VISCHER

SWISS DPA: COMPARISON WITH THE GDPR

Authors: David Rosenthal, Samira Studer, David Hausmann, VISCHER AG

Preliminary remark: The Swiss Federal Act on Data Protection of June 19, 1992 ("**old DPA**") has been completely revised and on September 25, 2020, the Swiss Parliament passed the new law ("**DPA**", together "**Swiss DPA**", accessible here). The DPA and its implementing Ordinances, including the Swiss Ordinance on Data Protection ("**DPO**", accessible here) came into force on September 1, 2023, with no relevant transition period.

The following table is intended to provide an overview of the main differences between the DPA and the GDPR, while also commenting on the differences between the old DPA and the DPA, where relevant. Please note that only the provisions applicable to the private sector will be commented on, i.e. excluding those applicable to Swiss federal public authorities (note that that private sector organizations may be required to comply with the DPA rules for federal authorities if they fulfill a public function, for example as a pension fund).

GDPR	DPA
Definition of personal data (Art. 4(1) GDPR)	Comparable. The DPA provides essentially the same definition of personal data as the GDPR. As under the GDPR, only data relating to natural persons are covered by the DPA (Art. 5(a) DPA). Personal data relating to legal entities are no longer protected under the DPA (this Swiss peculiarity has been abandoned with the revision). In Switzerland, we follow the "**relative approach**" to personal data in the sense that for data to be considered personal data, the relevant person must not only be reasonably able to identify the data subject to whom the information relates (objective component), but also be willing to undertake the necessary efforts to do so (subjective component). Accordingly, if personal data is securely encrypted or otherwise pseudonymized, it is no longer considered personal data to those who are unable to decrypt it or reidentify the data subjects with reasonable efforts. Hence, the same information may be personal data for one party, but not for other ones.
Territorial scope (Art. 3 GDPR)	Different. The territorial scope of the Swiss DPA is broader than that of the GDPR. The Swiss DPA has two types of provisions with different rules for determining the territorial scope, namely: • *Private law* provisions (e.g., the basic rules of pro-

Questions: dataprivacy@vischer.com

GDPR	DPA
	cessing, the rights of data subjects); and • *Public law* provisions (e.g., information and notification obligations, the obligation to conduct a data protection impact assessment under the DPA, provisions governing investigations by the Swiss data protection authority). The application of **the private law provisions** of the Swiss DPA is conditional upon a data subject being able to enforce them against the controller, its processor or any other party involved in the processing of the personal data at issue. This is the case when a data subject can bring a civil claim before a Swiss court and have such court apply the Swiss DPA: • Jurisdiction over claims of foreign data subjects is established according to Swiss Private International Law (Art. 129(1) Federal Private International Law Act (PILA), Art. 5(3) Lugano Convention). Specifically, jurisdiction in Switzerland is: o At the defendant's domicile in Switzerland; o For claims based on the activities of a business establishment in Switzerland, at the relevant business establishment in Switzerland; or o At the place where the harmful act took place or the result of this act occurred in Switzerland. • Once jurisdiction is established in Switzerland, Swiss private international law allows a data subject claiming a violation of his or her data protection rights to have Swiss law, including the Swiss DPA, apply to him or her if (Art. 139(1) and (3) PILA): o The data subject has his or her habitual residence in Switzerland, provided that the perpetrator should have expected the result to occur in Switzerland; o The perpetrator has its business establishment or habitual residence in Switzerland; or o The results of the harmful act occurred in Switzerland, provided that the perpetrator should have expected the result to occur in Switzerland. The application of the **public law provisions** of the Swiss DPA is determined on the basis of the principle of territoriality, part of which is the so-called "effects doctrine" (now expressly regulated in Art. 3(1) DPA). According to the "**effects doctrine**", the public law provisions of the Swiss DPA apply to situations that, although they occur abroad, have a significant impact (effect) in Switzerland. This means that if a data processing operation

GDPR	DPA
	is carried out abroad but has a relevant effect in Switzerland – if only because the server is operated in Switzerland or because the data subjects are in Switzerland – that part of the operation (the "effect") takes place in Switzerland, which is sufficient for the entire operation to be assessed under the Swiss DPA, irrespective of where the data processing takes place or where the controller is located. In other words, the Swiss DPA applies to foreign controllers who process personal data abroad if such processing has a relevant *effect* in Switzerland. This concept is comparable to the provisions of the GDPR concerning the jurisdiction of national data protection authorities.
Processing Principles (Art. 5(1) GDPR)	Comparable. The Swiss DPA in Art. 6 provides for more or less the same processing principles as found in Art. 5(1) GDPR. This includes the principle of lawfulness and fairness, the principle of purpose limitation, the principle of data minimization, the principle of accuracy and the principle of storage limitation. The principle of transparency is not expressly mentioned in Art. 6 DPA but considered to be part of the principle of "processing personal data in good faith", which is the Swiss equivalent to the fairness principle. The principle on lawfulness under Swiss law means that personal data shall not be processed by breaching other laws; it does not refer to the requirement of a legal basis (see below). The principle of integrity and confidentiality is provided for as a separate provision in Art. 8 DPA ("data security"). With regard to the principle of accountability, see below.
Legal basis for processing personal data (Art. 6(1) GDPR)	Different. The Swiss DPA follows a different concept than the GDPR. Under the Swiss DPA, no "legal basis" (so-called "justification", i.e. the Swiss equivalent of the GDPR legal basis under Art. 6/9) is in principle required to lawfully process personal data. Thus, a justification is *only* required *if* the processing of personal data results in a violation of the personality of the data subjects (Art. 30(2) DPA), i.e. if alternatively: • The processing principles (Art. 6 and 8 DPA) are not complied with; • The data subject has expressly objected to the processing; or • Sensitive personal data is disclosed to a third party. If one of the above alternatives applies and a justification

GDPR	DPA
	is required, such justification exists if (Art. 31(1) DPA): • The data subject has consented to the processing; • Swiss (federal, cantonal or municipal) law provides for such processing; or • An overriding private or public interest justifies such processing. The "overriding private interest" test under the DPA is comparable to the "legitimate interest" test under the GDPR, except that under the DPA, an overriding private interest can also be used to justify the processing of *sensitive* personal data. It should be noted, however, that no justification is in principle required if the data subject has made the personal data accessible to everyone and has not expressly objected to the processing (Art. 30(3) DPA).
Requirements for valid consent (Art. 4 (11) and Art. 7 GDPR)	Different. The requirements for valid consent under the Swiss DPA are not as strict as those under the GDPR. Under the Swiss DPA, a valid consent is one that is given voluntarily upon provision of adequate information ("**informed consent**"). It is effective if it was given prior to the processing. Implied consent may be sufficient in certain circumstances, for e.g., if it occurs in the context of an existing contractual relationship and the terms and conditions specifically provide for such implied (or "presumed") consent. However, the fact that a data subject does not object to a particular processing of his or her personal data or to a notice of such processing is generally not sufficient to presume consent. Also, implied consent does not apply to sensitive personal data or profiling "involving a high risk" (i.e. profiling that results in a personality profile and carries a high risk of negative consequences for the data subject). In both cases, if consent is required in a particular case, it must be *explicit* (Art. 6(7)(a) and (b) DPA). Explicit does not mean that consent must be given in writing, but for evidentiary purposes, it is recommended to ask for written consent (also in the case of non-sensitive personal data). Furthermore, contrary to the provisions of the GDPR, boxes can be pre-ticked on forms that contain an "acceptance" button and a consent declaration can be included in a contract if it has a factual connection to the contract. Thus, under the Swiss DPA, there is no prohibition on linkage within the meaning of Art. 7(4) GDPR. Finally, the validity of consent does not require to inform the data subjects of their right to withdraw consent at any time.

GDPR	DPA
Processing special categories of personal data (Art. 9 GDPR) and disclosure to third parties	Different. The Swiss DPA follows a different concept than the GDPR. Under the Swiss DPA, no "legal basis" (so-called "justification", i.e. the Swiss equivalent of the GDPR legal basis under Art. 6/9) is in principle required to lawfully process "sensitive personal data". The term "sensitive personal data" in Art. 5(c) DPA is slightly broader than the "special categories of personal data" in Art. 9 GDPR. Under the Swiss DPA, "sensitive personal data" also includes data on administrative or criminal proceedings and sanctions (which are partly regulated in Art. 10 GDPR), data on social security measures and data on the intimate sphere (only data concerning a natural person's sex life or sexual orientation is covered under Art. 9 GDPR). As under the GDPR (but unlike the old DPA), genetic data and biometric data that unequivocally identifies a natural person are also considered "sensitive personal data" under the DPA. The DPA no longer uses the Swiss concept of "personality profiles" (which under the old DPA is treated as sensitive personal data); this concept has been replaced by "profiling", the definition of which is comparable to the GDPR. The DPA also introduces the concept of profiling "involving a high risk" (i.e. profiling that results in a personality profile and carries a high risk of negative consequences for the data subject). Contrary to what has been generally reported, the DPA does not provide that profiling requires consent. What the DPA does say is that if consent is required in a particular case, such consent must be explicit in the case of profiling "involving a high risk" (Art. 6(7)(b) DPA; see above). Generally speaking, the Swiss DPA follows a "**risk-based approach**" with respect to the processing of personal data, meaning that the higher the risks for the data subjects, the stricter the general data processing principles must be applied. Hence, the processing of sensitive personal data must generally meet higher standards than the processing of personal data that involves lower risks. Furthermore, sensitive personal data may only be disclosed to third parties in their capacity as controllers if (Art. 30(2)(c) and 31(1) DPA): • The data subject has consented to the processing; • Swiss (federal, cantonal or municipal) law provides for such processing; or • An overriding private or public interest justifies such processing. Note that, unlike the GDPR, an "overriding private interest"

GDPR	DPA
	can also be invoked to justify the processing of sensitive personal data (see above).
Information to data subjects (Art. 13 and 14 GDPR)	Different. The information obligation under the DPA goes less far than the enhanced transparency information required under Art. 13/14 GDPR, with two exceptions: Unlike the GDPR, the privacy notice must also contain a list of the countries or international bodies to which personal data is transferred (see vi below) and the safeguards or exemptions relied upon by the controller in case of exports to non-whitelisted countries (see vii below). Specifically, under Art. 19 DPA, the controller must provide at least the following information: (i) the identity and contact details of the controller, (ii) the identity and contact details of its data protection advisor and representative, if any (Art. 10(2) and 14(2) DPA) (iii) the categories of personal data collected, unless the data is collected directly from the data subject, (iv) the purposes of processing, (v) the recipients or categories of recipients of the personal data, if any, (vi) the name of the countries or international bodies to which personal data is disclosed, if any, (vii) the safeguards or exemptions relied upon in case of exports to non-whitelisted countries and (viii) automated individual decisions that have legal consequences for the data subject or that materially and negatively affect him or her, unless an exception applies (Art. 21(1) and (3) DPA; see below). In exceptional cases, the controller must provide additional information if this is necessary to ensure an adequate level of transparency and permit data subjects to exercise their rights (this provision is generic, but is likely not to go beyond what is provided for in Art. 13/14 GDPR). Art. 20 DPA defines a number of cases in which no information or limited information must be provided by the controller, namely: (i) where the data subject already has the information, (ii) where the processing is required under Swiss law, (iii) where the controller is a private person bound by a statutory confidentiality obligation, (iv) where the controller can rely on certain media privileges, (v) in case of indirect data collection, if informing the data subject is not possible or would require a disproportionate effort, (vi) in case of an overriding third party interest, and (vii) in case of an overriding private interest of the controller, provided that no data is shared with third party controllers (except for group companies, Art. 20(4) DPA).
Data subject rights (Art. 15-22 GDPR)	Comparable. The rights of data subjects *vis-à-vis* the controller are basically the same, with some Swiss peculiarities (see below). **Right of Access**

GDPR	DPA
	The concept is the same (Art. 25-27 DPA), but the list of additional information that can be requested is shorter, while at the same time other information must be provided that the GDPR does not require (e.g., the list of export countries including the legal basis for the transfer of data and the right of access to "useful" information). Additionally, the grounds to refuse, restrict or defer the right of access are slightly different than those under the GDPR in that the controller may do so if (i) a formal law provides for it, in particular to protect a professional secret, (ii) it is required by prevailing interests of third parties, (iii) the request for information is manifestly unfounded in particular if it pursues a purpose that is contrary to data protection (typically understood as meaning "not for data protection purposes") or is obviously of a frivolous nature, or (iv) it is required by its own overriding private interest (e.g., business secret), provided, however, that the controller has not been sharing data with another (sole) controller. Furthermore, unlike the GDPR, individuals responding to an access requests may themselves be subject to criminal sanctions if they provide an incorrect or incomplete response (see below). The information must in principle be given to the data subjects within 30 days and free of charge, unless the efforts required to do so would be disproportionate, in which case fees of up to CHF 300 may be incurred (Art. 19 DPO). According to Art. 16(5) DPO, reasonable measures must be taken in order to identify the person seeking information while that person is required to cooperate. **Right to Objection, Erasure and Restriction** The same data subjects' rights exist under the Swiss DPA, but the situation in Switzerland is much easier than under the GDPR: The data subject has the right to object to any aspect of a processing activity (e.g., the use of the data for a certain period of time, the retention period of the data, and the way the data was collected). Once such an objection request is received, the controller has to determine whether it has an overriding private or public interest or a binding consent (i.e. a consent that you cannot withdraw without commercial consequences, see Decision of the Swiss Federal Supreme Court 136 III 401) or whether it can rely on a provision of Swiss law to justify ignoring the objection and continuing with the processing. In the absence of such a justification, the controller must stop the processing activity in question, delete the data, stop disclosing it to a third party, etc. The Swiss version of the "right to object" already includes the right to erasure and the right to restriction (e.g., you can object to your data being stored any longer). **Right to Rectification** The data subject has the right to rectification. There are

GDPR	DPA
	very limited exceptions to the right to rectification (i.e. legal obligation and archival purpose of public interest). If the accuracy of the personal data in question cannot be established, the data subject can request the controller to put a note in the file that he or she claims the data to be inaccurate. **Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing** Unlike Art. 19 GDPR, there is no obligation to notify each recipient to whom the personal data has been disclosed that the data subject has exercised his or her right to rectification, erasure or restriction with respect to the personal data that the recipient has received. **Right to Data Portability** The DPA introduces a right to data portability that is inspired by, but differs from, the GDPR. Under the DPA, the data subject can request from the controller, usually free of charge, the release of his or her personal data in a common electronic format or its transfer to another controller, if the controller processes the data automatically and the data is processed with the consent of the data subject or in direct connection with the conclusion or execution of a contract. **Automated Individual Decision-Making** The DPA regulates automated individual decision-making, but the rules are slightly different from the GDPR (and do not include profiling). In principle, an information obligation applies when decisions are based exclusively on automated processing and have legal consequences for the data subject or otherwise significantly impair him or her, unless the decisions are (i) taken with the explicit consent of the data subject or (ii) occur in connection with the conclusion or performance of a contract with the data subject with the decision actually approving the data subject's request (Art. 21(3) DPA). There is therefore no prohibition of such decision-making, but a right for the data subject to have a human being review the automated individual decision (i.e. right to be heard by a human being or right to human intervention) (Art. 21(2) DPA). **Right to Withdraw Consent** As under the GDPR, the data subject has the right to withdraw consent at any time, if the processing is based on his or her consent (but unlike the GDPR, this right does not have to be communicated to the data subject; see above). In some circumstances, even if the data subject has withdrawn his or her consent, it may still be possible to justify a particular processing of personal data on the basis of an overriding private interest of the controller, the data subject or another party. However, the controller may suffer

GDPR	DPA
	reputational harm if it gives the impression to the data subject that he or she can stop the processing of his or her data at any time by withdrawing consent, when in fact this is not the case. See also the Decision of the Swiss Federal Supreme Court 136 III 401 on the possibility of restricting the withdrawal of consent under Swiss law, in particular if the consent was given as part of an economic transaction.
Joint controllers (Art. 26 GDPR)	Different. Unlike the GDPR, the Swiss DPA does not require joint controllers to enter into an "arrangement" to govern their relationship. That said, in practice, joint controllers subject to the Swiss DPA generally conclude such an "arrangement" because it helps them clarify their respective roles and responsibilities with respect to the joint processing at issue and the exercise of data subjects' rights.
Local representatives (Art. 27 GDPR)	Different. Under the DPA, private controllers with their seat out-side of Switzerland are required to appoint a representative in Switzerland, if cumulatively (i) they process personal data of data subjects in Switzerland, (ii) the data processing is in connection with offering them goods or services in Switzerland or monitoring their behavior, (iii) the data processing is extensive, (iv) it occurs on a regular basis, and (v) it involves a high risk for the personality of such data subjects (Art. 14 DPA). In our opinion, a Swiss representative will be necessary in far fewer cases than a representative pursuant to Art. 27 GDPR; the provision mainly aims at the large U.S. tech companies that offer online services in Switzerland.
Processors (Art. 28 GDPR), others working under instructions (Art. 29 GDPR)	Comparable. The DPA adopts the GDPR concept of processors (Art. 9 DPA). However, the DPA does not provide for detailed requirements regarding data processing agreements as does the GDPR. GDPR-compliant data processing agreements continue to be compliant with the DPA, but it is recommended to add references to the Swiss DPA (in addition to the GDPR), to ensure that data exports from Switzerland (in addition exports from the EU) are also covered and that if the data processing agreement requires the use of the EU Standard Contractual Clauses for international transfers they are amended for compliance with the DPA. As opposed to Art. 28 GDPR, the DPA does not contain an equivalent to Art. 29 GDPR. In practice, those who would fall under Art. 29 GDPR are often treated in the same manner as set forth in Art. 9 DPA (or, in effect, as per Art. 29 GDPR): The controller or processor will typically have to ensure that these persons will follow its instructions with regard to the processing of personal data, keep it secure

GDPR	DPA
	and not use it for own purposes.
Records of processing activities (Art. 30 GDPR), Accountability (Art. 5(2) GDPR)	Different. **Records of Processing Activities (ROPA)** The DPA (unlike the old DPA) also requires controllers and processors to maintain a record of processing activities with the same content as under the GDPR, *plus* an indication of the countries and international organizations to which personal data is disclosed and the safeguards or exemptions relied upon for data exports to non-whitelisted countries. On the other hand, the contact details of the representative and data protection officer, if any, are not required. According to Art. 24 DPO, private companies and organizations with less than 250 employees (headcount) on January 1st of any given year, as well as natural persons, are exempt from this obligation, unless they (i) process sensitive personal data on a large scale or (ii) conduct high-risk profiling. **Audit Trails** Art. 4 DPO requires private organizations to log their data processing activities (i.e. storage, modification, disclosure, deletion and destruction of personal data) if (a) they (i) process sensitive personal data on a large scale or (ii) engage in high-risk profiling and (b) there are no measures in place to ensure an adequate level of data protection. The audit trails must contain information about the identity of the user, among other things, and has to be retained for at least one year and separated from the system for which the audit trail has been created. The log shall permit the controller to verify, among other things, whether the data has been processed in compliance with the DPA and in case of data breaches. **Processing Policy** According to Art. 5 DPO, private organizations that (i) process sensitive personal data on a large scale or (ii) engage in high-risk profiling they must maintain what is referred to a "processing policy" or "processing regulation", which is a document that describes the internal organization, data processing and activities controlling such processing, as well as measures taken to ensure data security. This is comparable to the "accountability" principle under the GDPR, but does not go as far in practice. Beyond that, there are no other provisions that match Art. 5(2) GDPR. This is why the Swiss DPA is generally not considered to provide for the principle of accountability.
Technical and organizational measures (Art. 32 GDPR)	Comparable. The data security obligations are comparable to those under the GDPR, with the controllers and processors being

GDPR	DPA
	required to implement and maintain a level of data security that is adequate to the potential risks by implementing appropriate technical and organizational measures (Art. 8 DPA). However, unlike the GDPR, the DPA does not detail any particular method of data security (e.g., pseudonymization, encryption). Rather, the DPO goes further in defining the expectations with regard to data security. These include, in particular, the following measures: (i) access control, (ii) user control, (iii) storage control, (iv) transport control, (v) data integrity, (vi) system security, (vii) input control as well as (viii) measures to detect and eliminate consequences arising from data breaches.
Data protection by design and default (Art. 25 GDPR)	Comparable. **Data protection by design** The requirement of data protection by design is comparable to Art. 25(1) GDPR. It already existed under the old DPA where it was combined with the requirement to have the necessary measures in place to prevent any unauthorized processing. It is important is reduced under the new law by the fact that there is no direct consequence for a controller not complying with it. **Data protection by default** The requirement of data protection by default is only broadly comparable to the concept under the GDPR. The Swiss implementation is much narrower in that it only applies to pre-defined privacy settings (e.g., in an app or on a website) that are relied upon for processing personal data before the data subject is given the opportunity to change them. It does neither require a controller to implement such settings nor does it apply where the data subject is asked for its choice before the processing starts.
Notification of data breaches (Art. 33 and 34 GDPR)	Different. While the data breach notification obligations are comparable to those provided under the GDPR, the thresholds are higher (for notification to the Swiss data protection authority), respectively different (for notification to the data subjects) than under the GDPR. This can result in a situation where under Swiss law it is necessary to notify a data subject, but not the supervisory authority. Note that other Swiss laws also contain notification obligations in cases of data breaches or cyber attacks, e.g., for regulated financial institutions and, soon, critical infrastructures. **Notification to the Federal Data Protection and Information Commissioner (FDPIC, website here)** The controller is required to notify a data breach (defined in the same way as under the GDPR) to the FDPIC only if

GDPR	DPA
	the breach is likely to result in a *high risk* for the personality of the data subject (Art. 24(1) DPA). The notification must be made "as soon as possible" (with no fixed maximum time limit as under the GDPR) and must include the following information (Art. 24(2) DPA, Art. 15 DPO): • the nature of the breach; • where possible, the time and duration; • where possible, the categories and approximate number of personal data concerned; • where possible, the categories and approximate number of individuals affected; • the consequences, including the risks, for the persons concerned; • what measures have been taken or are planned to remedy the deficiency and minimize the consequences, including any risks; • the name and contact details of a contact person. The FDPIC has set up an (optional) data breach reporting portal for the notification of such data breaches (but only accepts notifications where the controller expressly qualifies the breach as being a "high risk" one): https://databreach.edoeb.admin.ch/report. **Notification to the data subjects** Additionally, the controller has to inform the data subject, "*if this is necessary for his or her protection*" (e.g., because the notification allows the data subject to take precautionary steps such as changing his or her password or watching out for incorrect credit card charges) or if the FDPIC so requires (Art. 24(4) DPA, Art. 15(3) DPO). Under certain conditions (e.g., a statutory obligation of confidentiality), the notification to the data subject may be delayed, limited or even not made at all (Art. 24(5) DPA). On the other hand, processors are required to inform controllers of data breaches (of any severity) as soon as possible (Art. 24(3) DPA). There is no general duty to keep a record of data breaches as required under the GDPR. However, records must be kept for two years with regard to those breaches that have been notified to the FDPIC (Art. 15(4) DPO).
Data protection impact assessments (DPIA) (Art. 35 and 36 GDPR)	Comparable. The obligation to conduct a data protection impact assessment (DPIA) is comparable to the one provided under the GDPR. Like under the GDPR, the DPA introduces an obligation upon controllers to perform and document a DPIA if their

GDPR	DPA
	intended processing may result in a high risk for data subjects (e.g., if the processing involves a large amount of sensitive personal data or if public areas are systematically monitored) (Art. 22(1) and (2) DPA). Limited exemptions exist for controllers if they for e.g. process personal data on the basis of a legal obligation under Swiss law or follow certain codes of conduct. The DPIA has to include a description of the processing, an assessment of the risks involved for the data subject and the measures undertaken or planned to protect the data subject (Art. 22(3) DPA). Should the DPIA reveal that, despite the measures taken or to be taken, the risks for the data subjects remain high, the FDPIC must be consulted (unless this consultation can be done with the controller's own "data protection advisor"; see below). The DPIA has to be retained for at least two years after the completion of the data processing activity (Art. 14 DPO).
Obligation to appoint a data protection officer (DPO) (Art. 37 GDPR)	Different. There is no formal obligation to appoint a data protection officer for private controllers. However, the DPA provides for the possibility for private controllers to appoint a voluntary data protection officer (referred to as a "data protection advisor"). If such data protection advisor fulfills the requirements provided under the DPA (which are comparable prerequisites to the GDPR data protection officer), the controller is not obliged to consult the FDPIC in case of a data protection impact assessment entailing a high risk for the data subject (see above), but may consult its data protection advisor instead (Art. 23(4) DPA). As under the GDPR, the data protection advisor must have the necessary expertise and shall exercise their function in a professionally independent manner and not bound by instructions (Art. 10(3) DPA). Their contact details are published and must be reported to the FDPIC (Art. 10(3)(d) DPA). They serve as a contact point for the FDPIC, shall train and advise the private controller and assist in data protection compliance matters (Art. 10(2) DPA).

Transfer of personal data to third countries (Art. 44-49 GDPR), in particular with regard to transfers to the EU	Comparable. Like the GDPR**,** an organization transferring personal data to a country or territory outside Switzerland must comply with the transfer requirements of the DPA and ensure that the organization has taken appropriate steps to ensure that personal data is adequately protected. Although the DPA does not define data exports in exactly the same manner as does the GDPR, Art. 16 et seq. DPA and Chapter V of the GDPR are applied, in essence, in a very similar manner and in the same scenarios. As with the GDPR, the DPA draws a distinction between transfers to jurisdictions deemed to provide an adequate level of protection ("**whitelisted jurisdiction**") and those that do not. Annex 1 to the DPO contains a list of all the whitelisted jurisdictions as decided on by the Swiss Federal Council. It is comparable to the adequacy decisions of the European Commission, but currently the Swiss list does not include Japan and South Korea. Transfers to U.S. companies certified under the CH-US Data Privacy Framework are expected to be listed soon under Annex 1. **Restricted Transfers** Transfers of personal data to a jurisdiction or territory outside Switzerland which is not a whitelisted jurisdiction is subject to additional requirements under the DPA ("**restricted transfer**"). A restricted transfer is only permitted if: • there are sufficient safeguards in place to compensate for such lack of protection (Art. 16(2) DPA); or • one of the exceptions set out in the DPA applies (Art. 17 DPA). The **sufficient safeguards** are the following: • a treaty under international law; • data protection clauses in an agreement between the controller or the processor and its contractual partner, notice of which has been given to the FDPIC beforehand; • specific guarantees drawn up by the competent federal body, notice of which has been given to the FDPIC beforehand; • standard data protection clauses that the FDPIC has approved, issued or recognized beforehand (such as the European Commission's Standard Contractual Clauses, with amendments for the Swiss DPA, as published by the FDPIC); or • binding corporate rules that have been approved in advance by the FDPIC or by the authority responsible for

GDPR	DPA
	data protection in a jurisdiction that guarantees an adequate level of protection (e.g., all EEA countries). The FDPIC has followed a similar approach concerning **Transfer Impact Assessments** (TIAs) as have done the supervisory authorities under the GDPR. The exceptions listed in the DPA are the following (and, thus, comparable to the **derogations** in Art. 49 GDPR): • the data subject has explicitly consented to the disclosure; • the disclosure is directly connected with the conclusion or performance of a contract: 1. between the controller and the data subject; or 2. between the controller and its contractual partner in the interests the data subject. • the disclosure is necessary in order to: 1. safeguard an overriding public interest; or 2. establish, exercise or enforce legal rights before a court or another competent foreign authority. • the disclosure is necessary to protect the life or the physical integrity of the data subject or a third party, and it is not possible to obtain the consent of the data subject within a reasonable time; • the data subject has made the data generally accessible and has not explicitly prohibited processing; • the data originate from a statutory register that is public or accessible to per-sons with a legitimate interest, provided the statutory requirements for access are met in the case concerned. Under the DPA, remote access to data stored in Switzerland from outside of Switzerland is considered a disclosure of data abroad. Publications on websites, however, are not. This is comparable to the GDPR.
Liability for damages (Art. 82 GDPR)	Different. Under the Swiss DPA, any person who participates in a data processing activity that violates the personality of a data subject may be held civilly liable, whether that person acted intentionally or negligently. This includes employees and other persons integrated in the company who are neither processors nor controllers (e.g., consultants or agents within the meaning of Art. 29 GDPR, although there is no similar provision in the DPA), to the extent that they can be held liable for the violation of the personality of the data subject.

GDPR	DPA
	As for criminal liability, the fines are directed at the responsible individuals, *not* the companies (see below).
Administrative fines (Art. 83 GDPR)	Different. Under the DPA, criminal fines are directed at the responsible individuals (see below), not the companies. According to the majority opinion, it is not possible to insure against this risk and companies cannot pay the fines on behalf of the individual. However, in cases where the identification of the responsible individual acting within a company would require a disproportionate effort and the expected fine does not exceed CHF 50'000, it is possible to fine the company instead (Art. 64 DPA). The individuals exposed to such fines are: • Those who actually committed the breach (see below); • Those who had the obligation and power to prevent the breach or mitigate its consequences, but failed to do so (e.g., the board of directors, management, superiors). The catalog of fines has been significantly expanded in comparison to the old DPA. Specifically, under the DPA, individuals acting for private controllers may be fined for up to CHF 250'000 if they: (i) breach their privacy notice obligations or right of access obligations by intentionally providing wrong or incomplete information, (ii) intentionally fail to provide certain information required under their privacy notice obligations or provide wrong information, (iii) intentionally refuse to cooperate with the FDPIC or intentionally provide him or her wrong information, (iv) intentionally make available personal data to a foreign recipient in violation of the restrictions on such data exports, (v) in their capacity as controllers delegate the processing of data processing to a processor intentionally in violation of the DPA's preconditions (except for the obligation to maintain control over the appointment of sub-processors), (vi) intentionally fail to comply with the minimum data security requirements defined by the Federal Council (it is not clear what they really are; whereas the DPO defines a number of requirements, the majority view is that they are too generic to serve as a legal basis for fining responsible person's non-compliance with them) or (vii) intentionally fail to comply with an order of the FDPIC. Violations of the processing principles of the DPA, on the other hand, continue to be exempt from punishment – an important difference to the GDPR. The same applies to the failure to make a data breach notification, to undertake a data protection impact assessment or to maintain a records of processing activities. The fines are not issued by the FDPIC, but by the cantonal

GDPR	DPA
	criminal authorities (which are not specialized in data protection). The DPA also introduced a broad obligation of professional secrecy and a new provision sanctioning identity theft.
Other sanctions including criminal law (Art. 84 GDPR)	Different. **Imprisonment** More severe criminal sanctions may apply to violations of professional secrecy provided by the Swiss Penal Code and other Swiss laws (e.g., the Swiss Banking Act). In addition, the Swiss Penal Code provides that a person who obtains sensitive personal data from a non-public data collection without authorization can be punished by imprisonment or fined. **Compensation** Data subjects may claim for damages, satisfaction and/or surrender of profits if their personality has been violated without sufficient justification. Damages and satisfaction may only be claimed in cases of negligence or willful intent. The prerequisites for claims for surrender of profits are not entirely clear for violations of personality, but it is likely that a claim will only be possible in the case of bad faith behavior. **Expanded Enforcement Powers of the FDPIC** The enforcement of the Swiss DPA will also change under the DPA. Under the old DPA, the FDPIC is only able to issue "recommendation" to controllers and processors who, in his opinion, do not comply with the old DPA and can sue them if they do not comply with his recommendation. Under the DPA, the FDPIC is granted more extensive powers: He can conduct investigations *ex officio* (if there are sufficient indications that a processing activity is done in violation of the DPA) or upon complaint, collect evidence and issue orders indicating how personal data is to be processed by a particular controller or processor (and which become binding if they are not successfully appealed by the addressee). The FDPIC can also order the processing to be suspended or terminated, as well as compliance with various provisions of the DPA. The FDPIC may issue a "warning" if the person targeted takes the necessary measures to restore compliance with the DPA during the investigation. If necessary, the FDPIC can issue temporary restraining orders. Recourse is possible to the Swiss Federal Administrative Court. However, the FDPIC still cannot impose fines, which remains the competence of the cantonal enforcement authorities (which are not specialized in data protection).
Apart from the above	Yes.

GDPR	DPA
general data protection regime, are there any specific data protection provisions in the field of employment law in Switzerland?	With respect to the processing of personal data of employees, Art. 328b of the Swiss Code of Obligations applies in addition to the Swiss DPA. This provision provides that an employer may handle employee data only to the extent it concerns the employee's suitability for his or her job or is necessary for the performance of the employment contract. In our view, this provision is a concretization of the principle of proportionality and its violation can be justified in individual cases. Other views, however, consider this provision to be a general obligation, the violation of which cannot be justified. Furthermore, Art. 26 of the Ordinance on Employment Act 3 prohibits the use of systems that monitor the behavior of employees at the workplace. If monitoring or control systems are necessary for other reasons (e.g., technical reasons, security reasons), they must be designed in such a way that they do not to impair the health or movement of the employees. If monitoring is required for legitimate reasons, it must at all times be proportionate (i.e. limited to what is absolutely necessary) and the employees must be informed in advance about the use of such monitoring systems. Permanent monitoring is generally not permitted.
Apart from the above general data protection regime, are there any specific data protection provisions in Switzerland relating to online advertising, tracking and direct marketing (e.g., unsolicited emails and phone calls)?	Yes. **Cookies** Cookies that do not contain or relate to personal data (i.e. that are not connected to identified or identifiable individuals from the perspective of the person using the cookies) can be used without restriction (e.g., typical session cookies). If cookies (or similar techniques such as clear GIFs or web-beacons) are related to identified or identifiable persons or otherwise connected to personal data, then they may be used only if they comply with the "Swiss cookie provision" (Art. 45c Swiss Telecommunications Act (TCA)), namely if: • They are required for the provision of telecommunications services or invoicing for such services; or • The user has been informed about their processing, their purpose and that he or she can decline the processing of related data (for e.g., a reference to the browser settings). This information can be provided in the website privacy notice, with the (optional) indication that without cookies, the user may for instance no longer use all the functionalities of the website. A violation of this Swiss cookie provision can be punishable with a fine of up to CHF 5'000 (Art. 53 TCA). However, there is so far no requirement under Swiss law to obtain the user's consent for using cookies. Consent may be required if the cookies exceptionally (i) go very far and

GDPR	DPA
	therefore no longer comply with the principle of proportionality or (ii) involve sensitive personal data and such data is shared with third parties. In the case of (ii), if consent is collected and relied upon in a particular case, it must be explicit (Art. 6(7)(a) and (b) DPA; see above). **Direct Marketing by E-Mail** Pursuant to the Swiss Federal Act against Unfair Competition (UCA), sending unsolicited mass direct marketing e-mails is only allowed if the recipient has provided his or her prior consent (i.e. **opt-in**). The recipient's consent does not necessarily have to be in writing. However, it is not permissible to obtain consent by sending out unsolicited mass e-mails asking for such consent. As an **exception**, mass advertisings may be sent without the consent of the recipient (i.e. **opt-out**) if cumulatively: • The sender received the contact information in the course of a sale of his or her products or services, and • The recipient was given the opportunity to refuse the use of his or her contact information upon collection, and • The mass advertising relates to similar products or services of the sender. The UCA requires businesses performing direct marketing to consult the official Swiss phone directories for numbers that have been marked with a standardized telemarketing opt-out declaration, unless the person has otherwise consented to receiving e-mail marketing or has a customer relationship with the sender. Furthermore, mass advertising e-mails must contain the correct name, address and e-mail contact of the sender and must allow the recipient to easily opt out of receiving future advertising emails at no cost. The UCA generally applies to business-to-consumer and business-to-business relationships. **Direct Marketing by Telephone** Direct marketing by telephone is legal in Switzerland as long as it is not carried out in an aggressive manner (e.g., by repeatedly calling the same person). However, the UCA prohibits direct marketing by telephone to persons whose names are marked with an asterisk (*) in the official telephone books and online telephone directory (i.e. persons who have opted-out), and Swiss law makes it a crime not to comply with this, unless the person has otherwise consented to receiving marketing by e-mail or has a customer relationship with the sender. Unlisted numbers must be treated in the same way as numbers with an asterisk, which is particularly important for calls to direct numbers at companies, because they are not listed. Moreover, for

GDPR	DPA
	marketing by telephone, the caller ID must be a Swiss registered number. It is also a crime to rely on information that has been obtained through illegal marketing calls. Hence, unsolicited marketing phone calls to unlisted numbers should only be made if a business contact has already been established (because it then counts as a call to an existing customer).