TerraLex

Global Crisis Management Regulatory Guide

Switzerland

Authors

Contributed by:	Roesle Frick & Partners Lalive Adam El-Hakim Heloisa Zimmermann Cornelia Mattig Martin K. Weber Alexandre Schwab

Date posted:	October 09 2022
Last update:	October 08 2025

Data breach

On discovering a data breach, which regulators or other government agencies should be notified?	Under the amended Swiss Federal Data Protection Act (DPA) in force since 1 September 2023 (see in particular Article 24 DPA), data controllers are responsible for reporting any data breaches that are likely to lead to a high risk to the data sub-jects' personality or fundamental rights as quickly as possible to the Federal Data Protection and Information Commissioner (FDPIC). The data processor must notify the data control-ler as soon as possible of any data security breach. Further, data control-lers shall also inform the affected data subjects if this is required for their protection or if the FDPIC so requests. With the data controller's consent, the FDPIC may forward the notifica-tion to the National Cyber Security Centre for analysis. In addition, several sector-specific notification obligations to sector-specific supervisory entities apply (e.g., in the medical device sector to Swissmedic, in the financial market sector to the Swiss Financial Market Supervisory Authority FINMA). Moreover, on 1 April 2025 the notifica-tion obligation regarding cyberattacks on critical infrastructure under the Information Security Act (ISA) entered into force requiring a notification within 24 hours. A voluntary notification for entities that are not consid-ered a critical infrastructure under the ISA remains.
What legislation, relating to both criminal offences and civil wrongs, covers such a breach?	Data protection issues are generally regulated under the Swiss Federal Data Protection Act (DPA) and Federal Data Protection Ordinance (DPO); however, the DPA does not set forth criminal or civil penalties specifically for failure to notify the Federal Data Protection and Information Commissioner (FDPIC). Other breaches of the DPA are however subject to fines. For example, a refusal to comply with a ruling issued by the FDPIC is subject to a fine not exceeding CHF 250,000 (Art. 63 DPA). For critical

	infrastructure, the failure to notify a breach within 24 hours may ultimately result in a fine of up to CHF 100,000. Violations of related obligations under the Swiss Code of Obligations (SCO), including the duty of care and loyalty of an employee (Art. 321a SCO), duty of care and faithful performance of an agent (Art. 398 SCO) or business secrecy, may result in civil liability. Furthermore, criminal sanctions may be imposed for violations of professional confidentiality obligations (Art. 62 DPA and Art. 69 Federal Act on Financial Institutions, FinIA), breach of business secrets (Art. 162 Swiss Criminal Code, SCC), breach of banking secrecy (Art. 47 of the Swiss Banking Act) and breach of professional secrecy (Art. 321 SCC). In addition, further sector-specific obligations may apply (e.g., in the financial or medical sector).

"Dawn" raids

What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?	The following authorities notably have the power to conduct dawn raids on private sector companies: • All cantonal and federal criminal prosecution authorities (i.e., the cantonal and federal police, the cantonal prosecution offices, the Of-fice of the Attorney General (OAG) and the cantonal and federal courts): Swiss Criminal Procedure Code and Federal Act on the Organization of Criminal Authorities. • The Federal Tax Administration: Federal Law on Direct Federal Tax and Federal Law on Administrative Criminal Proceedings. • The Swiss Competition Commission: Federal Cartel Act. • The Federal Office for Customs and Border Security: e.g., Federal Act on Customs, Federal Act on Administrative Criminal Proceedings. • The Swiss Financial Market Supervisory Authority FINMA: Federal Act on the Financial Market Supervisory Authority. • The Federal Data Protection and Information Commissioner (FDPIC) may order access to premises and facilities: Federal Act on Data Protection.
On what bases, including privilege and/or confidentiality, may organisations refuse to permit the seizure of documents?	The holder of the documents can within three days of the document being seized request that they are placed under seal. In return, within twenty days, the investigating authority can request the coercive measures court to lift the seal (Art. 248 and 248a Swiss Criminal Proce-dure Code, SCPC). The following documents cannot be seized (Art. 248 (1) and 264 SCPC): • documents used in communications between the defendant and his or her defence lawyer; • personal records and correspondence belonging to the defendant if the interest in protecting his or her privacy outweighs the interest in prosecution; • items and documents used in communications between the defend-ant and persons who may refuse to testify in accordance with Articles 170 –173 SCPC (i.e., official secrecy, professional confidentiality, protection of journalists' sources and other duties of confidentiality) and who are not accused of an offence relating to the same case; and • items and documents used in communications between another per-son and his or her lawyer provided the lawyer is entitled to represent clients before Swiss courts and is not accused of an offence relating to the same case.

Whistleblowing

What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?	For the time being, there is no whistleblowing regulation in Switzerland, the proposal for a legislation having been rejected by the parliament. Employees who report corporate wrongdoing are generally not specifically protected under Swiss law. In fact, disclosure of alleged wrongdoing directly to the authorities or to the public may result in both criminal liabilities, for instance in violation of business secrecy (Art. 162 Swiss Criminal Code) or banking secrecy (Art. 47 of the Swiss Banking Act), as well as civil liability for violating the duty of loyalty to the employer (Art. 321 Swiss Code of Obligations). This said, establishing whistleblowing systems is considered best prac-tice for Swiss undertakings. As a general rule, employees must first report an offence internally within the company or to an external whistleblower office appointed by the company. Indeed, reporting the case to the authorities because management did not take appropriate remedial measures is acceptable only as a means of last resort.
What legislative protection does that employee enjoy?	As stated above, Swiss law does not grant specific protection to employees who report wrongdoings directly to authorities. At present, those unlawfully dismissed in retaliation for whistleblowing, or who refuse to commit a criminal act, would only be entitled to limited remedies under Swiss employment law. For bank employees and representatives, a breach of professional confidentiality (“Swiss banking secrecy”), even under the auspices of whis-tleblowing, can result in a prison sentence or a fine. Also, people who disseminate such secrets may be liable to prosecution (e.g. journalists).

Anti-bribery and corruption

What are the main anti-corruption laws and regulations in your jurisdiction?	The main anti-corruption laws and regulations in Switzerland are: • The Swiss Criminal Code (SCC) covers bribery of public officials and bribery in the private sector (Art. 322ter to 322decies SCC). Furthermore, the granting and acceptance of improper advantages are also subject to criminal sanctions. This pertains to illicit benefits that are not directed at a specific official act but are granted or accepted regarding future official conduct (Art. 322sexies and 322septies SCC). • Private commercial bribery within the context of the distortion of competition is covered by Art. 4a of the Federal Act on Unfair Competition. • The Federal Act on Foreign Illicit Assets covers the freezing, confiscation and restitution of assets obtained unlawfully and deposited in Switzerland by foreign potentates who have been or are about to be ousted. • Additionally, administrative sector specific laws include rules on hospitality, travel and entertainment expenses, as well as provisions on public procurement aimed at preventing bribery and corruption. Internationally, Switzerland is party notably to: • The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. • The United Nations Convention Against Corruption. • The Council of Europe Criminal Law Convention on Corruption and Additional Protocol.

Does the legislation have extra-territorial effect?	Yes, to a limited extent. The Swiss Criminal Code (SCC) may apply to bribery offenses committed abroad under specific conditions, which include international obligations to prosecute and the presence of the offender in Switzerland without extradition. Switzerland also exercises extraterritorial jurisdiction when a foreign bribery offense has effects on Swiss territory, such as a deficient corporate organization existing there. A Swiss parent company may be sanctioned with a fine of up to CHF 5m if an employee of its foreign subsidiary committed an act of bribery abroad, provided that the Swiss parent company did not undertake all requisite and reasonable organisational precautions required to prevent such a crime (Art. 102(2) SCC). For example, Alstom Network Schweiz AG was fined with CHF 2.5m and had to pay a compensatory claim of CHF 36.4m for not having taken all necessary and reasonable organizational precautions to prevent bribery of foreign public officials in Latvia, Tunisia and Malaysia.
What are the main enforcement bodies?	The Office of the Attorney General of Switzerland is competent to investigate bribery and corruption if it involves federal authorities or if the suspected crime has been substantially committed abroad or committed in several cantons if there is no unambiguous focus on one canton. Otherwise, the case falls within the competence of the cantonal public prosecutors.

Internal investigations

Is there any duty to report the issue, for example to a regulator?	There is no general obligation for organisations to self-report suspected misconduct and no statutory framework for selfreporting, safe for reporting obligations for financial intermediaries in case of suspicious activities as set forth in the Federal Act on Combating Money Laundering and Terrorist Financing. However, there are various legal obligations for self-reporting legal risks in specific cases (which have not all yet been tested in court). For instance: • Members of the board of directors and the executive committee of an undertaking should conduct an internal investigation in cases of suspected or actual (material) misconduct (e.g., bribery of foreign officials), as part of the duty of care and loyalty imposed upon them (e.g., Art. 717 Swiss Code of Obligations). • Based on the Financial Market Supervision Act, supervised persons and entities (e.g., financial intermediaries and traders) as well as their auditors must disclose to the Swiss Financial Market Supervisory Authority FINMA any incident that is of material importance for supervisory purposes, such as the suspicion of money laundering involving significant assets or any incident that may have an impact on the institution's or the financial market's reputation. • The Federal Cartel Act specifically outlines selfreporting and the leniency an applicant may receive, including full immunity from fines. Applications are typically filed with the Swiss Competition Commission Secretariat within the first hours of an investigation.
What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?	Legal privilege exists under Swiss law, in principle broadly protecting information exchanged with lawyers acting in their professional capacity as lawyers (but not if acting in a mere business capacity). Legal privilege also covers any submandated auxiliaries of the lawyer, e.g. external accountants, forensic specialists etc. Based on the wording of the statutory law, this protection applies only to Swiss attorneys and EU lawyers authorised to practise in Switzerland. All work products (memoranda, reports, correspondence, or interview notes) related to the "typical" activity of a registered lawyer (by contrast to

	non-registered lawyers or in-house counsel) are in principle protected by legal privilege and do not have to be disclosed, and cannot be seized, if they are part of the communication between a person or business and outside counsel, irrespective of their location. According to a recent decision of the Federal Supreme Court, the investigation of facts in connection with advice and representation regarding existing and impending legal disputes, or the selection of pre-existing items of evidence with a view to a legal issue are considered typical legal activities. Legal privilege may not be invoked, however, to allow a specific activity, typically not performed by lawyers, to be carried out by an attorney merely so that the information and any resulting advice are protected by confidentiality and do not have to be disclosed to third parties, such as regulators or law enforcement authorities. In recent decisions, the Federal Supreme Court has clarified that legal privilege does not extend to tasks outsourced to external counsel if the underlying legal obligation belongs to the company itself, namely compliance obligations relating to anti-money laundering laws. As a result, internal investigation reports analysing breaches of the antimoney laundering provisions were held not to be legally privileged. Therefore, it is advisable to identify and document the link to (pending or imminent) legal disputes. If an organisation decides to self-report misconduct and discloses in-formation in the absence of a legal obligation, it must comply with: • The Federal Act on Data Protection, which requires personal data (i.e., all data relating to an individual) to be processed according to the principles outlined in the relevant act. To comply with this obli-gation personal data resulting from internal investigations may only be disclosed if in compliance with the applicable data protection principles of lawfulness, good faith, proportionality, purpose limitation, data minimisation and accuracy. • Its duties under employment law, in particular its duty of care towards its employees, according which it shall ensure the latter's privacy (Art. 328 Swiss Code of Obligations).
Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?	The answer depends on the applicable procedure. In civil proceedings, a party may refuse to cooperate and refuse to disclose documents related to its in-house legal department if (i) it is registered as a legal entity in the Swiss commercial register or a comparable foreign register; (ii) the legal department is headed by a person who holds a cantonal law li-cense or meets the professional requirements for practicing law in their home country; and (iii) the activity in question would be considered profession-specific for a lawyer (Art. 167a Swiss Civil Procedure Code) (cf. to the "profession-specific activity", see the question above). In contrast, in criminal and administrative proceedings (such as pro-ceedings before the Swiss Financial Market Supervisory Authority FINMA or the Swiss Competition Commission), an in-house lawyer will generally not be able to invoke their right to refuse cooperation and the corresponding legal advice will generally not be privileged or confidential.