walderwyss attorneys at law

Walder Wyss Ltd.
Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

Telephone +41 58 658 58 58
Telefax +41 58 658 59 59
www.walderwyss.com

Revised DPA and GDPR

Data protection compliance implementation

230310/V017

The revised Swiss Federal Data Protection Act ("revDPA") was adopted on 25 September 2020 and will **come into force on 1 September 2023**, along with the revised Ordinance to the DPA ("revDPO").

The implementation of the revDPA requires planning. It is only effective if it takes account of the activities and structure as well as the risks and needs of a company – one-size-fits-all is the wrong approach here. Rather, the implementation must consider the **specific circumstances.**

These include the scope and the complexity of the business activities of the company or companies, the importance of data processing for the company's business model, but also the sensitivity of the personal data processed and the applicability of regulatory or sectoral data protection provisions. The importance of reputation for the company and the expectations of the public and authorities are also of significance. Finally, it is important to consider the complexity of the company's IT landscape and the existing processes and their documentation, especially in the areas of goods production, services and sales, IT, HR and marketing.

«Compliance» is not an end in itself, but rather the requirement to recognise and understand risks for the data subjects and to deal with them appropriately and consciously. This is an ongoing task.

The **first and most important steps** are often possible with relatively little effort. This is particularly true if work has already been done to implement the EU General Data Protection Regulation («GDPR»). This document therefore contains information on the most important steps for companies that are at the beginning of the implementation process and on work that is required in addition to the implementation of the GDPR.

We recommend the following initial or key measures to companies that are beginning to implement the GDPR or the revDPA:

1. Review applicable legal provisions
2. Draft a data protection policy
3. Create records of processing activities
4. Draft privacy notices for products/services, the company's website or for apps, employees and possibly for job applicants
5. Make sure that data security is adequate and proportionate to the risks
6. Draft data processing agreements for customers where the company provides services in the IT sector or otherwise acts as a processor

We help clients with a comprehensive toolbox of instructions, checklists and templates that control and reduce effort, time and costs.

This document is also available in German and French.

Planning questions

The implementation of the GDPR and the revDPA is not necessarily costly or time-consuming but requires planning – if only for reasons of budgeting and reporting. Checklists and other materials are available as planning aids. What is important is not completeness, but a concrete idea of the approach so that companies can react appropriately to changes and delays.

1 *Project scope and project subject*

The implementation project and its scope and subject must be planned.

The key questions here are, for example, whether we are dealing with a (partially) group-wide implementation or implementation by individual companies, whether only overall participations or also majority and minority participations are to be included, and whether group companies must participate or are merely involved via recommendations and assistance. Next, the implementation work already carried out on the basis of the GDPR or the current DPA must be taken into account and the project objectives including performance measurement must be determined.

If GDPR implementation is completed: determination of the efforts required to adapt existing documents and processes

In terms of the timetable, the **revDPA** and the **revDPO** enter into force on 1 September 2023. It contains hardly any (relevant) transitional periods. The revDPO contains provisions on data security, the data protection advisor, exceptions for records of processing activities, the information duty and exceptions for rights of data subjects.

For **smaller companies** not involved in high-risk processing of personal data and that are outside the scope of the GDPR, implementation is usually neither time-consuming nor cost-intensive.

2 *Implementation requirements*

1 Key task

It is important to review the relevant legal framework that defines the project objectives. On the one hand, this relates to the GDPR and, if applicable, its implementation law, but also to the group requirements (such as compliance with the GDPR).

Furthermore, it must be examined to what extent the revDPA is applicable, in particular with regard to the international level (territoriality/effects doctrine) as well as the provisions on federal bodies. Finally, sectoral regulations (in Switzerland and/or abroad) raise the question of voluntary application of stricter rules and their scope.

If GDPR implementation is completed: determine additional requirements that may not have been taken into account in the implementation of the GDPR, and decide on the potential voluntary implementation of the GDPR (together with the revDPA) in Switzerland

Some of the implementation law contains stricter requirements, especially in regulated areas (including, where appropriate, professional secrets subject to criminal penalties). In this respect it may be appropriate to actively exclude the applicability of the GDPR (for example by excluding customers from the EEA or the tracking of visitors from the EEA).

In contrast**, voluntary application** of the GDPR often makes sense in the case of integration into a foreign group, for service providers with foreign customers and for providers with a substantial customer base abroad. Voluntary application is often limited (and therefore does not lead to consent requirements that the revDPA does not recognise).

3	*Project approach*	It is also crucial to plan the specific approach of the project. The approach varies according to the circumstances. Particular attention should be paid to the question of whether to aim for central control or to leave it at assistance and resources for the individual companies or divisions and also let them bear the responsibility for implementation. The most important support services must be planned and the internal project sponsoring as well as any external support must be determined. Other important factors are time specifications as well as budgeting, controlling and reporting.	

Functions and responsibilities

Data protection compliance as an ongoing task requires a structure and the knowledge appropriate to the size and complexity of a company. However, there is no legal requirement for a separate specialised unit or dedicated function for data protection, with the exception of the appointment of a data protection officer (DPO) within the scope of the GDPR for certain more sensitive data processing activities. The revDPA does not require appointment of a DPO, but provides for a data protection advisor, whose appointment is purely voluntary.

Both the GDPR and the revDPA provide, under certain conditions, for a local representation of a company outside the EEA or Switzerland.

4	*Intra-group functions*	Central functions, their competencies and responsibilities and their role in implementation must be planned. In addition to a company's own dedicated data protection unit, a company's own data protection expertise in the Legal & Compliance division may be considered and data protection champions or similar functions in group companies or divisions may be created The choice in this respect must be tailored to the complexity and the degree of centralisation as well as the available competences and capacities .	**If GDPR implementation is completed**: review the group functions' knowledge and capabilities with regard to the revDPA, where required, or establish a relationship with external advisors
5	*Data protection officer (DPO in accordance with the GDPR)*	It must be determined whether a **data protection officer** (DPO) must or should be appointed under the GDPR. Such appointment is determined in accordance with the GDPR and local implementation law, which in some cases, such as e.g. in Germany, has stricter requirements. In addition to the selection and appointment process of the DPO, reporting must be planned and roles and responsibilities clearly defined. This may also require adaptations of the	**If GDPR implementation is completed**: assess the appointment of the DPO as a data protection advisor (see section 6 below)

records of processing activities, privacy notices and existing processes. Specifically, for example, the involvement of the DPO, e.g. in data protection impact assessments (DPIA), must be specified.

An **external** body can be appointed as the DPO, whereby legal entities are also considered for this purpose according to not uncontroversial practice.

6 *Data protection advisor (in accordance with the revDPA)*

According to the revDPA, there is no appointment obligation. Nevertheless, a **voluntary appointment** may be worthwhile, especially for companies with riskier processing activities. Here, too, care must be taken to ensure that, in addition to the selection and appointment process of the data protection advisor, reporting is planned and roles and responsibilities are clearly defined. This may also require adaptations of the records of processing activities, privacy notices and existing processes.

Specifically, for example, the involvement of the data protection advisor in **data protection impact assessments** ("DPIA") must be specified. Although the appointment of the data protection advisor is voluntary, the correct appointment exempts the data protection advisor from the obligation to report high net risks in a DPIA to the FDPIC (cf. Section 21).

If GDPR implementation is completed: consider appointing an independent data protection advisor

Certain requirements with respect to **independence** apply: the data protection advisor should not have executive functions. It is possible for the DPO to simultaneously act as data protection advisor if the DPO has sufficient knowledge or access to it.

An **external body** - including legal entities, amongst others - may also be considered as data protection advisor.

7 *EU and UK representative*

For companies that fall under the GDPR but are not established in the EEA or the UK, the EU or UK representative is a local contact person for authorities and data subjects. Here, too, it is important to review the appointment obligation. In the event of an appointment of an EU or UK representative, adaptations of privacy notices and of the records of processing activities and its processes must be made, such as the receipt of copies for the attention of the EU representative.

If GDPR implementation is completed: consider appointing an EU representative

An appointment obligation exists if the GDPR is applicable according to Article 3(2) (i.e. in the case of market orientation or monitoring of data subjects' behaviour), provided that the corresponding data processing is not only occasional and/or special categories of data are processed extensively and/or the processing leads to an increased risk.

The EU representative must be in an EEA state where the persons addressed or monitored are located. The EU representative may be a natural person or legal entity. The same applies to the territory of the United Kingdom under the UK GDPR.

8	*Swiss representative*	The Swiss representative is also a local contact person for the FDPIC and data subjects in Switzerland. The Swiss representative is tailored to companies established abroad but subject to the revDPA. Here, too, the appointment obligation must be reviewed. An appointment makes adaptations of privacy notices necessary, but not necessarily of the records of processing activities. An appointment obligation exists if the controller is based abroad and under the following conditions: (i) data relating to individuals in Switzerland is processed; the processing is (ii) connected with the offering of goods or services to these individuals or the monitoring of their behaviour; (iii) it is **extensive and done on a regular basis** and (iv) involves a **high risk** for the data subjects.	**If GDPR implementation is completed**: consider appointing a Swiss representative (e.g. a group company that is established in Switzerland) The Swiss representative may be a natural person or legal entity including a law firm.

Documentation

Under the GDPR, the controller must be able to prove that and how he complies with the GDPR ("accountability"). Any violation is subject to sanctions. The revDPA has no general accountability obligation, but documentation is necessary to a certain extent, especially in the form of records of processing activities.

9	*Documentation in general*	A **central recording** of data protection-relevant actions and events makes sense and may be mandatory. This includes, for example, records of processing activities, guidelines and other documentation, legitimate interest assessments, data protection impact assessments (DPIA) and follow-up actions, data protection breaches and responses, reference to data security measures (TOMs), third-party and contract management, data subject requests (all/escalated), intra-group data processing, joint controller and third-party disclosure circumstances, data disclosure to third countries, if necessary, with a risk assessment (transfer impact assessment (TIA); cf. section 26), reporting and recommendations by the DPO/data protection advisor; referral to third parties/contract management and contacts with authorities. This documentation can be kept in different ways, such as e.g. in an Excel spreadsheet, in a document via Sharepoint, possibly also in an area of the intranet, in addition, via OneTrust, Confluence,	The revDPA has no genuine accountability obligation. However, a certain amount of documentation is still necessary, as part of governance, but also for reasons of evidence.

etc. The documentation should be user-friendly and enable control of access permissions.

10 *Regulations, policies, guidance*

2 Key task

Some instructions are necessary under the accountability principle, but also as a data security measure and as part of the responsibility of a company and its management bodies. However, the circumstances matter, and unnecessary rules and instructions should be avoided. **Data protection policies** such as e.g. a code of conduct or a directive may be considered and, if necessary, also additional policies, guidelines, fact sheets, implementation aids, etc.

Typical examples are IT policies (which often already exist, and regulate permitted use or monitoring), but also video surveillance, the use of cloud services, HR requirements such as BYOD; CRM and marketing tools and rights of data subjects. Corresponding documents should be adapted to respective needs and only drafted if they are necessary and maintained (cf. section 15). Finally, the implementation, such as an internal sign-off or roll-out, must be planned.

If GDPR implementation is completed: review and, if necessary, adaptation of existing regulations

Deviations from regulations based on the GDPR are very likely. What is required is a **review and, if necessary, an adaptation** to Switzerland or to the revDPA.

Formal enactment of policies by the bodies or agencies responsible for Swiss companies is also required.

Records of processing activities

The record of processing activities is an inventory in which the various processing activities are recorded with certain minimum details. It is mandatory according to both the GDPR and the revDPA and can often be a valuable tool for companies. It does not cover IT applications or individual sets of personal data, but rather the various purposes of processing and their essential means.

11 *Technical implementation*

Especially in larger companies or in case of a wide range of data processing activities, a **user-friendly implementation** of the records becomes important. The technical basis to collect and maintain records of processing activities must therefore be assessed (cf. section 9).

If GDPR implementation is completed: use existing systems

12 *Content, design, scope*

In addition to the prescribed minimum content, when it comes to **design** attention must be paid to interfaces to other inventories, such as the application inventory or those of third parties. With regard to the scope, it must be decided whether the minimum content is sufficient or whether further details should be included, such as a threshold value assessment for data protection impact assessments through risk questions.

Finally, the design depends on whether the record is kept by a **controller** or a **processor**.

If GDPR implementation is completed: use existing templates and processes

13 *Initial collection*

3 Key task

At this point, the necessary processes must be planned, i.e. the responsibilities, the responsibility for content, approach and documentation, the involvement of the DPO or data protection advisor, furthermore the validation, time requirements and the documentation of the EU or Swiss representative by providing them with copies.

If necessary, **assistance** should also be prepared, such as training, templates of typical records, written guidance and interviews.

If GDPR implementation is completed: collect records of in-scope processing activities on the basis of existing processes, with adjustments according to responsibilities and capacities in Switzerland

The revDPA has an **obligation to keep records** of processing activities as well. A breach of this obligation is not sanctioned directly, but there is a risk of a lack of evidence, a de facto reversal of the burden of proof in the case of violations and a stricter review in case of other violations.

The GDPR standard also meets the requirements of the revDPA. There is an exception for **SMEs** with respect to creating records of processing activities so long as these have less than 250 employees and do not process sensitive data on a large scale and do not

engage in high-risk profiling. – Federal bodies must notify the FDPIC of their records of processing activities.

14 *Ongoing collection*

Just as important as the initial collection of records is the **ongoing collection** of new types of processing. This includes checking the trigger (new data processing activities, certain changes to existing data processing activities) and planning the corresponding processes (responsibilities, accountability for content, approach, documentation, involvement of the DPO or data protection advisor, copies to the EU/Swiss representative).

In addition, interfaces to other processes must be considered or such interfaces in these processes must be planned, e.g. project approval or budgeting.

If GDPR implementation is completed: use of established processes

The SME exception (cf. section 13) must be observed, as well as any further regulations in the revDPO.

15 *Maintenance*

Existing records must be kept up to date. There is no specific requirement for a dedicated process, but a process for regularly verifying records (e.g. at certain intervals or according to a certain pattern, usually by the body with ultimate responsibility on the business side) is useful, as are random checks, especially for more sensitive data processing activities.

If GDPR implementation is completed: use of established processes

Transparency, information and consent

Both the GDPR and the revDPA require that the controller inform all data subjects about the collection of their personal data and certain additional points. Applicable sector regulation may trigger additional duties to provide information. In addition, consent requirements may apply, in particular under the GDPR, but also under the revDPA and potentially in connection with obligations of secrecy where disclosures are anticipated.

16 *Determine existing privacy notices and data processing*

As a starting point, an understanding of the types of processing and existing data protection information is required. This requires, on the one hand, the collection of information about data processing activities that trigger special information duties (possibly profiling/high risk profiling/automated individual decisions) and, on the other hand, the collection of information about all relevant existing privacy notices and information (also e.g. in general terms and conditions).

If GDPR implementation is completed: ensure the information collected before is up-to-date

The same information should be collected under the revDPA.

17 *Review applicable requirements*

It must also be reviewed where personal data is **specifically collected** or where the controller actively initiates the collection - these processes trigger information duties.

With regard to **consent**, it must be reviewed - depending on the applicable law - whether there is a consent requirement or whether information is sufficient and whether there are additional information and consent requirements under special laws.

Furthermore, in the case of secrets, declarations of release may be required, as well as additional consents when it comes to the disclosure of sensitive personal data.

If GDPR implementation is completed: gather information about deliberate collection of personal data from data subjects in Switzerland and by Swiss companies also abroad

The revDPA also has a general **information duty** when personal data is collected. A violation may be subject to criminal sanctions. The revDPO also recognises a general **data secrecy** which, depending on the circumstances, can lead to a consent or exemption requirement.

18 *Drafting of privacy notices*

4 Key task

The first step is to decide on the approach to be taken, especially if several complementary or overlapping pieces of information come into question. In particular, the initial question is whether to create **group-wide standard privacy notices** with selective additions or deviations or whether to prefer individual privacy notices. Based on

If GDPR implementation is completed: drafting of supplementary and/or adaptation of existing privacy notices (the need for adaptation is usually limited); review of the need for adaptation of general terms and conditions or contract documents

The same questions arise under the revDPA. However, **special features** must be **taken into account**. After all, the revDPA does not require an explicit reference to profiling.

this, the privacy notices are to be drafted or existing ones adapted. Depending on this, special instructions are also required for interfaces with users, such as web shops, contact forms or chatbots. Not only the privacy notices, but also the other documents such as applications, information letters and general terms and conditions should be kept up-to-date.

A **template** for a privacy notice in accordance with the GDPR and the revDPA will soon be available at www.dsat.ch.

In principle, this also applies in the case of a high risk, but in this case a duty of provide information usually arises from the principle of transparency.

In contrast to the GDPR, there are information duties for automated individual decisions, but no consent requirements. It is possible to assign this information duty to third parties, such as a customer.

Certain requirements **go beyond the GDPR** (e.g. individual recipient states/regions must be specified). In addition, further adaptations of privacy notices based on the GDPR are often useful, for example when it comes to references to the applicable law, the legal basis or the rights of data subjects. Finally, further regulations are possible in the revised DPA.

19 *Implementation planning*

During the implementation or **roll-out** of new privacy notices some procedural questions arise, for example the differentiation between existing and new customers or passive vs. active data processing. References to a privacy notice on the internet are generally permissible. This also applies to printed material. However, certain minimum information must be included in the referencing document.

In the case of a roll-out, further questions of implementation arise - e.g. references in the dispatch of order confirmations or invoice inserts or in e-mail signatures, but also a transfer of information duties regarding third parties to a customer in general terms and conditions. Finally, in particular in the case of changes of purpose, the provision of follow-up information should be considered.

If GDPR implementation is completed: planning the provision of revised or new privacy notices and, if necessary, general terms and conditions

The same questions also arise under the revDPA. In particular, it should be noted within the framework of **transitional law** that the information duty applies to data processing with new “collections” after entry into force - this may also apply to existing customers.

Data security

Data security is a key issue but is not regulated in detail in the GDPR and the revDPA. The main requirement is to recognise and assess security risks and to deal with them consciously and responsibly. Specific requirements result above all from recognised standards, industry practice, any special regulations in individual industries and activities and the expectations of customers and partners.

20 *Data security*

5 Key task

Data security is crucial from both a legal and a reputational perspective. The GDPR contains little specific requirements in this respect. Nevertheless, it is advisable to review existing applications and processes for security and related aspects such as data protection by design or data protection by default, to check the completeness of the relevant documentation and to refer to security measures in the records of processing activities.

If GDPR implementation is completed: checking for deviating/special regulatory or sectoral legal requirements

In terms of security requirements, there are not differences between the GDPR and the revDPA. However, the revDPO includes some specific minimum requirements. These include keeping "**processing regulations**" ("Bearbeitungsreglement") and collecting and **collecting log data** for systems that are used for large-scale processing of sensitive data or for high-risk profiling (and keeping log data separate from the productive environment for at least one year). In the event of violation, there may be a risk of criminal sanctions.

21 *Data protection impact assessments*

Data protection impact assessments (DPIAs) are structured and documented assessments of risks and mitigating measures. They may be obligatory in the case of data processing with increased risk and may trigger an obligation to notify the authorities.

When planning DPIAs, **typical data processing activities** of companies that may request a DPIA must be determined first and foremost, as well as any **exceptions** to the obligation to conduct them. In view of transitional law, a **time limit** must then be set for ongoing data processing activities.

In order to prepare the corresponding process, it is necessary to agree on the **trigger** of the DPIA, e.g. information in the records of processing activities, furthermore roles and responsibilities, involvement of the DPO, IT and business as well as completion and - in case of high residual risks - notification of the authorities. With regard to templates, it may be useful to create different templates for simple and complex cases or minimum and optional contents. Finally, careful documentation should be ensured.

If GDPR implementation is completed: checking for deviating or additional requirements

In terms of content, the revDPA contains few specifications and **hardly any deviations** from the requirements of the GDPR. Repeating DPIAs that were carried out under the GDPR is usually not necessary. An exception to the obligation to conduct a DPIA applies in the case of a legal obligation to process data accordingly (for example in the KYC area).

Similarly, in the case of high residual risks, there is an obligation to notify the FDPIC of the data processing, analogous to the GDPR, but only if no independent data protection advisor has been appointed (cf. section 6).

The revDPA provides for an obligation to conduct DPIAs in particular in the case of "**high risk profiling**", large scale processing of sensitive personal data and systematic monitoring of extensive public areas. In addition, conducting a voluntary DPIA – as under the GDPR – is often useful (however, in doing so, the voluntary nature of the DPIA must be documented).

22 *Personal data breaches*

One important issue, which the GDPR does not regulate in great detail, is the handling of personal data breaches. There is, however, an obligation to handle breaches appropriately and, under certain circumstances, to notify the authorities and data subjects thereof. It is therefore advisable to set up or adapt a **process for the handling of personal data breaches** (and any other "incidents"). In particular, this should include an obligation on employees to report personal data breaches, but also a regulation of competencies, responsibilities, contact points and an orderly escalation, as well as an obligation to notify the authorities and data subjects. Personal data breaches must be documented (cf. section 9).

Under the revDPA, personal data breaches must again be handled in a controlled manner, and there may be an **obligation to notify** the FDPIC (but with a higher threshold for doing so than under the GDPR) and possibly also the data subjects of such breaches. Voluntary notification of the FDPIC is possible, but generally not recommended.

Third parties

When working with third parties – primarily suppliers, customers and partners –, the roles of the parties involved determine the requirements. The GDPR and the revDPA define certain roles and attach certain legal consequences to these roles. Data security aspects are also particularly relevant here, and data disclosures to third parties must be recorded in records of processing activities and reflected in privacy notices.

23 *Existing contracts*

The starting point is a **review of existing contracts**, in particular with suppliers and customers, and the definition of the corresponding roles (controller, joint controller, processor).

If GDPR implementation is completed: if necessary, review of further contracts for Switzerland

24 *Suppliers*

In the case of suppliers, the key question arises whether or when a supplier acts as a processor and whether or how a supplier ensures appropriate data security. In order to properly integrate suppliers, adaptations of and addendums to **contracts** may be required, e.g. in the case of data processing without sufficient clauses.

In the event of riskier data processing activities, **vendor assessments** should be defined for suppliers with access to personal data, while a vendor (re-)assessment may have to be carried out for existing suppliers.

Standard data processing agreements in relation to suppliers (i.e. where the company acts as a controller) are usually required. It may be useful to draft supplier contracts or contractual clauses between independent controllers.

Further interactions with suppliers from a data protection perspective should be planned where a supplier is the controller (e.g. notification of erasures, rectifications and restrictions to processing). Recipients or categories of recipients must be stated in the records of processing activities and in privacy notices.

If GDPR implementation is completed: review and, if necessary, adapt supplier contracts according to the same standards

In terms of content, the revDPA does not have more extensive requirements for data processing agreements than the GDPR (although additional requirements may apply to regulated companies, e.g. banks and insurers). The **same measures** are required as under the GDPR. In the event of missing or insufficient data processing agreements the controller may be liable to sanctions.

If suppliers have access to personal data but do not act as processors, a waiver from data/professional secrecy obligations should be checked. Where the company and the supplier work together as joint controllers, the revDPA does not impose higher requirements than the GDPR.

Recipients or categories of recipients must be stated in the records of processing activities and in privacy notices.

25 *Customers*

6 Key task

On the customer side as well, the main question is when the company will act as a **processor** for customers. It is also important here – especially if the company provides IT services – to document adequate data security. The company will often need a standard data processing agreement where it acts as a processor.

Under certain circumstances, a standard agreement between joint controllers may be useful, but it can usually be concluded on an ad hoc basis. Standard contractual provisions with other independent controllers can also be useful.

Further interactions with customers from a data protection perspective should be planned if the company is a controller (e.g. notifications of erasures, rectifications and restrictions to processing).

If GDPR implementation is completed: review and, if necessary, adaptation of customer contracts according to the same standards

As mentioned above, the revDPA does not have more extensive requirements for data processing agreements than the GDPR. Moreover, the requirements for agreements between joint controllers are not higher (on the contrary). Moreover, recipients or categories of recipients must be stated in the records of processing activities and in privacy notices.

26 *Cross-border disclosure*

Disclosure of personal data is restricted under the GDPR, i.e. under certain circumstances only permitted with adequate safeguards. These restrictions apply, for example, to disclosure of data to the US, India and other countries outside the EEA, so-called "third countries").

Ongoing **cross-border disclosure** of data within (cf. section 27) and outside the group is to be established. In each case, the adequacy of the level of data protection in the recipient state (i.e. whether the level of data protection has been recognised as adequate by the EU Commission) must be determined. Furthermore, in the case of disclosure to third countries, **data transfer agreements** must be reviewed for the necessary safeguards. Typically, the EU standard contractual clauses published by the EU Commission on 4 June 2021 (Commission Implementing Decision EU 2021/914) have to be concluded. Existing agreements containing a previous version of the clauses must be amended.

The FDPIC has recognized the EU standard contractual clauses as basis for transfers of personal data to a country without an adequate level of data protection, provided that the necessary

If GDPR implementation is completed: adaptation of standard contractual clauses to Switzerland for data transfers from Switzerland to a country without an adequate level of data protection

In terms of content, the requirements of the revDPA are largely the same as those under the GDPR. In the event of unauthorised disclosure abroad, there are **risks of criminal liability**. In addition, obligations of secrecy are to be observed, for example in accordance with Article 273 of the Swiss Criminal Code and sectoral regulations.

adaptations and amendments are made for use under Swiss data protection law.

Since the European Court of Justice (ECJ) struck down the Privacy Shield in the "**Schrems II**" judgement and required a risk assessment when using the standard contractual clauses, further measures may be necessary. These include reviewing existing contracts with recipients in third countries and conducting a **transfer impact assessment** (TIA) of the specific risks arising from the disclosure. Depending on the outcome of such TIAs, additional technical and/or organizational measures may be required in order to mitigate the specific risks of the transfer. In certain cases, according to the FDPIC, transfers may not be continued and must be stopped.

If records of processing activities and privacy notices still refer to the Privacy Shield, adaptations thereof are also required.

Here again, in terms of content the revDPA does not have more extensive requirements than the GDPR. However, the FDPIC also requires a risk assessment and, if necessary, an addition to the standard contractual clauses.

Intra-group data flows

In principle, the same rules apply to data flows within a group of companies as those applicable for transfers to other third parties, in relation to cooperation with third parties and cross-border disclosure of data. In most cases, however, companies have special regulations for their intra-group processing and transfers.

27 *Regulation of intra-group data flows (roles and cross-border disclosure)*

Intra-group data flows are generally regulated separately, either on a **case-by-case basis** or in the form of a **framework agreement**. In addition to the establishment of intra-group data flows, the review and, if necessary, the conclusion of or amendment to a framework agreement ("IGDTA" or "IDPA") should be considered, whereby the recorded data flows and processing must generally be recorded centrally (see section 9).

Alternatively, existing contracts can be supplemented, for example, by internal data processing agreements, agreements between joint controllers and/or standard contractual clauses for cross-border disclosure. Intra-group recipients must also be recorded in records

If GDPR implementation is completed: review of existing intra-group principles; as a rule, only selective adaptations are necessary

Where a framework agreement has been drawn up in accordance with the GDPR, only a few adaptations to the revDPA are usually necessary. In the event of unauthorised disclosure abroad, there are **risks of criminal liability**. Under certain circumstances, data/professional secrecy regulations may particularly need to be reviewed.

According to the revDPA, intra-group recipients are also to be recorded as a category of recipients in the records of processing activities and privacy notices; however, unlike the GDPR, the revDPA requires recording of all recipient states.

of processing activities and privacy notices (for example as a category of recipients).

Rights of data subjects

Data subjects have certain rights (for example the access right and the right to rectification). Compliance with the rights of data subjects is important both legally and to avoid reputational risk.

28 *Handling rights of data subjects*

There are relatively **detailed specifications** for dealing with data subjects rights. The first step is to plan the appropriate processes. In addition to determining the subject and scope depending on frequency, the data subjects must be identified, internal responsibilities must be defined, the admissibility of the rights and their exceptions must be clarified, and it must be determined how the necessary information is to be collected, compiled and communicated in the event of data subject access requests. The information in privacy notices must be aligned with these processes, for example regarding communication channels, identification and responsibilities. Finally, the technical implementation must be considered and in particular the capability to provide information, erase data (cf. section 30 et seq.) and with respect to data portability.

If GDPR implementation is completed: adaptation of existing processes and templates

With regard to the subject and the handling of requests from data subjects, there are in some cases significant **deviations from the GDPR** (for example with regard to procedure and exceptions). For certain violations there are risks of criminal liability. Additional regulations in the revDPO apply for deadlines and cost in the case of data subject access requests.

29 *Correspondence*

For more frequent data subject access requests (SARs), check whether sample correspondence should be drafted.

If GDPR implementation is completed: review and, if necessary, adaptation of sample correspondence

There are some deviations from the GDPR in the response to data subject access requests.

Storage and erasure

A key aspect of data protection compliance is the erasure or anonymisation of personal data the processing of which is no longer required (i.e. after the purpose of the processing has been achieved). Controlled erasure of data after certain events or deadlines places high demands on the IT and applications in use.

30	*Erasure of data*	The technical ability for defined storage and controlled erasure of data is crucial in this respect. If necessary, this should be developed as a separate sub-project.	In terms of content, the revDPA does not have more extensive requirements than the GDPR.
31	*Data erasure concept*	As the basis of a (partly technical) solution, it is necessary to determine applicable storage periods and types depending on the category or classification of data, and erasure or anonymisation (retention policy).	**If GDPR implementation is completed**: adapt existing retention policies; if necessary, plan adjustments on a system-level

Training

Neither the GDPR nor the revDPA require training explicitly. However, training is often helpful or necessary, may reduce liability, and may possibly also be mandatory as part of proper governance and accountability.

32	*Subject matter*	Training measures must be planned in particular with regard to their addressees (for example all employees, certain employees, certain divisions of the company, etc.), their content, frequency and measurement of success.	**If GDPR implementation is completed**: adaptation of existing training material where necessary
33	*Implementation*	Training material can be purchased or created or adapted by the company itself.	

Abbreviations

DPIA	Data Protection Impact Assessment(s)
DPA	Swiss Federal Data Protection Act. This includes an ordinance (DPO).
DPO	Data Protection Officer (DPO) within the meaning of the GDPR
ECJ	European Court of Justice
EEA	European Economic Area (in addition to the EU, it also includes Liechtenstein, Norway and Iceland)
EU	European Union
GDPR	EU General Data Protection Regulation (Regulation (EU) 2016/679)
revDPA	revised Swiss DPA
revDPO	revised Ordinance to the (revised) DPA

Walder Wyss Ltd.

Attorneys at Law

Telephone +41 44 498 98 98
reception@walderwyss.com

www.walderwyss.com
Zurich, Geneva, Basel, Bern, Lausanne, Lugano

Contacts

Jürg Schneider

Dr. iur., Attorney at Law

Partner

Telephone direct: +41 58 658 55 71

juerg.schneider@walderwyss.com

David Vasella

Dr. iur., Attorney at Law, CIPP/E, CIPM

Partner

Telephone direct: +41 58 658 52 87

david.vasella@walderwyss.com