DATA PROTECTION
LAWS OF THE WORLD
Switzerland
SWITZERLAND

LAW

The processing of personal data is mainly regulated by the Federal Act on Data Protection of June 19, 1992 (DPA) and its ordinances, ie, the Ordinance to the Federal Act on Data Protection (DPO) and the Ordinance on Data Protection Certification (ODPC).

In addition, the processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

It should be noted that the DPA has recently been subject to a substantial revision. On September 15, 2017, the Federal Council published the final draft and the dispatch to the Federal Parliament regarding the new DPA. In the summer of 2018, the revision was split into two parts. The first part relates to the implementation of the EU Directive 2016/680 in the context of the Schengen/Dublin treaty and has no immediate impact on data subjects (as it is generally limited to the federal authorities’ competencies in the context of administrative and judicial assistance in criminal matters). This part has come into force on March 1, 2019.

The second part is the actual comprehensive revision of the DPA (based on the draft legislation of September 15, 2017). The detailed consultation in Parliament started in June 2018. On September 25, 2020, the Parliament has approved the final text of the revised law. This concludes the legislative project to revise the DPA. The revised DPA is subject to an optional referendum. After the expiry of the 100-day referendum period, the Federal Council will decide on the entry into force. The revised DPA is not expected to enter into force before mid-2021. In addition, the revised implementing ordinances (in particular the revised DPO) have not yet been published. It should be noted, though, that the revised DPA does not provide for a transition period, but will become effective immediately upon its entry into force. The revision of the DPA aims to strengthen data protection in general and to align the DPA with the requirements of the EU General Data Protection Regulation (GDPR), in order to facilitate compliance of Swiss companies with those aspects of the GDPR that are applicable to controllers or processors outside of the EU, and to ensure that the EU will continue to consider Switzerland as providing an adequate level of data protection.

Territorial scope

Similar to the GDPR, the revised DPA states an extraterritorial effect, that is to say it may apply to events and circumstances having an impact in Switzerland even if they are initiated abroad.

In addition, the revised DPA foresees that private controllers domiciled abroad must designate a representative in Switzerland if they process personal data of data subjects in Switzerland and the data processing fulfils all of the following requirements:

- The data processing is connected to offering goods or services in Switzerland or to monitoring the behavior of data subjects in Switzerland.

- The processing is extensive.
The processing is regular.

- The processing involves a high risk for the personality of the data subjects.

For civil claims, the Swiss conflict of law rules apply.

**DEFINITIONS**

**Definition of personal data**

Personal data means all information relating to an identified or identifiable natural or legal person. It should be noted that data relating to legal entities falls within the scope of current Swiss data protection law, as opposed to most EU members’ data protection laws. Under the revised DPA data regarding legal entities will be exempted.

**Definition of sensitive personal data**

Sensitive personal data is defined as data on:

- Religious, ideological, political or trade union related views or activities
- Health, the intimate sphere or racial or ethnic origin
- Social security measures
- Administrative or criminal proceedings and sanctions

The revised DPA proposes that in addition genetic data and biometric data which unequivocally identifies a natural person be considered “sensitive personal data”.

"Personality profiles" are protected to the same extent under the current DPA as sensitive personal data. Personality profiles are collections of data that allow the appraisal of essential characteristics of the personality of an individual.

The revised DPA replaces the concept of "personality profiles" by the concept of "profiling", whereby the definition of "profiling" is substantially consistent with the definition under the GDPR. In addition, the revised DPA introduces the concept of "high-risk profiling" which is not limited to certain personal aspects relating to a natural person, but creates a pairing between data enabling an assessment of essential aspects of the personality of a natural person.

**NATIONAL DATA PROTECTION AUTHORITY**

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH - 3003 Berne Switzerland
T +41 (0)58 462 43 95
F +41 (0)58 465 99 96

The FDPIC 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.

The FDPIC informs the public about his findings and recommendations, and maintains and publishes the register for data files.

Under the revised DPA the FDPIC’s supervisory powers will be extended.

**REGISTRATION**

Under the current DPA the processing of personal data by private persons does not usually have to be notified or registered, respectively. However, private persons must register their data files before the data files are opened, if:

- They regularly process sensitive personal data or personality profiles, or
They regularly disclose personal data to third parties;

...and if none of the following exemptions applies:

- The data is processed pursuant to a statutory obligation.
- The Swiss Federal Council has exempted the particular processing from the registration requirement because it does not prejudice the rights of the data subjects (which the Swiss Federal Council has done in the DPO, *inter alia*, regarding data files from suppliers or customers, provided they do not contain any sensitive personal data or personality profiles).
- The data controller 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.
- The data is processed by journalists who use the data file exclusively as a personal work aid.
- The data controller has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files.
- The data controller has acquired a data protection quality mark under a certification procedure and has notified the FDPIC of the result of the evaluation.

The revised DPA provides for a general duty for controllers and processors to maintain a list of processing activities with certain minimal information, whereby the Federal Council may provide for exceptions for companies with less than 250 employees and whose processing entails only a low risk of infringing the personality of the data subjects.

**DATA PROTECTION OFFICERS**

There is no requirement under the current and the revised Swiss data protection law to appoint a data protection officer. However, under the current law a data controller can be dispensed from registering its data files if it has designated a data protection officer who:

- Carries out his / her duties autonomously and independently
- Has a certain level of expertise that is appropriate for the relevant data processing at the company (whereas it is not relevant whether or not the respective expertise was acquired in Switzerland)
- Must check and audit the processing of personal data within the company
- Must be in a position to recommend corrective measures when detecting any breaches of applicable data protection rules
- Must have access to all data files and all data processing within the company as well as to all other information that he/she requires to fulfill his/her duties
- Must maintain records of all data files controlled by the company and provide this list to the FDPIC or affected data subjects upon request, and
- May not carry out any other activities that are incompatible with his/her duties as data protection officer

The data controller must notify the FDPIC of the appointment of a data protection officer and thereupon such data controller will be listed on the public list of companies exempt from the requirement to register their data files.

The revised DPA also provides that controllers have the option to appoint a data protection officer whose contact data may be published and notified to the FDPIC. In such case, the controller has no obligation to consult with the FDPIC in the event that a data protection impact assessment indicates a significant risk to the personality or the fundamental rights of the data subject.

**COLLECTION & PROCESSING**

**Data Processing Principles**

The following principles apply to the collection and processing of personal data (whereby under current law personal data of legal entities is included):

- Personal data may only be processed lawfully, in good faith and according to the principle of proportionality. In addition, the revised DPA introduces the concepts of privacy by design and default.
- The collection of personal data and, in particular, the purpose of its processing must be evident to the data subject. In
addition, the revised DPA explicitly introduces the following duties on data controllers:

- Duty to inform the data subject on the collection of personal data similar as under the GDPR, with the list of minimum information being shorter (however providing for information on the countries of processing), but drafted more openly with a non-exhaustive list of minimum information;
- Under certain circumstances the duty to inform the data subject on decisions based solely on automated processing that have legal consequences or significant impact on the data subject (automated individual decision).

- Personal data should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, or provided for by law.
- The data controller and any processor must ensure that the data processed is accurate. Personal data must not be transferred abroad if the privacy of the data subject may be seriously endangered (see below).
- Personal data must be protected from unauthorized processing by appropriate technical and organizational measures.
- Personal data must not be processed against the explicit will of the data subject, unless this is justified by:
  - An overriding private or public interest, or
  - law, and
- Sensitive personal data or personality files must not be disclosed to a third party, unless this is justified by:
  - the consent of the data subject (which must be given expressly in addition to being voluntary and based on adequate information)
  - an overriding private or public interest

Whilst the current DPA does not provide for a formal duty to conduct a data protection impact assessment, the revised DPA introduces such formal obligation if the processing may constitute a high risk for the personality or the fundamental rights of the data subject (particularly when new technologies are used) and also defines specific cases where a data protection impact assessment is necessary, including in the event of processing sensitive personal data on a broad scale and systematic surveillance of extensive public areas. The FDPIC generally needs to be notified if the data protection impact assessment shows that the processing presents a high risk for the personality or fundamental rights of the data subject despite the measures envisaged by the controller.

Rights of the Data Subject

Data subjects enjoy certain rights to control the processing of their personal data:

Right of access

A data subject is generally entitled to request access to, and obtain a copy of, his or her personal data that is contained in a "data file" (or, under the revised DPA, that is being processed), together with prescribed information on the identity and contact details of the controller, the source of the data, the purpose of, and if applicable the legal basis for, the processing as well as the categories of personal data processed, the other parties involved with the file and the data recipients. The revised DPA foresees additionally that the period of storage of personal data (or the criteria used to determine such period) and, if applicable, the existence of an automated individual decision as well as the logic on which the decision is based is provided to the data subject. There are certain exceptions, e.g. a data controller may invoke its own overriding interests, however only if it does not disclose the personal data to third parties (whereby companies controlled by the same legal entity are not considered third parties under the revised DPA).

Right to rectify / Right to erasure / Right to restriction of processing / Right to object

Data subjects may generally require inaccurate or incomplete personal data to be corrected or complemented. In addition, the above-mentioned rights may arise from the general data protection principles, in particular the principle of proportionality (i.e. the data must only be processed to the extent and as long it is required to achieve the legitimate processing purpose). The revised DPA explicitly states that data must be erased or anonymized once it is no longer required to achieve the processing purpose.

Right to data portability

Whilst current data protection law does not explicitly provide for any right to data portability, the revised DPA introduces such a right similar as in the GDPR.
TRANSFER

Personal data may be transferred outside Switzerland if the destination country offers an adequate level of data protection. The FDPIC maintains and publishes a non-binding list of such countries (the revised DPA provides for binding adequacy decisions by the Federal Council). It should be noted that, under Swiss data protection law, remote access to data residing in Switzerland from outside of Switzerland is considered a transfer / disclosure abroad.

The FDPIC deems the data protection legislation of all EU and EEA countries to be adequate with regard to personal data of individuals. With regard to personal data of legal entities, only a few EU or EEA countries, such as Austria and Liechtenstein, and Argentina (for legal entities domiciled in Argentina), are deemed to provide an adequate level of data protection.

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if at least one of the following conditions is fulfilled:

- Sufficient safeguards, such as data transfer agreements, or other contractual clauses, ensure an adequate level of protection abroad. Data transfer agreements or other contractual clauses must be notified and submitted for approval to the FDPIC whereas mere information is sufficient if model clauses acknowledged by the FDPIC (such as the EU Standard Contractual Clauses for Controller-to-Controller or Controller-to-Processor Transfers, with the necessary amendments for Switzerland) are used.
- Until recently US companies that process data could be certified under the Swiss-US Privacy Shield regime and thereby make themselves subject to its rules. To do so, they had to register on the Department of Commerce (DOC) website privacyshield.gov/PrivacyShield/ApplyNow and meet the certification requirements. However, on September 8, 2020 the FDPIC issued an opinion concluding that the Swiss-U.S. Privacy Shield Framework does not provide an adequate level of protection for data transfers from Switzerland to the United States pursuant to the DPA. As a result of that opinion, organizations wishing to rely on the Swiss-U.S. Privacy Shield to transfer personal data from Switzerland to the United States should seek guidance from the FDPIC or legal counsel. That opinion does not relieve participants in the Swiss-U.S. Privacy Shield of their obligations under the Swiss-U.S. Privacy Shield Framework.
- Binding corporate rules that ensure an adequate level of data protection in cross-border data flows within a single legal entity or a group of affiliated companies. Such rules must be notified to the FDPIC.
- The data subject consents to the particular data export (consent must be given for each individual case or, according to legal doctrine and practice, for a number of cases under the same specific circumstances, eg, data export for certain specifically defined purposes; in contrast, a generic consent which does not further specify the circumstances under which data is disclosed is not sufficient). The revised DPA foresees that the consent must be explicit.
- The processing is directly connected with the conclusion or performance of a contract with the data subject. The disclosure is essential in order to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal rights before the courts (the revised DPA extends the derogations to include the establishment, exercise or enforcement of legal rights before other competent foreign authorities, i.e. not necessarily courts).
- The disclosure is required in order to protect the life or the physical integrity of the data subject (or, under the revised DPA, of a third party), or the data subject has made the personal data publicly accessible and has not expressly prohibited its processing.

SECURITY

The data controller and any processor must take adequate technical and organizational measures to protect personal data against unauthorized processing and ensure its confidentiality, availability and integrity. In particular, personal data must be protected against the following risks:

- Unauthorized or accidental destruction
- Accidental loss
- Technical errors
- Forgery, theft or unlawful use
- Unauthorized altering, copying, accessing or other unauthorized processing

The technical and organizational measures must be appropriate, in particular with regard to the purposes of the data processing,
the scope and manner of the data processing, the risks for the data subjects and the current technological standards. The DPO sets out these requirements in more detail. The revised DPO may impose additional or other minimum requirements.

BREACH NOTIFICATION

The current DPA does not impose an explicit statutory requirement to notify the FDPIC or the affected data subjects of data security breaches. However, depending on the scale and severity of a breach, a notification of the data subjects may be necessary based on the data controller’s and processor’s obligation to ensure data security (to avoid further damage), the principle of good faith or pursuant to contractual obligations.

The revised DPA introduces the obligation to notify the FDPIC of any data breach, however only if the breach is probable to result in a high risk to the personality rights or the fundamental rights of the data subject. The notification has to occur as soon as possible. In addition, a formal obligation to notify the data subject exists under the revised DPA in case that such notification is necessary to protect the data subject’s interests or if the FDPIC so requests.

ENFORCEMENT

Under current data protection law the FDPIC does not have specific direct powers to enforce the DPA. He may investigate cases on his own initiative or at the request of a third party and may issue recommendations that a specific data processing practice be changed or abandoned. If the FDPIC’s recommendation is not complied with, he may refer the matter to the Swiss Federal Administrative Court for a decision (as a recent example, in response to a health insurer’s practice to collect health data from policyholders via a mobile app and in turn providing cash or other monetary value to these policy holders, the FDPIC has recommended to the health insurer in April 2018, inter alia, to withdraw the mobile app from the market. The health insurer refused to implement the FDPIC’s recommendations and the FDPIC has subsequently referred the matter to the Swiss Federal Administrative Court for a decision).

The revised DPA extends the FDPIC’s supervisory powers: In particular, the FDPIC may under certain conditions initiate an investigation against a federal body or a private person and has the authority to issue orders and warnings. However, the FDPIC shall only investigate on cases if there are sufficient indications that any data processing is not in line with the requirements of the DPA.

The current DPA provides for criminal liability and fines of up to CHF 10,000 if a private person intentionally fails to comply with the following obligations under the DPA:

- Duty to provide information when collecting sensitive data and personality profiles
- Duty to safeguard the data subject’s right to information
- Obligation to notify the FDPIC with regard to contractual clauses or binding corporate rules in connection with data transfers abroad
- Obligation to register data files, or
- Duty to cooperate in an FDPIC investigation

Furthermore, the DPA provides for criminal liability and fines of up to CHF10,000 if a private person willfully discloses confidential, sensitive personal data or personality profiles that have come to his or her knowledge in the course of his or her professional activities, where such activities require the knowledge of such data, or in the course of his or her activities for a person bound by professional secrecy obligations or in the course of training with such a person.

Criminal proceedings must be initiated by the competent cantonal prosecution authority.

Under the revised DPA a number of violations of the DPA or lack of cooperation with the FDPIC can result in criminal fines of up to CHF 250,000 against responsible individuals (acting intentionally).

Finally, under Swiss civil law the data subject may apply for injunctive relief and may file a claim for damages as well as satisfaction and/or surrender of profits based on the infringement of his/her privacy.

ELECTRONIC MARKETING
Electronic marketing practices must comply with the provisions of the Swiss Federal Act against Unfair Competition (UCA).

With regard to the sending of unsolicited automated mass advertisement (which, in addition to emails, includes SMS, automated calls and fax message(s)), the UCA generally requires prior consent by the recipient, ie, 'opt-in'. As an exception, mass advertisings may be sent without the consent of the recipient:

- If the sender received the contact information in the course of a sale of his / her products or services
- If the recipient was given the opportunity to refuse the use of his / her contact information upon collection (opt-out), and
- If the mass advertising relates to similar products or services of the sender

In addition, mass advertising emails must contain the sender’s correct name, address and email contact and must provide for an easy-access and free of charge 'opt-out' from receiving future advertisements.

The UCA generally applies to business-consumer relationships as well as to business-business relationships, ie, mass advertisements sent to individuals and to corporations are subject to the same rules.

Direct marketing by telephone is lawful in Switzerland as long as it is not done in an aggressive way (eg, by repeatedly calling the same person). However, the UCA prohibits direct marketing by telephone to people who do not wish to receive commercial communication and have expressed that wish (ie, opted-out) by having their entry marked in the telephone books and online telephone registers (eg, through an asterisk next to their name).

In addition to the rules of the UCA, the general data protection principles under the DPA also apply with regard to electronic marketing activities, eg, the collection and maintenance of email addresses or processing of any other personal data.

**ONLINE PRIVACY**

The processing of personal data in the context of online services is subject to the general rules pertaining to the collection of personal data under the DPA. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is also subject to the Swiss Telecommunications Act (TCA).

Under the TCA, the use of cookies is considered to be processing of data on external equipment, eg, another person’s computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, eg, by configuring their web browser to reject cookies.

In addition, the general rules under the DPA apply where cookies collect data related to persons who are identified or identifiable, ie, personal data. The collection of personal data through cookies as well as the purpose of such a collection must be evident to the data subject. The personal data collected may only be processed for the purpose:

- Indicated at the time of collection
- That is evident from the circumstances, or
- That is provided for by law

Where the personal data collected through a cookie is:

- Considered sensitive data, eg, data regarding religious, ideological, political views or activities, or
- So comprehensive that it forms a personality profile, ie, permits an assessment of essential characteristics of the personality of a person, or (under the revised DPA) is considered resulting from high-risk profiling

The stricter rules pertaining to the processing of sensitive personal data are applicable.

These stricter rules provide, inter alia, that the data subject must be informed of:

- The identity of the data controller
- The purpose of data processing, and
- The categories of data recipients if the data shall be disclosed to third parties.
Further, in relation to the processing of sensitive personal data or personality profiles, or (under the revised DPA) in relation to high-risk profiling implied consent is not sufficient; consent must be given expressly.

**KEY CONTACTS**

Schellenberg Wittmer Ltd
www.swlegal.ch/

**Roland Mathys**  
Partner / Attorney at Law  
T +41 (0)44 215 3662  
roland.mathys@swlegal.ch

**Samuel Klaus**  
Partner / Attorney at Law  
T +41 (0)44 215 3695  
samuel.klaus@swlegal.ch

**Claudia Jung**  
Associate / Attorney at Law  
T +41 (0)44 215 3498  
claudia.jung@swlegal.ch

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2021 DLA Piper. All rights reserved.