), comply with the principles of good faith and proportionality (Art. 6(2) RDPA), and may only be collected for determined purposes evident to the data subject (Art. 6(3) RDPA). Personal data should be destroyed or anonymized once it is no longer necessary (Art. 6(4) RDPA) and all appropriate measures must be taken to ensure that

[3] A list of the countries which are deemed to guarantee such adequate protection is available on the Federal Data Protection and Information Commissioner's website here: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html.

incorrect or incomplete data is rectified, erased or destroyed (Art. 6(5) RDPA). In the event that the data subject's consent is required, said consent is only valid if the data subject has freely expressed his consent after having been duly informed (Art. 6(6) RDPA). Additionally, the data subject's consent must be "express"[4] if the processing involves sensitive data, high-risk profiling, or profiling performed by a federal body (Art. 6(7) RDPA).

If a data process does not comply with the RDPA's principles, a remedial measure must be proposed for adapting such activity in order for it to comply with the data processing principles. If not essential and prone to data protection risks, a company's activity must for instance be reduced geographically or in time or terminated.

At a final stage, the DPIA must provide adequate measures capable of preventing and mitigating the risks identified as well as identifying future risks. To this end, the DPIA's conclusion report should contain (i) a mapping of the company's data protection risks; (ii) regular evaluation procedures of the company's subsidiaries, subcontractors and suppliers; (iii) adequate actions to mitigate the data protection risks identified and prevent potential future risks; (iv) an alert mechanism; and (v) a roadmap for monitoring the implementation and effectiveness of the proposed measures.

It is only once all high-risk data processing activities, if any, have been identified and categorised that a company may begin implementing its data protection management system. Thereafter, a DPIA, if required, should be conducted on an ongoing basis as the risks already identified may evolve with time or additional risks may develop.

4 ENFORCEMENT AND SANCTIONS

The Federal Data Protection and Information Commissioner ("**FDPIC**") has been granted broadened enforcement powers (Art. 49 ff RDPA). With the RDPA, the FDPIC will be enabled to (i) investigate suspected non-

[4] The term "express" is synonym with "explicit" and refers to a declaration formulated orally or in writing resulting directly from the words used. Consent may be "express", by way of example, by ticking a box (but may not be implicit).

compliance *ex officio* or further to a complaint and (ii) issue binding orders (to restrict, change or stop data processing activities).

The RDPA also provides new criminal sanctions, e.g. a personal fine of up to CHF 250,000 (Art. 60 ff RDPA), in case of breach of certain duties (e.g. duty to provide information). Companies can however be fined in cases where the offence sanctioned with a fine of up to CHF 50,000 would require disproportionate efforts to identify the liable person within the company. Cantonal criminal authorities remain responsible for enforcing such sanctions. Furthermore, civil claims are still possible in accordance with Art. 28 ff Swiss Civil Code. However, the RDPA does not provide for any specific sanctions with regard to the duties related to a company's ROPA or DPIA (described under Sections 2 and 3 above).

5 DEADLINE FOR COMPLIANCE WITH THE RDPA

The RDPA does not provide for a transitional period. Although the RDPA will not apply retroactively to the processing of personal data prior to its entry into force (Art. 69 RDPA), companies will need to properly document their data processing activities and possibly their DPIA as of the date of the entry into force of the RDPA.

Contact the authors:

Simone Nadelhofer, Partner, snadelhofer@lalive.law

Daniel Lucien Bühr, Partner, dbuhr@lalive.law

Tatiana Jullier, Associate, tjullier@lalive.law

Warren Martin, Associate, wmartin@lalive.law