
Image: Henryk Sadura / Moment Open / Getty Images

**The Federal Council confirmed its intention to end a long standing tradition of treating corporate entities as individual people when it comes to the protection of their data.**

**Sylvain Métille** Partner
metille@hdclegal.ch

**David Raedler** Senior Associate
raedler@hdclegal.ch

HDC, Lausanne

# Swiss Data Protection Act reform set in motion

In December 2016, the Federal Council launched a public consultation on the preliminary draft of a new Data Protection Act to replace the Federal Act on Data Protection 1992 ('the DPA Draft'). According to the Federal Department of Justice and Police, the DPA Draft, once adopted, will enable the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe ('Convention 108') and align Swiss law with the requirements set out in the General Data Protection Regulation (Regulation (EU) 679/2016) ('GDPR') in conformity with Switzerland's commitments to the Schengen system. Sylvain Métille and David Raedler, Partner and Senior Associate respectively at HDC, discuss the changes proposed by the DPA Draft and highlight its shortcomings, which include the lack of strong enforcement powers for the Federal Data Protection and Information Commissioner ('FDPIC').

The DPA Draft is open to comment until April 2017. The revision will be conducted at a high pace and the revised law is supposed to enter into force simultaneously with the GDPR in 2018. It aims to reinforce both the rights of the data subject and the obligations of the data controller. The published DPA Draft does not, however, answer all expectations and two important regrets remain: the limited powers of enforcement that are given to the FDPIC and the applied criminal liability regime, which focuses on the individuals employed by the controller instead of the company itself.

## Bye bye corporate privacy

The Federal Council confirmed its intention to end a long standing tradition of treating corporate entities as individual people when it comes to the protection of their data. Hence, the DPA Draft does away with a special feature of Swiss data protection law and narrows its protection to cover only natural persons, to the exclusion of corporate entities.

This change is notably welcome for cross-border transfers of data, as Standard Contractual Clauses ('SCCs') or Binding Corporate Rules ('BCRs') will no longer be required to export data from Switzerland to the EU. Although this change may seem important, it is tempered by the fact that such a protection was often not respected in practice. That being said, corporate entities (including their data) shall remain protected through other existing rules, including copyright laws, rules on unfair competition and (most of all) personality rights.

## New obligations for the controller

**1. A proactive information obligation as a general rule:** An extensive information obligation that involves actively informing the data subject of several elements pertaining to the processing of his/her data, including the data controller's identity and contact details, the data being processed, and the purposes of the processing. As this information obligation goes much further than the recognisable standard that is currently applied, in particular by the fact that such information must as a rule proactively be given and not only upon request of the data subject, data controllers will have to adapt their practice and compliance standards.

**2. Documenting the data processing:** The obligation to document any and all processing mechanisms and, if the data is being communicated to any third party, to inform the recipient(s) of any and all rectification, deletion, destruction or violation of the DPA Draft. Due to this broad documentation and update obligation, the filing obligation is abandoned for private companies (but remains for government bodies). This will limit the formalities to be respected towards the FDPIC, but not really ease the work of the data controller.

**3. Privacy breach notification:** An information obligation towards the FDPIC as well as (under certain circumstances) the data subject in case of any unauthorised processing or loss of personal data (privacy breach).

**4. Privacy Impact Assessment:** The need to complete (and communicate to the FDPIC) a Privacy Impact Assessment for each case in which the planned processing may result in an 'increased risk' for the data subject's personality and fundamental rights, as well as detail the planned measures to be applied. The FDPIC shall then have three months to inform the data controller of any objections to the planned processing. It is worth noting that the concept of 'increased risk' is not defined by the DPA Draft, nor are the consequences of not taking into account the FDPIC's comments.

**5. Privacy By Design and Privacy By Default:** The obligation to implement the principles of Privacy By Design and Privacy By Default.

**6. Information in cases of outsourcing or subcontracting:** An obligation to provide the data subject with the


continued

identity and contact information of the processors, as well as a description of the data or the categories of data being processed, in any case of outsourcing or subcontracting. A change of provider is likely to trigger a notice obligation;

**7. Information on automated decision making:** An obligation to inform the data subject and give him/her the opportunity to comment when an individual decision that produces legal effects or significantly affects him/her is taken solely on the basis of an automated data processing system.

## Criminal penalties for individuals instead of administrative fines for companies

The DPA Draft reinforces the FDPIC's powers in two respects, at least on paper. It shall have the possibility to open investigations in any case of infringement of data protection laws and not only (as is the case today) for data processing methods that have a systematic impact on an important number of people. It shall also have the ability to issue binding decisions, for example by ordering the interruption of a specific case of data processing or the destruction of data collected by infringing the DPA Draft. The data controller can challenge such a decision before the courts. Surprisingly enough, however, and in opposition to the European trend, the FDPIC cannot impose any fines itself and has to report the case to the criminal authorities. In addition to the fact that this shall make the FDPIC lose all control on how the prosecutor will treat the case, this solution may even be incompatible with the Directive on Data Protection in Law Enforcement (Directive (EU) 680/2016) as well as the Schengen *Acquis*.

Most of the violations provided for in the DPA Draft (including the violation of the Privacy By Design or Privacy By Default principles) will be deemed criminal offences subject to fines up to CHF 500,000 (approx. €468,042); CHF 250,000 in case of mere negligence (approx. €234,000). Unlike EU law, however, only the responsible individual within the company will as a rule be sanctioned, not the company itself. Such sanctions will be registered in the person's criminal record. The only exception shall apply if the responsible individual cannot be identified and that the investigation required to potentially do so would be out of proportion. In such a case, and only then, the company itself could be criminally prosecuted and fined, but only up to CHF 100,000 (approx. €93,600).

By refusing to give the FDPIC real powers, the draft firstly complicates the data controller's activities, as it may have to face at the same time an administrative proceeding (if the FDPIC requests a stop or change in the processing), a criminal proceeding and civil proceedings opened by the data subjects who cannot take part in the administrative and criminal cases. Secondly, doubts may be cast on how prosecutors will treat privacy violations, especially considering the lack of coordination with the FDPIC. Thirdly, the sanctioning system focused on individuals does not take into account that privacy violations are often the responsibility of the company and increases the risk that an employee be used as a scapegoat.

In parallel to this, and taking advantage of the DPA Draft, the Government has also introduced new offences in the Swiss Criminal Code, including a new provision on identity theft as well as a duty of secrecy that falls upon any profession that is characterised by the knowledge of personal data or the processing of such data for commercial purposes.

## Conclusion: Room for improvement

**Although some of the proposed measures are to be welcomed because of the new rights they offer to data subjects and the harmonisation with surrounding countries (including EU law), as well as the general inspiration by the GDPR and Convention 108 it is based on, the opportunity should have been used to go further and better clarify some of the clauses.**

**Several important goals have also been missed. The absence of any possibility of class action, including for public interest organisations, the absence of any reference to data portability or to the role of a data protection officer within companies, and finally the absence of any explicit rule relating to the use of cookies or other tracking systems, are regretful. So is the absence of any sanctioning power given to the FDPIC, who is therefore compelled to follow the criminal path in order for its own binding decisions to be executable.**

**We may still hope that the public consultation and the discussion within Parliament will help to improve the DPA Draft; however most of the measures included in the Draft will likely be confirmed. As the new law will likely enter into force in May 2018 without a grace period (together with the GDPR), companies should now start to review and document their organisational and data processing methods, in order to ensure all the required compliance.**