Swiss revDPA: Comparison with the GDPR

*Preliminary remark: The Swiss Federal Data Protection Act of June 19, 1992 ("**current DPA**") has been completely revised and on September 25, 2020, the Swiss Parliament passed the new law ("**revDPA**", together "**Swiss DPA**"). The revDPA is expected to come into force sometime in 2022.*

The following table is intended to provide an overview of the main differences between the revDPA and the GDPR, while also commenting on the differences between the current DPA and the revDPA, where relevant. Please note that only the provisions applicable to the private sector will be commented on, excluding those applicable to Swiss federal public authorities.

GDPR	revDPA
Does the Swiss DPA provide a materially different regime than the GDPR in the following areas:	
Definition of personal data (Art. 4(1) GDPR)	Comparable. The revDPA 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 revDPA (Art. 5(a) revDPA). Personal data relating to legal entities are no longer protected under the revDPA (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 re-identify the data subjects.
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 processing, 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 revDPA, 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

Questions: dataprivacy@vischer.com

GDPR	revDPA
	(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) revDPA). 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 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.
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) revDPA), i.e. if alternatively:

GDPR	revDPA
	• The processing principles (Art. 6 and 8 revDPA) 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 is required, such justification exists if (Art. 31(1) revDPA): • 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 revDPA is comparable to the "legitimate interest" test under the GDPR, except that under the revDPA, 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) revDPA).
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) revDPA). 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	revDPA
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) revDPA 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 current DPA), genetic data and biometric data that unequivocally identifies a natural person are also considered "sensitive personal data" under the revDPA. The revDPA no longer uses the Swiss concept of "personality profiles" (which under the current DPA is treated as sensitive personal data); this concept has been replaced by "profiling", the definition of which is comparable to the GDPR. The revDPA 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 revDPA does not provide that profiling requires consent. What the revDPA does provide 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) revDPA; 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) revDPA): • 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" 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 revDPA goes less far than the enhanced transparency information required under Art. 13/14 GDPR, with two exceptions: Unlike the

GDPR	revDPA
	GDPR, the privacy notice must also contain a list of countries or international organizations 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 revDPA, 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) revDPA) (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 countries or international organization 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) revDPA; 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 revDPA 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) revDPA).
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** The concept is the same (Art. 25-27 revDPA), 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 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

GDPR	revDPA
	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. **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. **Right to Rectification** The data subject has the right to rectification. There are 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 revDPA introduces a right to data portability that is inspired by, but differs from, the GDPR. Under the revDPA, 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 revDPA 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,

GDPR	revDPA
	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) revDPA). 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) revDPA). **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 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 revDPA, private controllers with their seat outside 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 revDPA). We expect that a Swiss representative will be necessary in far fewer cases than a representative pursuant to Art. 27 GDPR.
Processors (Art. 28 GDPR)	Comparable. The revDPA adopts the GDPR concept of processors (Art. 9 revDPA). However, the revDPA 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 revDPA, but it is recommended to add references to the Swiss DPA (in addition to the GDPR) and to ensure that data exports from

GDPR	revDPA
	Switzerland (in addition exports from the EU) are also covered.
Records of processing activities (Art. 30 GDPR)	Comparable. The revDPA (unlike the current 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.
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 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 revDPA). However, unlike the GDPR, the revDPA does not detail any particular method of data security (e.g., pseudonymization, encryption).
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. **Notification to the Federal Data Protection and Information Commissioner (FDPIC)** The controller is required to notify a data breach (defined in the same way as under the GDPR) to the FDPIC only if the breach is likely to result in a *high risk* for the personality of the data subject (Art. 24(1) revDPA). The notification must be made "as soon as possible" (with no fixed maximum time limit as under the GDPR) and must include information on the type of breach, its consequences and the measures taken or envisaged (Art. 24(2) revDPA). **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) revDPA). 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) revDPA). On the other hand, processors are required to inform controllers of data breaches (of any severity) as soon as possible (Art. 24(3) revDPA). There is no duty to keep a record of data breaches.

GDPR	revDPA
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 revDPA introduces an obligation upon controllers to perform and document a DPIA if their 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) revDPA). Limited exemptions exist for controllers if they for e.g. process personal data on the basis of a legal obligation provided by 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) revDPA). If the DPIA reveals 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).
Obligation to appoint a data protection officer (DPO) (Art. 37 GDPR)	Different. There is no formal obligation to appoint a data protection officer. However, the revDPA provides for the possibility for private controllers to appoint a voluntary data protection officer (so-called "data protection advisor"). If such data protection advisor fulfills the requirements provided under the revDPA (which are comparable prerequisites to the GDPR data protection officer), the controller is not obliged to consult the FDPIC in case of a DPIA that results in a high risk for the data subject (see above), but may consult its data protection advisor instead (Art. 23(4) revDPA).
Transfer of personal data to third countries (Art. 44-49 GDPR), in particular with regard to transfers to the EU	Comparable. Personal data may be transferred outside Switzerland if the destination country offers an adequate level of data protection. The FDPIC deems the data protection legislation of all EU/EEA countries to be adequate with regard to personal data of individuals. With regard to personal data of legal entities (which are still protected under the current DPA; see above), only a few EU/EEA countries, such as Austria and Liechtenstein, and Argentina (for legal entities located in Argentina), are deemed to provide an adequate level of data protection. The restrictions on transfers to third countries are comparable to those under the GDPR: It is only permitted to disclose personal data to recipients in non-whitelisted countries if there are either sufficient safeguards to compensate for such lack of protection (Art. 16(2) revDPA) or if one of the exemptions defined by the Swiss DPA applies (Art. 17 revDPA). Note that these provisions only apply to data exports *from Switzerland*. With the revDPA, there has been a conceptual change in the way exports are governed. Prior to the revision of the

GDPR	revDPA
	current DPA, each controller and processor had to determine for itself whether the country of destination of the data transfer offered an adequate level of data protection. Under the revDPA, it will be up to the Federal Council to maintain a binding list such countries (which is not yet known). So far, the FDPIC has maintained a list of countries with his assessment on the topic, but this list was not binding (see https://www.edoeb.admin.ch/edoeb/en/home/data-protection/arbeitsbereich/transborder-data-flows.html). It is expected that the Federal Council's list will contain most of the whitelisted countries as per the European Commission's adequacy findings. Switzerland is itself awaiting an adequacy decision from the European Commission. It should be noted that, under the Swiss DPA, remote access to data stored in Switzerland from outside of Switzerland is considered a disclosure of data abroad. Also, compared to the current DPA, the possible justifications for exports to non-whitelisted countries are expanded in the context of foreign proceedings. Thus, the revDPA also allows data exports to exercise or enforce claims in proceedings before foreign authorities and courts (and not only courts, as under the current DPA). This will facilitate data exports for foreign regulatory proceedings before administrative authorities rather than courts, which has triggered a number of litigation proceedings under the current DPA. **Standard Contractual Clauses (SCC)** Prior to the revision, the use of standard contractual clauses, including the Model Clauses, had to be notified to the FDPIC prior to their use. This is no longer necessary under the revDPA. A notification is necessary only for contractual clauses not already recognized, approved or issued by the FDPIC (i.e. individually drafted contractual clauses). If the Model Clauses are used, it is useful (but not mandatory) to adapt the references to the applicable law to also include the Swiss DPA and to make sure that data exports from Switzerland are also covered (not only exports from the EU/EEA). With regard to the CJEU's "Schrems II" Decision of July 16, 2020 it should be noted that the decision is not legally binding with effect in Switzerland, but most companies in Switzerland follow a similar approach as companies in the EEA, and the Swiss data protection authorities have stated that they consider the decision to apply *mutatis mutandis* also under Swiss law (which, however, is widely considered a political statement). In practice, it is certainly a reasonable approach to implement the same additional measures (if any) for data transferred from Switzerland as for data transferred from the EEA when relying on the Model Clauses. As to the European Commission, it is expected to publish its revised Model Clauses in the near future. Once this happens, we expect them to be adopted also under Swiss law. **Binding Corporate Rules (BCR)** Under the revDPA, Binding Corporate Rules (BCR) must be formally approved. This approval does not necessarily have to be done by the FDPIC; it is sufficient that the BCR have been approved by a competent data protection authority in

GDPR	revDPA
	an EU/EEA country or another country with adequate level of statutory data protection (provided that they are drafted in such a way that they also cover Switzerland, even though the foreign data protection authority will not cover this aspect). It is still unclear whether these approvals must nevertheless be notified to the FDPIC.
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 revDPA), insofar as they can be held liable for the violation of the personality of the data subject. 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 revDPA, criminal fines are directed at the responsible individuals (e.g., management, employees responsible for data protection tasks), *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, if, in a particular case, 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 revDPA). The catalog of fines has been significantly expanded in comparison to the current DPA. Specifically, under the revDPA, 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 revDPA'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 (so far, they are not yet known) or (vii) intentionally fail to comply with an order of the FDPIC. Violations of the fundamental processing principles of the revDPA, on the other hand, continue to be exempt from punishment – an important difference to the GDPR. The fines are not issued by the FDPIC, but by the Swiss cantonal criminal authorities (which are not specialized in data protection).

GDPR	revDPA
	The revDPA also introduces 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). Further, 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 a fine. **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 conduct. **Expanded Enforcement Powers of the FDPIC** The enforcement of the Swiss DPA will also change under the revDPA. Under the current DPA, the FDPIC may only issue "recommendation" to controllers and processors who, in his opinion, do not comply with the current DPA and can sue them if they do not comply with his recommendation. Under the revDPA, 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 revDPA) 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 revDPA. The FDPIC may issue a "warning" if the person targeted takes the necessary measures to restore compliance with the revDPA 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 Swiss cantonal enforcement authorities (which are not specialized in data protection).
Apart from the above general data protection regime, are there any specific data protection provisions in the field of employment law in Switzerland?	Yes. 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

GDPR	revDPA
	provision to be a general obligation, the violation of which cannot be justified. Additionally, Art. 26 of the Ordinance on Employment Act 3 prohibits the use of systems that monitor the behavior of employees at the workplace. If a surveillance or control system is necessary for others reasons (e.g., technical or security reasons), it must be designed in such a way that it does not impair the movement or health of the employees. If a surveillance or control system is necessary for legitimate reasons, it must be proportionate to its purpose (i.e. limited to what is absolutely necessary) and the employees must be informed in advance of its use. Permanent surveillance of employees at the workplace 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 related to identified or identifiable individuals from the perspective of the person using the cookies) can be used without restriction (e.g., session cookies). If cookies (or similar techniques such as web-beacons or clear GIFs) are related to identified or identifiable individuals or otherwise connected to personal data, they can 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 to the use of cookies. Explicit consent is only required if the cookies exceptionally involve 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) (Art. 6(7)(a) and (b) revDPA; 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 unsolicited mass marketing e-mails requesting such consent. As an **exception**, mass marketing emails may be sent without the consent of the recipient (i.e. **opt-out**) if cumulatively:

GDPR	revDPA
	• 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 companies performing direct marketing to search in the Swiss official telephone directories for numbers that have been marked with a standardized telemarketing opt-out declaration, unless the person has otherwise consented to receiving marketing emails or has a customer relationship with the sender. Furthermore, mass advertising emails must contain the correct identity 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 numbers are marked with an asterisk (*) in the Swiss official telephone directories. The asterisk indicates that the person does not wish to receive marketing calls, and Swiss law makes it a crime not to comply with it, unless the person is a customer or has otherwise consented to such marketing calls. 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 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).