July 16 2021

Data Protection Ordinance pre-draft specifies private entity obligations under revised data protection law

Walder Wyss Ltd | Tech, Data, Telecoms & Media - Switzerland

JÜRG SCHNEIDER

LENA GÖTZINGER

Introduction

The pre-draft of the revised Federal Data Protection Ordinance (rev-DPO) specifies and complements the provisions of the revised Federal Data Protection Act (rev-DPA) that Parliament adopted on 25 September 2020 (for further details please see "Revised Data Protection Act approved").

Companies that are currently reviewing and adapting their data processing activities to the rev-DPA are recommended to take into account the pre-draft of the rev-DPO. While the final version of the rev-DPO will certainly differ on certain points from the pre-draft, variations will most likely be limited and can be addressed with little effort once the final version of the rev-DPO is known.

The rev-DPO and rev-DPA will take effect at the same time. According to the press release of the Federal Council,[(1)] this should happen in the second half of 2022.

Key provisions to take into account

The provisions of the pre-draft of the rev-DPO that apply to private individuals or entities (as opposed to federal bodies) touch on the following areas in particular:

- data security (articles 1 to 5);
- processing by processors (articles 6 and 7);
- cross-border disclosure of personal data (articles 8 to 12 and Annex 1);
- duties of the controller and the processor (articles 13 to 19);
- access right (articles 20 to 23);
- data portability (article 24);
- data protection advisor (article 25); and
- exception from maintaining an inventory of data processing activities (article 26).

The respective provisions in the pre-draft of the rev-DPO are explained in and clarified by the explanatory report of the Federal Council.[(2)] Further, differences between the pre-draft of the rev-DPO and the current Federal Data Protection Ordinance are illustrated in a comparison table.[(3)]

An overview of the aforementioned key provisions is provided below, as the rev-DPO (published on 23 June 2021 by the Federal Council) is available for download only in German, French and Italian.

Data security

Article 8(3) of the rev-DPA requires the Federal Council to issue provisions on the minimum requirements for data security. Instead of prescribing rigid specific minimum data security requirements, the rev-DPO takes a risk-based approach; the controller and processor must determine the appropriate measures based on the respective risk. The rev-DPO specifies which criteria (article 1 of the rev-DPO) are to be considered in this assessment and provides guidelines on how these measures should be designed by listing protection objectives that must be met (article 2 of the rev-DPO). Compared with the current DPO, article 2 of the rev-DPO has added additional data protection objectives.

If it results from a data protection impact assessment (DPIA) concerning an automated processing of personal data that despite the measures envisaged by the controller, such processing still presents a high risk for the data subject's personality or fundamental rights, the private controller and its processor must record certain processing activities and keep such records for at least two years separate from the system in which the processing of the personal data takes place (article 3 of the rev-DPO).

The private controller and its processor must establish a processing policy for automated processing activities if they process sensitive personal data on a broad scale or in case of high-risk profiling (article 4(1) of the rev-DPO). Article 4(2) of the rev-DPO sets out the minimum content of such policy. The policy must also be regularly updated (article 4(3) of the rev-DPO).

Engagement of processors

If the controller assigns the processing of personal data to a processor, the controller remains responsible for data protection and must ensure that the data is processed in compliance with contractual and statutory provisions (article 6(1) of the rev-DPO).

Article 6(2) of the rev-DPO further specifies that if the processor is not subject to the rev-DPA, the controller must ensure that other statutory provisions provide for an equivalent protection of personal data. In the absence of such provisions, this must be ensured

contractually. However, contrary to article 28 of the EU General Data Protection Regulation (GDPR), article 6 of the rev-DPO does not require such contractual arrangement to meet specific minimum (content) requirements.

This being said, compliance with article 28 of the GDPR is not necessary *per se* from a rev-DPA perspective. However, in practice, compliance with article 28 of the GDPR will in most cases also satisfy the requirements under the rev-DPA and will be the preferable solution.

Cross-border disclosure of personal data

Under article 16(1) of the rev-DPA, the Federal Council shall now determine which states or international bodies guarantee an adequate level of protection in case of cross-border disclosure of personal data. According to article 8(3) of the rev-DPO, the adequacy of the data protection legislation must be reassessed periodically. Interestingly, article 8(2) of the rev-DPO mentions that assessments made by international bodies or foreign authorities that are responsible for data protection (eg, the European Commission) may be taken into account by the Federal Council for its own determination.

The states, territories, specific sectors in a state and international bodies with an adequate data protection legislation are listed in annex 1 to the rev-DPO. Currently, the draft (but non-final) list includes all European Economic Area (EEA) member states. If a state is not listed in annex 1, this does not necessarily mean that such state does not have an adequate protection of personal data (for example, the Federal Council may not yet have assessed the respective state's legal framework). However, in the absence of a positive determination by the Federal Council and any exceptions pursuant to article 17 of the rev-DPA, any disclosure abroad requires that adequate protection is guaranteed otherwise, for example through:

- contractual clauses or specific safeguards;
- standard contractual clauses previously approved, established or recognised by the Federal Data Protection and Information Commissioner (FDPIC); or
- binding corporate rules on data protection previously approved by the FDPIC or a foreign authority (article 16(2) of the rev-DPA).

Article 9(1) of the rev-DPO sets out the aspects that, as a minimum, must be covered by such contractual clauses or specific safeguards. Approval by the FDPIC is not required, but the contractual clauses or specific safeguards must be communicated to the FDPIC beforehand. Further, the specific safeguards must be developed by the competent Swiss federal authority (article 16(2)(b) of the rev-DPA). Also, the use of contractual clauses or specific safeguards is not sufficient in itself. The controller must take adequate measures to ensure that the recipient complies with such contractual clauses or specific safeguards (article 9(2) of the rev-DPO).

As regards standard contractual clauses, the FDPIC shall publish a list of standard contractual clauses that it has approved, established or recognised (article 10(2) of the rev-DPO). However, as in the case of transfers based on contractual clauses or specific safeguards, the controller must take adequate measures to ensure that the recipient complies with the standard contractual clauses (article 10(1) of the rev-DPO). Article 11 of the rev-DPO sets out more detailed requirements for binding corporate rules.

Finally, according to article 16(3) of the rev-DPA, the Federal Council can provide for additional adequate safeguards allowing for a transfer to states without adequate data protection. The Federal Council has used this competence by foreseeing in article 12 of the rev-DPO that personal data may be disclosed abroad if through a code of conduct approved by the FDPIC or a certification that an adequate data protection is ensured, provided that certain additional requirements are met. The possibility to use codes of conduct and certification may offer additional flexibility to companies. However, codes of conduct must be previously approved by the FDPIC.

Further duties of controllers and processors

The controller must inform any recipients to whom it disclosed personal data without delay of any correction, deletion, destruction as well as the restriction of the processing of personal data, unless such notification is impossible or involves a disproportionate effort (article 16 of the rev-DPO).

Article 18 of the rev-DPO requires the controller to record in writing (including documents in electronic format) a DPIA and to safeguard such records for two years after the termination of the processing activity.

Articles 19(1) and (3) of the rev-DPO set out the information that the controller must provide to the FDPIC and the data subjects (as applicable under article 24 of the rev-DPA) in case of a data security breach. As regards the notification to the FDPIC, article 19(2) of the rev-DPO explicitly allows the controller to provide the information successively without undue delay, if the controller is not in a position to provide all of the required information at the time that the data security breach is discovered. Importantly, the controller must also document data security breaches. Such documentation must include:

- all facts that relate to the incident;
- its consequences; and
- the measures taken.

The documentation must be kept for at least three years after the notification of the incident to the FDPIC (article 19(5) of the rev-DPO).

Modalities of data subject's right to access and data portability

Articles 20 to 23 of the rev-DPO specify the modalities, responsibilities, time limits and exceptions to the exemption from costs in respect of the data subject's access right.

As is currently the case, the information must be provided to the data subject within 30 days of receipt of the access request. If the controller refuses, restricts or defers the provision of information, it must inform the data subject within the same period (article 22(1) of the rev-DPO).

If the controller is not in a position to provide the information within 30 days of the receipt of the request, it must inform the data subject thereof and communicate the period of time within which the information will be provided (article 22(2) of the rev-DPO).

As a general rule, the information must be provided free of charge to the data subject. An appropriate share of the costs (up to a maximum of Sfr300) may be requested from the data subject if the provision of the information requires a disproportionate effort. However, the data subject must be informed in advance about the amount of the share and may withdraw their access request within 10 days (article 23 of the rev-DPO).

As regards data portability, article 24 of the rev-DPO simply mentions that certain requirements relating to the modalities, responsibilities,

time limits and exceptions to the exemption from costs in respect of the access rights also apply to the right of data portability.

Data protection advisor

Article 25(1) of the rev-DPO specifies the following duties of the data protection advisor of a private controller:

- audit the processing of personal data as well as its prerequisites and recommend corrective measures if they ascertain that the data protection regulations have been infringed; and
- participate in the preparation of the DPIA and review it, in any case if the private controller wishes to abstain from consulting the FDPIC in accordance with article 23(4) of the rev-DPA.

In its explanatory report, the Federal Council mentions that the data protection advisor, as its designation suggests, is a consulting and supporting position and that, as a consequence and based on its decision power, the controller remains solely liable for data protection compliance, in particular towards the data subject. Also, according to the Federal Council, the duties of the FDPIC under article 25(1)(a) of the rev-DPO do not create a liability of the data protection advisor if the controller infringes the data protection legislation. This precision is welcome and hopefully the courts will follow this approach.

Exemptions from duty to maintain inventory of processing activities

According to article 12(5) of the rev-DPA, the Federal Council provides for exceptions to the obligation to keep an inventory of processing activities for companies that have fewer than 250 members of staff and whose processing entails only a low risk of infringing the personality of the data subject.

Based on the foregoing, article 26 of the rev-DPO foresees that companies and other private law organisations that have fewer than 250 members of staff at the beginning of a year as well as individuals are exempt from the duty to maintain an inventory of processing activities for companies, unless one of the following conditions is fulfilled:

- they process sensitive personal data on a broad scale;
- they carry out high-risk profiling.

In its explanatory report, the Federal Council mentions that the threshold of 250 members of staff is to be understood regardless of the level of employment (ie, full time or part time).

Preliminary high-level assessment

The provisions contained in the pre-draft of the rev-DPO do not come as a surprise and appear quite balanced. This being said, some of the requirements do not appear to be absolutely necessary.

For example, the requirement to establish a processing policy *prima facie* exceeds the accountability requirement under articles 5(2) and 24(1) of the GDPR. Under the GDPR, the duty of documentation is of a general nature that is only selectively reinforced (eg, the requirement to record data breaches or maintain an inventory of processing activities). However, an additional processing policy is not required and may be considered unnecessary. Controllers that must maintain an inventory of processing activities (article 12 of the rev-DPA) will already document a large part of the minimum content required for the processing policy pursuant to article 4(2) of the rev-DPO (eg, purpose of processing, categories of data processed and data security measures) for such inventory. Further, in cases where the controller must establish a processing policy, it will generally have to conduct a DPIA, which must be recorded in writing (article 18 of the rev-DPO). Thus, it seems to be an unnecessary administrative burden on private controllers and their processors to additionally establish a handbook or guideline (ie, the processing policy). It seems that the Federal Council was unwilling to let go of the processing policy obligation provided for in the current DPO.

Another example is the discrepancy to the GDPR with regard to contractual clauses (not to be mistaken for standard contractual clauses) that may be used as a guarantee for disclosure of personal data to recipients based in states without an adequate level of data protection. Whereas article 46(3)(a) of the GDPR does not provide for the minimum requirements of contractual clauses but requires their prior approval by the competent data protection authority, notification of the contractual clauses to the FDPIC is sufficient (which is welcomed), provided that they meet the minimum standard set out in article 9 of the rev-DPO. The same applies to the specific guarantees (article 16(2)(c) of the rev-DPA). Companies planning to make use of one-size-fits-all contractual clauses for their EEA and Swiss cross boarder transfers will need to take the Swiss minimum requirements into account before seeking approval of the respective European data protection authority. This being said, most companies will likely – as in the past – rely on the EU standard contractual clauses for transfers to third countries and based on the assumption that the FDPIC will also recognise the recently adopted new EU standard contractual clauses for transfers to third countries, article 9 of the rev-DPO may in practice be of limited effect.

Comment

Going forward, and from a practical point of view, it is to be hoped that the provisions of the rev-DPO that go beyond (or contradict) the requirements of the GDPR will be re-drafted as they would create additional burdens on companies subject to the DPA (and the GDPR), compared with those only subject to the GDPR.

For further information on this topic please contact Jürg Schneider or Lena Götzinger at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com or lena.goetzinger@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) The press release of the Federal Council is available in German, French and Italian.

(2) The explanatory report of the Federal Council is available in German, French and Italian.

(3) The comparison table is available in German, French and Italian.