Draft of the Swiss Federal Data Protection Act (DPA): Still Room for Improvement

24.11.2017

On 15 September 2017, the Swiss Federal Council issued the draft of the revised Swiss Federal Data Protection Act (DPA). The DPA revision has thus taken another step in this ongoing process. For further information on this process, see our news of 15 September 2017 and 22 December 2016.

The draft of the revised DPA (Draft DPA) is now closer to the GDPR. Many points of criticism of the preliminary draft were considered. However, there is still room for improvement.

The following list contains a selection of points of criticism of the Draft DPA (in order of the draft law):

– **Applicability to proceedings** (Art. 2 para. 3 Draft DPA): the present DPA is not applicable during pending proceedings due to possible delimitation problems and potential for misuse. The Draft DPA leaves this open to the procedural laws. It would be better if the revised DPA continued to regulate this issue in the same manner as in the present DPA.

– **Sensitive personal data** (Art. 4 (c) Draft DPA): like the GDPR, the Draft DPA protects certain categories of data more extensively. Under the Draft DPA this is also true with respect to data on social security measures. This contradicts the GDPR and leads to implementation problems. It is also not necessary because personal data with higher risks must already be better protected (Art. 7 Draft DPA). Art. 4 (c) subpara. 6 Draft DPA must therefore be deleted.

– **Profiling** (Art. 4 (f) Draft DPA): according to Art. 4 (f) Draft DPA, profiling means the evaluation of certain characteristics of a person on the basis of personal data processed in an automated manner. This includes evaluations "by hand" as long as the data basis has been processed in an automated manner. As a result, each evaluation would qualify as profiling because there are hardly any areas where the data basis is not processed in an automated manner in one way or another. Art. 4 (f) Draft DPA must therefore be amended accordingly.

– **Consent** (Art. 5 para. 6 Draft DPA):

  - In certain cases, consent is only effective if it is "explicitly" given. What this means exactly is already unclear under the present law and has neither been clarified in the Draft DPA nor in the dispatch of the Swiss Federal Council. Art. 5 para. 6 Draft DPA must therefore be further specified.

  - In addition, consent must always be "unambiguously" given. The meaning of “unambiguously” is not clear. It leads to legal uncertainty and must be deleted.

- **Data protection counsellor** (Art. 9 and 21 Draft DPA): according to Art. 21 para. 4 Draft DPA, companies with a data protection counsellor can refrain from reporting the data protection impact assessments to the Federal Data Protection and Information Commissioner (FDPIC). This is to be welcomed but should be expanded: the reporting obligations according to Art. 14 para. 2 and Art. 22 para. 1 DPA should also not apply if a data protection counsellor has been appointed.

- **Codes of conduct** (Art. 10 Draft DPA): the preliminary draft stated that compliance with the DPA is presumed if the codes of conduct are complied with but that the DPA can also be complied with in other ways (Art. 9 of the preliminary draft). This provision was useful and should be reintroduced into Art. 10 Draft DPA.

- **Cross-border disclosure** (Art. 13 et. seqq. Draft DPA):

  - Cross-border disclosure is only permissible under certain conditions if the legislation of the state concerned does not guarantee an adequate level of protection (this applies, for example, to the US, India and China). The Swiss Federal Council is competent to determine such adequacy (Art. 13 para. 1 Draft DPA). As a consequence, if the Swiss Federal Council has not yet determined if a state guarantees adequate protection, cross-border disclosure is prohibited according to Art. 13 para. 1 Draft DPA. This is more restrictive compared to the present DPA and data handlers must continue to have the right – as is already the rule today – to determine for themselves in such cases if an adequate level of protection is afforded. Art. 13 para. 1 Draft DPA should be amended accordingly.

  - If there is no adequate data protection level in the state concerned, cross-border disclosure is, inter alia, still possible if the data subject has explicitly consented to the disclosure. As the present DPA does not require explicit consent in such a case and as this has not led to any problems in the

past, the requirement of explicit consent should be deleted from Art. 14 para. 1 (a) Draft DPA.

- **Data of deceased persons** (Art. 16 Draft DPA): regulating the right of access and erasure concerning deceased persons in the DPA is wrong from a systematic point of view: deceased persons do not have any personality rights. The DPA should not implement such a new type of post-mortem personality rights. Art. 16 Draft DPA should be deleted. If there is a need for new regulation in this area, the right place for it would be the law of inheritance.

- **Duty of information** (Art. 17 et. seqq. Draft DPA):

  - The scope of the duty of information is determined by a general clause and a list of mandatory information. The general clause in Art. 17 para. 2 Draft DPA should be deleted: it is unnecessary and even goes beyond the GDPR. This leads to legal uncertainty and disproportionate implementation efforts.

  - The obligation to provide information about the state in which the recipient is located in case of cross-border disclosure also goes beyond the GDPR and does not bring any added value to the data subjects. This obligation should be deleted from Art. 17 para. 4 Draft DPA.

  - Art. 18 Draft DPA sets out exceptions from the duty of information. The duty of information may be restricted, deferred or waived, inter alia, if the controller has overriding interests (e.g. protection of business secrets). However, it is only possible to claim such overriding interests if the data is not disclosed to third parties (Art. 18 para. 3 (c) Draft DPA). There is no reason for this restriction. The protection of the data subject is in any case taken into account within the context of the balancing of interests. This restriction has already been heavily criticised in the consultation procedure and should be deleted.

  - It should be considered to empower the Swiss Federal Council to provide for exceptions from the duty of information for small and medium-sized companies (similar to Art. 11 para. 5 Draft DPA).

- **Access right** (Art. 23 Draft DPA):

  - The right of access pertains to personal data (Art. 23 para. 2 (b) Draft DPA). Despite this fact, data subjects often request copies of the docu-

ments containing personal data. This is inconsistent with the system and leads to misuse. Art. 23 para. 2 (b) Draft DPA should therefore specify that the right of access pertains to personal data, but not to copies of documents.

- As with the aforementioned duty of information, the scope of the right of access is determined by a general clause and a list of mandatory information. The general clause in Art. 23 para. 2 should be deleted: it is unnecessary, goes beyond the GDPR and leads to legal uncertainty and disproportionate implementation efforts. An exhaustive list of mandatory information obligations is required.

- According to Art. 24 para. 2 (a) Draft DPA, the access right may be restricted, deferred or waived, inter alia, if the controller has overriding interests and under the condition that it does not disclose personal data to third parties. As with the analogous exemption from the duty of information, there is no reason for such a restrictive condition. It must be deleted.

– **Automated individual decisions** (Art. 19 Draft DPA): the special requirements for automated individual decisions do not apply if, inter alia, the data subject has explicitly consented. There is no obvious reason to require explicit consent. "Normal" consent is sufficient. This also results from Art. 5 para. 6 Draft DPA, which requires explicit consent only in connection with sensitive personal data and profiling.

– **Data protection impact assessment** (Art. 20 et. seqq. Draft DPA):

  - If the intended data processing may lead to high risks for the data subject's privacy or fundamental rights, the controller must conduct a data protection impact assessment (Art. 20 para. 1 Draft DPA). According to Art. 20 para. 2 (b) Draft DPA, such high risks shall always exist in case of profiling. Such legal fiction is however not appropriate; many profiling processes are harmless and even in the interest of the data subjects (e.g. fraud prevention). It does also conflict with the GDPR, which would lead to disproportionate implementation efforts. Art. 20 para. 2 (b) Draft DPA must therefore be deleted. Furthermore, if the risk is evaluated as high in an individual case, the general clause in Art. 20 para. 2 Draft DPA applies anyway.

- The controller shall consult the FDPIC prior to processing when the data protection impact assessment shows that the processing would present a high risk if the controller did not take any measures (Art. 20 para. 1 Draft DPA). This wording leads to misunderstandings. It should be clarified that (as under the GDPR) there is no obligation to consult the FDPIC if the controller does take security measures.

- According to Art. 21 para. 2 Draft DPA, the FDPIC must inform the controller of his objections against the envisaged processing within three months. This inhibits innovation in the field of data management. The deadline should be adequately shortened.

– **Verification of creditworthiness** (Art. 27 para. 2 Draft DPA): an overriding private interest of the controller is still presumed if the controller processes personal data in order to verify the data subject's creditworthiness (Art. 27 para. 2 (c) Draft DPA).

  - However, this justification only applies if there is no profiling. This makes no sense as the creditworthiness often represents a profiling. Thus, the justification would be useless. Art. 27 para. 2 (c) (subpara. 1) Draft DPA must therefore be deleted.

  - The justification is also not applicable to data older than five years. This restriction leads to a deterioration of the data basis and thus of the credit ratings. Address histories and other data must be stored for up to 20 years because loss certificates do not expire until after this period. The creditor must at least be able to obtain information about the creditworthiness for this period. Art. 27 para. 2 (c) (subpara. 3) Draft DPA must therefore be deleted.

– **Investigation of FDPIC** (Art. 43 Draft DPA):

  - The FDPIC must initiate an investigation if there are any indications that a data processing could violate data protection regulations. This obligation should be deleted as it undermines the confidence of the economy in the FDPIC and the advisory activities of the FDPIC (Art. 52 para. 1 Draft DPA). The decision whether to initiate investigations or not should be left to the discretion of the FDPIC.

  - The plaintiff's right to information (Art. 43 para. 4 Draft DPA) must be deleted. It invites the plaintiff to file complaints for investigative purpos-

es and contradicts the fact that the plaintiff shall not be a party to the proceedings (Art. 46 para. 2 Draft DPA). In case that the plaintiff is the data subject, he could make use of his access right according to Art. 23 Draft DPA.

– **Criminal provisions** (Art. 54 et. seqq. Draft DPA):

  – Criminal liability according to Art. 54 et. seqq. Draft DPA affects individuals and not companies. This fact was rightly criticised in the consultation procedure. However, the Swiss Federal Council has decided to stick to this choice. This makes it all the more important to precisely formulate the provisions whose violation may be criminally sanctioned.

  – Because violations of the duties of information and of the access rights set forth in Art. 17, 19 and 23 Draft DPA may be criminally sanctioned according to Art. 54 para. 1 DPA, these obligations must be interpreted restrictively. For the same reason the aforementioned general clause concerning the duty of information (Art. 17 para. 2 DPA) must be deleted.

  – The criminal liability of disclosure of secret personal data goes generally too far (Art. 56 Draft DPA). In the present DPA, disclosure is only punishable if it concerns secret sensitive personal data (and secret personality profiles). This should be maintained. In any case, many personal data are comprehensively protected by special confidentiality provisions (e.g. Art. 321 of the Swiss Penal Code for patient data, clients of an attorney, etc.).

– **Modifications of the Swiss Civil Procedure Code (CPC)**: the draft provides for several modifications to the CPC whose purpose is to facilitate civil actions under the DPA (by conferring jurisdiction on the plaintiff's court and by exemptions from securities and court fees). This is intended to limit the enforcement efforts of the FDPIC. It is however based on the false assumption that data protection law is consumer protection law. It leads to false incentives and burdens the budgets of the cantons. The intended changes are to be dropped.

The recently published Draft DPA brought a number of improvements. In particular, many aspects of the "Swiss finish" (i.e. discrepancies from the GDPR) have been dropped. However, as shown above, there are still many provisions which differ from the GDPR without need and are overly burdensome. It is to be hoped that a least some of these aspects will be improved during the parliamentary process.