Bloomberg BNA | Bloomberg Law®: Privacy & Data Security

Country Profile: SWITZERLAND

Dr. Jürg Schneider and Dr. Monique Sturny, of Walder Wyss Ltd., Zurich, provided expert review of the Switzerland Country Profile and wrote the Risk Environment section. [Last updated May 2016 – Ed.]

I. Applicable Laws and Regulations

A. Introduction

Privacy is recognized as a fundamental right under the Federal Constitution of the Swiss Confederation of April 18, 1999 (the Constitution; unofficial English translation provided by the Swiss government). Specifically, the Constitution states that every person has the right to privacy in their private and family life, in their home, and in relation to their mail and telecommunications. They also have the right to be protected against the misuse of their personal data (Constitution, Title 2, ch. 1, art. 13).

On a federal level, data privacy in Switzerland is more specifically governed by the Federal Act of 19 June 1992 on Data Protection (FADP; unofficial English translation provided by the Swiss government). It is supplemented by the Ordinance of 14 June 1993 to the Federal Act on Data Protection (OFADP; unofficial English translation provided by the Swiss government) and by the Ordinance of 28 September 2007 on Data Protection Certification (DPCO; unofficial English translation provided by the Swiss government).

The FADP applies to the processing of personal data by private persons and federal bodies, including sensitive personal data and personality profiles. "Personal data" means all information relating to an identified or identifiable natural or legal person (FADP art. 3, ¶ a). Hence, unlike the data protection regulations of most other countries, the FADP applies not only to natural persons, but equally to legal entities.

"Sensitive personal data" is information on (1) religious, ideological, political, or trade union-related views or activities; (2) health, the intimate sphere, or racial origin; (3) social security measures; and (4) administrative or criminal proceedings and sanctions (FADP art. 3, ¶ c). "Personality profiles" refer to collections of data that permit an assessment of essential characteristics of the personality of a natural person (FADP art. 3, ¶ d). Protection for personality profiles and sensitive personal data is stronger than for "ordinary" personal data.

Note that further data protection-related rules may be relevant in specific cases (such as, e.g., banking secrecy provided in art. 47 of the Swiss Federal Banking Act; available in German, currently no English translation available). Furthermore, cantonal data protection laws apply to any data processing by cantonal bodies. There are 26 cantons in Switzerland and hence 26 different cantonal regimes. Such cantonal data protection laws may have a broader scope of protection than the FADP (e.g., the Act on Information and Data Protection of the Canton of Zurich [IDG] of 12 February 2007 (available in German) applies to "information" at large, IDG § 1, ¶ 1).

B. General Requirements Applicable to Processing of Personal Data

When processing personal data, the following requirements apply in particular (FADP art. 4 - 7):

- personal data may only be processed lawfully, in good faith, and according to the principle of proportionality (FADP art. 4, ¶¶ 1, 2);
- personal data may only be processed for the purpose that is indicated at the time of the collection, evident from the circumstances at the time of collection, or provided for by law (FADP art. 4, ¶ 3);
- the collection of personal data and, in particular, the purpose of its processing must be evident to the data subject (FADP art. 4, ¶ 4);

- where consent of the data subject is required for the processing of personal data, such consent must be given voluntarily after receiving sufficient information (FADP art. 4, ¶ 5);
- anyone who processes personal data must ensure that the data processed is accurate (FADP art. 5);
- unless an exception applies (see next bullet point), personal data may not be disclosed abroad if the privacy of the data subject would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection (FADP art. 6, ¶ 1);
- even if the privacy of the data subject would be seriously endangered thereby, cross-border disclosure of personal data is permissible under certain circumstances, *inter alia* if a data transfer agreement ensuring an adequate level of protection is entered into and the Swiss Federal Data Protection and Information Commissioner (Commissioner) is informed accordingly before the first disclosure takes place, if the data subject has given its consent in the specific case, or if there is an overriding Swiss public interest (FADP art. 6, ¶ 2) (for more details, see subsection D. Disclosure Abroad, below); and
- personal data must be protected from unauthorized processing by appropriate technical and organizational measures (FADP art. 7).

Processing of personal data does not necessarily require a justification. However, anyone who processes personal data must not unlawfully breach the privacy of the data subjects in doing so, unless it is justified by the consent of the injured party, by an overriding private or public interest (from a Swiss perspective), or by Swiss federal, cantonal, or municipal law (FADP art 12, ¶ 1, in conjunction with FADP art. 13). In particular, justification is required when processing personal data in contravention of the principles set forth in FADP art. 4, art. 5, ¶ 1, and art. 7, ¶ 1; when processing personal data pertaining to a person against that person's express wish; or when disclosing sensitive personal data or personality profiles to third parties for such third parties' own purposes. All such instances constitute an unlawful breach of privacy and therefore require justification (FADP art. 12, ¶ 2).

C. Data Processing by Third Parties

The FADP explicitly addresses the processing of personal data by third parties (FADP art. 10*a*, ¶ 1). However, assignment of duties to a third party is permitted only if the assignee processes the personal data exclusively in the manner permitted for the assignor and if the assignment is not prohibited by a statutory or contractual duty of confidentiality (FADP art. 10*a*, ¶ 1(a) and (b)). Furthermore, the assignee must in particular guarantee the security of the personal data (FADP art. 11*a*, ¶ 2).

The FADP does not require data processing agreements to be made in written form. However, in practice, such agreements are often made in writing, and this is certainly recommended. It further needs to be noted that data processing agreements must not necessarily be separate from the underlying business agreement. It is very frequently the case that provisions governing the processing of personal data by the assignee are directly made part of and are thus integrated into the underlying business agreement.

D. Disclosure Abroad

Special rules apply to the disclosure of personal data from Switzerland abroad (FADP art. 6).

For the purpose of the FADP, a disclosure abroad occurs if personal data is transferred from Switzerland to another country or if personal data located in Switzerland is accessed from another country.

The FADP prohibits a transfer of personal data abroad if such transfer could seriously endanger the personality rights of the data subjects concerned, in particular due to the absence of legislation that guarantees adequate protection (FADP art. 6, ¶ 1).

The Commissioner has published a (non-binding) list (in German) of countries that provide adequate data protection for personal data pertaining to individuals. The United States is not on that list. The Commissioner does not consider U.S. law (either federal or state) as providing an adequate level of protection for any type of personal data.

Most European Union/European Economic Area countries have not implemented protection for legal entities in their national data protection law and therefore cannot *per se* be considered as providing an adequate level of protection for personal data pertaining to legal entities. However, in our view, one could reasonably argue that adequate protection for personal data pertaining to legal entities may in certain circumstances be covered by legislation other than data protection legislation. Furthermore, transfers of personal data pertaining to legal entities do not necessarily and in each case seriously endanger personality rights. However and in any case, this would need to be checked and verified on an individual basis and creates additional risks for the transferor. In addition, it is not certain that Swiss courts would follow the aforementioned arguments.

If personal data is disclosed to recipients located in countries where legislation does not provide an adequate level of protection for the personal data being transferred, such personal data may be disclosed only if:

(a) sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad (FADP art. 6, ¶ 2(a));

(b) the data subject has consented in the specific case (FADP art. 6, ¶ 2(b));
(c) the processing is directly connected with the conclusion or the performance of a contract, and the personal data is that of a contractual party (FADP art. 6, ¶ 2(c));
(d) disclosure is essential in the specific case in order to safeguard an overriding public interest or for the establishment, exercise, or enforcement of legal claims before the courts (FADP art. 6, ¶ 2(d));
(e) disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject (FADP art. 6, ¶ 2(e));
(f) the data subject has made the data generally accessible and has not expressly prohibited its processing (FADP art. 6, ¶ 2(f)); and
(g) disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection (FADP art. 6, ¶ 2(g)).

Typically, the EU Commission's model contracts for the transfer of personal data to third countries, adapted to Swiss law requirements, are used in order to ensure an adequate level of data protection in accordance with item (a) above. The contract(s) must be entered into with the recipient(s) before the first disclosure occurs.

Finally, if the disclosure is based on the exceptions listed in items (a) and (g) above, the Commissioner must be informed of the safeguards or data protection rules used to ensure an adequate level of protection (FADP art. 6, ¶ 3). Notice to the Commissioner must take place before the first disclosure is made. If this is not possible, the notice must take place immediately after disclosure (OFADP, art. 6, ¶ 1). The intentional failure to inform the Commissioner is, upon complaint filed with the criminal prosecution authorities, punishable by a fine of up to CHF 10,000. Non-payment of the fine may result in imprisonment for up to three months (FADP art. 34, ¶ 2(a), in conjunction with art. 106, ¶ 1 Swiss Criminal Code [SCC] (unofficial English translation provided by the Swiss government)).

E. Registration of Data Files

The Commissioner maintains a public register of data files (FADP art. 11*a*, ¶ 1).

There is no general duty under the FADP to register all data files and processing activities. However, private controllers of data files must declare their data files to the Commissioner before they are opened if they regularly process sensitive personal data or personality profiles or regularly disclose personal data to third parties for such third parties' own purposes (FADP art. 11*a*, ¶¶ 3, 4). This duty to declare a data file for registration does not apply if:

- the controller of the data file processes the personal data pursuant to a Swiss statutory obligation (FADP art. 11*a*, ¶ 5(a));
- the Swiss Federal Council has exempted the particular processing from the registration requirement because it does not prejudice the rights of the data subjects (FADP art. 11*a*, ¶ 5(b));
- the controller of the data file uses the data exclusively for publication in the edited section of a periodically published medium and does not pass on any data to third parties without informing the data subjects (FADP art. 11*a*, ¶ 5(c));
- the data is processed by journalists who use the data file exclusively as a personal work aid (FADP art. 11*a*, ¶ 5(d));
- the controller of the data file has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files (FADP art. 11*a*, ¶ 5(e)) (see below for details); or
- the controller of the data file has acquired a data protection quality mark under a certification procedure and has notified the Commissioner of the result of the evaluation (FADP art. 11a, ¶ 5(f)).

The intentional failure to declare a data file for registration to the Commissioner is, upon complaint filed with the criminal prosecution authorities, punishable by a fine of up to CHF 10,000. Non-payment of the fine may result in imprisonment for up to three months (FADP art. 34, ¶ 2(a), in conjunction with SCC art. 106, ¶ 1).

It must be noted that there is no general requirement for a controller of a data file to appoint a data protection officer. However, if the controller of a data file wishes to be exempted from an existing duty to declare its data files for registration and unless any of the other aforementioned exceptions apply, the controller of a data file must appoint an operational data protection officer who fulfills the requirements of the Ordinance to the Federal Act on Data Protection (OFADP, art. 12*b*) and notify the Commissioner of such appointment (OFADP art. 12*a*, ¶ 1). According to the OFADP, a data protection officer must:

- carry out his duties autonomously and independently (OFADP art. 12*b*, ¶ 2(a));
- have the level of expertise that is appropriate for his function, taking into account the processing activities as well as the personal data concerned (OFADP art. 12*a*, ¶ 2);
- audit the processing of personal data by the controller of the data files (OFADP art. 12*b*, ¶ 1(a));

- recommend to the controller of the data files corrective measures when detecting any breaches of applicable data protection rules (OFADP art. 12*b*, ¶ 1(a));
- have access to all data files and all data processing by the controller of the data files, as well as to all other information that is required to fulfill his duties (OFADP art. 12*b*, ¶ 2(c));
- maintain a list of all data files operated by the controller of the data files and provide this list to the Commissioner or affected data subjects upon request (OFADP art. 12*b*, ¶ 1(b)); and
- not carry out any other activities incompatible with the duties of a data protection officer (OFADP art. 12*a*, ¶ 2).

II. Regulatory Authorities and Enforcement

On the federal level in Switzerland, the Swiss Federal Data Protection and Information Commissioner (Commissioner) supervises compliance with federal data protection regulation. In particular, the Commissioner supervises federal and private bodies, advises and comments on the legal provisions on data protection, and assists federal and cantonal authorities in the field of data protection. In addition, the Commissioner informs the public about his findings and recommendations, and maintains and publishes the register for data files.

The Commissioner is appointed by the Swiss Federal Council for a term of office of four years. The appointment must be approved by the Swiss Federal Assembly (FADP art. 26, ¶ 1).

The Commissioner has published several guides regarding the processing of personal data:

- Guidance on processing of personal data in the area of employment (in German; in French; in Italian);
- Guidance on processing of personal data in the medical sector (in German; in French; in Italian);
- Guidance on processing of personal data in the private sector (in German; in French; in Italian);
- Guidance on processing of personal data by federal bodies (in German; in French; in Italian);
- Guidance on the rights of data subjects (in German; in French; in Italian);
- Guidance on Internet and e-mail surveillance at the workplace (in German; in French; in Italian);
- Guidance on biometric recognition systems (in German; in French; in Italian); and
- Guidance on technical and organizational measures (in German; in French; in Italian; in English).

The above guides do not have binding character but, in practice, have become *de facto* standards in many areas.

The Commissioner may also initiate investigations in the private sector on his own initiative or at the request of a third party under certain conditions. He may issue recommendations to private persons based on such investigations (FADP art. 29).

The Commissioner regularly publishes his recommendations (in German) on his website. From January 2011 to February 2016, the Commissioner published ten recommendations on his website. Five of these recommendations have been issued to Swiss banks concerning the delivery of employee data to U.S. authorities. Others concerned biometric data for a reservation system, publication of personal data on business and credit information platforms, the implementation of the right of information and objection, and data protection issues regarding the use of public transportation services.

If the addressee of the recommendation objects to it or does not comply with it, the Commissioner may refer the case to the Swiss Federal Administrative Court for a decision. The decision of the Swiss Federal Administrative Court can be appealed before the Swiss Federal Supreme Court.

With respect to cybercrime-related issues, two additional agencies deserve mention.

The Reporting and Analysis Center for Information Assurance (MELANI) addresses issues regarding the security of computer systems and the Internet, as well as the protection of critical national infrastructures. MELANI is open to private computer users as well as small and medium-size enterprises (SMEs) in Switzerland. MELANI has a reporting form that can be used to report incidents involving threats and risks.

The Cybercrime Coordination Unit Switzerland (CYCO) is Switzerland's central office for reporting illegal subject matter on the Internet. After conducting an initial analysis of an incoming report and securing the relevant data, CYCO forwards the case to the appropriate law enforcement agencies in Switzerland and/or abroad. CYCO also actively searches the Internet for illegal subject matter and carries out in-depth analyses of Internet crime.

III. Risk Environment

Compared to other European countries, the risk of sanctions for infringements of the Swiss data protection legislation is rather low.

First, the Swiss Federal Data Protection and Information Commissioner (Commissioner) does not have the power to issue criminal or administrative penalties for infringements of the FADP, but merely has the competence to investigate and issue recommendations (including the recommendation to modify or even abandon certain processing activities).

Second, in accordance with the FADP, the Commissioner may only open investigations if the processing methods in question are capable of breaching the privacy of a larger number of persons (system errors), if data files must be registered, or if there is a duty to provide information under FADP art. 6, ¶ 3.

Third, the Commissioner only has limited resources (with respect to both budget and workforce) and thus focuses on major cases/issues with a certain preference for a rather pragmatic approach.

Based on the foregoing, the number of investigations as well as recommendations is rather low, and there has been no significant increase in investigations over the past few years.

That said, certain sectors are more extensively regulated than others, and relevant supervisory authorities do have extensive investigative powers within their fields of competence. For example, in the banking sector, the Swiss Financial Market Supervisory Authority (FINMA) amended its circular 2008/21 in 2014 on the operational risks of banks by adding new guidelines on the treatment of electronic client data by banks. The Commissioner also pays close attention to the financial sector, as evidenced by the fact that several of the Commissioner's past recommendations concerned Swiss banks.

The Commissioner's 22nd Annual Report for 2014/2015 (complete version in German; short version in English), in particular, focuses on data protection in the following sectors: Internet and telecommunications, healthcare and medical research, finance (insurance and banks), trading, and employment in general. In those sectors, and especially in the financial sector, data protection issues are more closely supervised and more often investigated.

Upon complaint, the competent Swiss courts have the power to issue criminal penalties for the intentional violation of a very limited number of obligations to provide information, to register, or to cooperate as specified in FADP art. 34, as well as for the intentional violation of professional confidentiality as specified in FADP art. 35. For each infringement, the maximum fine is CHF 10,000. Non-payment of the fine may theoretically result in imprisonment for up to three months (FADP art. 34 and art. 35, in conjunction with art. 106, ¶ 1 Swiss Criminal Code [SCC]. Furthermore and for the sake of completeness, it must be noted that, according to SCC art. 179^{novies}, any person who without authorization procures from a data file sensitive personal data or personality profiles that are not freely accessible is liable on complaint to a custodial sentence issued by the competent Swiss courts not exceeding three years or to a monetary penalty of up to CHF 1,080,000.

To our knowledge, no judgments on such penalties have been published, and according to the last available data of the Swiss Federal Statistical Office, only seven infringements of FADP art. 34 and/or art. 35 were reported in 2014. However, there are no statistics available on the amount of the penalties issued, and, as the statistics are incomplete, the actual number of penalties issued in 2014, and also 2015, is most likely higher. With respect to SCC art. 179^{novies}, only three infringements were reported in 2014.

Finally, with regard to civil claims, persons whose privacy rights have been infringed have the ability to obtain financial compensation. However, as class actions do not exist in Switzerland in this area, private individuals are in most cases not capable of asserting financial damages in an amount that merits a claim. Thus, the risk of civil damages claims is in general rather low.

Currently and in practice, the most important risk of non-compliance with the FADP likely consists of reputational damages, particularly in cases of data losses/leaks and excessive processing activities. Of course, the operational and financial aspects of a business can also suffer from an adverse recommendation by the Commissioner (if confirmed by the courts) or a court decision (stemming from a civil claim) requiring the business to amend or cease certain processing activities. The risk of criminal sanctions and civil claims for damages, however, is rather low.

IV. Emerging Issues and Outlook

A. Proposed Reform of the FADP

After conducting an evaluation of the FADP, the Swiss Federal Council has decided (text in German) that the FADP needs to be revised in order to adapt to technological and social developments and to remove certain practical issues that have arisen in relation

with its application. The reform of the FADP will be coordinated with current reform measures on the European Union (EU) level and within the Council of Europe.

On April 1, 2015, the Swiss Federal Council requested (text in German) the Federal Department of Justice and Police to draw up a preliminary draft by the end of August 2016. The purpose of reforming the FADP is in particular to strengthen the position of the Federal Data Protection and Information Commissioner and the rights of the data subjects in order to improve the enforcement of the FADP. The reform also aims at fostering the rules of good practice so that data protection principles are applied at an earlier stage. It remains to be seen if and to what extent the new General Data Protection Regulation (GDPR) of the European Union will influence the reform of the FADP. In any case, and due to the very broad scope of application of the GDPR, we expect that many companies located in Switzerland will in practice need to comply with the provisions of the GDPR if they wish to continue servicing customers located in the EU.

B. Cross-Border Transfer

The Federal Data Protection and Information Commissioner (Commissioner) addressed cloud computing and the disclosure of personal data outside Switzerland in his 22nd Annual Report for 2014/2015 (complete version in German; short version in English). Specifically, the Commissioner advised public bodies in Switzerland to refrain from using cloud providers headquartered in the United States or in other countries that do not offer a level of protection equivalent to that of Switzerland. This advice, however, is not backed up by the FADP, which allows the disclosure of personal data to countries that do not offer an equivalent level of protection of personal data, provided that certain exceptions apply (see Section I.D, above).

Interestingly, this aforementioned advice predated the European Court of Justice's ruling in *Schrems v. Data Prot. Comm'r*, No. C-362/14 (E.C.J., 2015), in which the ECJ declared the U.S.-EU Safe Harbor Framework to be invalid. In the wake of that ruling, the Commissioner issued press releases urging data processors to be especially cautious if data must be stored outside of Switzerland and declaring the U.S.-Swiss Safe Harbor Framework to be "invalid" as well. The Commissioner further advised those using products and services provided by American companies to enter into additional agreements to ensure better protection. It must be noted, however, that the Commissioner has no competence to declare the U.S.-Swiss Safe Harbor Framework to be "invalid." The Swiss Federal Council even decided not to suspend or cancel the U.S.-Swiss Safe Harbor Framework for the time being. It is at least questionable if transfers of personal data to recipients based in the U.S. that remain certified under the U.S.-Swiss Safe Harbor Framework could not continue to take place. This being said, in our view it is advisable to switch to a contractual solution until the new Privacy Shield is in place (see below).

The European Commission and the U.S. have agreed in the meantime on a new arrangement for transatlantic data flows: the EU-U.S. Privacy Shield. However, as the Article 29 Working Party has issued a negative opinion on the "draft" EU-U.S. Privacy Shield, it is not certain how this will in practice impact the time it will take the European Commission to adopt a final adequacy decision. This being said, once the EU-U.S. Privacy Shield is in place, it is expected that Switzerland and the U.S. will agree to a similar separate arrangement for personal data disclosed from Switzerland to recipients located in the U.S., which will replace the prior U.S.-Swiss Safe Harbor Framework. As it is not clear if and to what extent the new EU-U.S. Privacy Shield (and thus, implicitly, a new U.S.-Swiss Privacy Shield) will withstand a possible challenge in court, and taking into account the fact that the new EU-U.S. Privacy Shield will impose extensive obligations on U.S.-based recipients, it remains to be seen if the new EU-U.S. Privacy Shield (and a possible new U.S.-Swiss Privacy Shield) will in practice become a success and widely adopted by U.S.-based recipients.