

Art. 8 FADP: Data security

Function and place in the Act

Art. 8 FADP requires the controller and the processor to guarantee a level of data security appropriate to the risk by taking suitable technical and organisational measures (para. 1). The measures must make it possible to avoid breaches of data security (para. 2). The Federal Council issues minimum requirements (para. 3) **Art. 8 FADP**.

According to the Federal Council's Dispatch, para. 1 expresses the risk-based approach: «Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen.» (The greater the risk of a data security breach, the higher the requirements for the measures to be taken.) **BBI 2017 6941**. The same source says that para. 2 sets the objective of the measures. The provision was already part of the Federal Council's draft (Art. 7 D-FADP), which took over former Art. 7 FADP «mit einigen Änderungen» (with some changes) **BBI 2017 6941**. The Dispatch names these changes: the risk-based standard is stated expressly, the processor is covered alongside the controller, and the Federal Council must now define minimum requirements. It also presents the duty as a requirement of the modernised Council of Europe Convention 108 (Art. 7) and of Directive (EU) 2016/680 (Art. 29) **BBI 2017 6941**. Art. 8 FADP has not been amended since it entered into force on 1 September 2023. Because the provision builds on former Art. 7 FADP, case law under the old law remains useful for interpretation, as long as the changes just listed are kept in mind.

The Dispatch distinguishes data security from data protection: «Beim Datenschutz geht es um den Persönlichkeitsschutz des Einzelnen.» (Data protection concerns the protection of the individual's personality.) Data security, by contrast, «hingegen generell auf die bei einem Verantwortlichen oder Auftragsbearbeiter vorhandenen Daten ab und umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung» (targets generally the data held by a controller or processor and covers the general technical and organisational framework of data processing) **BBI 2017 6941**. This also separates Art. 8 from Art. 7 FADP (data protection by design). Art. 7 requires processing to be set up so that the data protection rules, in particular the principles in Art. 6, are complied with, and it is addressed only to the controller **Art. 7 FADP**. Art. 8 FADP, by contrast, protects the security objectives of the data themselves and also binds the processor.

Scope: cantonal bodies are outside the FADP

The FADP applies only to private persons and federal bodies. Exempt, among others, are processing exclusively for personal use and processing by the Federal Assembly and its committees in the course of their deliberations (Art. 2(1) and (2) FADP) **Art. 2 FADP**. According to the Federal Supreme Court, cantonal and communal bodies are not subject to the FADP, «même s'ils sont chargés de l'exécution de tâches de la Confédération» (even if they are entrusted with implementing federal tasks). The cantonal data protection act therefore applied to the Vaud disability insurance office **1C_125/2015**. Such bodies are governed by the security provisions of cantonal law. Geneva law, for example, requires in Art. 37 LIPAD suitable organisational and technical measures against any unlawful processing **ATA/663/2024**. Private entities can also count as cantonal

bodies, for example where they act under a service mandate or are mainly publicly funded. Supervision then lies with the cantonal authorities, and the classification must be examined case by case **150007355**. This opinion of the Federal Office of Justice is an administrative view, not a court decision.

Addressees and processing by processors

Within this scope, the duty applies to the controller and to the processor, whether a private person or a federal body (Art. 5(j) and (k) FADP) **Art. 5 FADP**. The processor therefore has its own security duty, not one merely derived from the controller. In addition, under Art. 9(2) FADP the controller must «insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten» (in particular satisfy itself that the processor is able to guarantee data security). Sub-processing requires the controller's prior authorisation (Art. 9(3) FADP) **Art. 9 FADP**.

This selection duty is backed by criminal law. Under Art. 61(b) FADP, anyone who wilfully hands over processing to a processor without the conditions of Art. 9(1) and (2) FADP being met is liable to a fine **Art. 61 FADP**. The Zurich High Court treats this offence as complete upon handover and not as a continuing offence. The recipient's continued possession of the data therefore does not extend the limitation period **UE240022**. The Schwyz Cantonal Court set aside a decision not to open proceedings under Art. 61(b) FADP because the public prosecutor had not examined a possible statutory duty of confidentiality (Art. 9(1)(b) FADP). Such a decision may only be issued where there is «offensichtlicher Straflosigkeit» (manifest absence of criminal liability) **BEK 2024 84**.

In its supervisory practice (the Xplain and Concevis cases), the FDPIC requires contracts with processors to set out the data life cycle precisely and to regulate controls and audits clearly **EDÖB 32. Tätigkeitsbericht 2024/2025**. This practice is not binding, but it shows how the supervisory authority understands the controller's duty under Art. 9(2) FADP to satisfy itself of the processor's ability.

Data security breaches and the duty to take measures

The legal definition in Art. 5(h) FADP covers a breach of security that leads to personal data being accidentally or unlawfully lost, deleted, destroyed or altered, or disclosed or made accessible to unauthorised persons **Art. 5 FADP**. According to the Dispatch, the data security provision was made more precise «weil ihr Anwendungsbereich sehr unklar schien» (because its scope seemed very unclear) **BBI 2017 6941**.

The Federal Administrative Court describes a breach as a «planwidrigen Vorfall mit Sicherheitsrelevanz» (an unplanned security-relevant incident). It holds: «Ob sich eine Verletzung der Datensicherheit ereignet hat, ist unabhängig davon zu beurteilen, ob diese schuldhaft oder widerrechtlich herbeigeführt wurde.» (Whether a data security breach has occurred must be assessed independently of whether it was caused culpably or unlawfully.) **a-3790-2024**. In that case a search-engine crawler was able to index customer-specific URLs, which the court classified as a «Konfiguration- oder Sicherheitsproblem» (configuration or security problem) of the

controller. Technical blocks put in place afterwards could not «eine bereits erfolgte unbefugte Offenlegung nicht rückwirkend zu beseitigen» (retroactively undo an unauthorised disclosure that had already occurred) **a-3790-2024**.

An important distinction follows. The concept of a breach does not depend on fault and is tied to the outcome. Art. 8 FADP, by contrast, imposes a duty to take measures: the measures must «make it possible» to avoid breaches (para. 2) **Art. 8 FADP**. An incident therefore does not in itself prove that Art. 8 FADP was violated. The Federal Supreme Court held under the former law: «Geschuldet ist kein absoluter Schutz» (absolute protection is not owed) **BGE 144 I 126**. The Explanatory Report on the Data Protection Ordinance (FADPO) says the same: «Eine absolute Sicherheit kann und soll nicht verlangt werden.» (Absolute security cannot and should not be required.)

EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) - Erläuternder Bericht

. Decision A-3790/2024 does not, however, expressly address how an incident relates to a breach of duty under Art. 8 FADP; it concerns the duty to inform under Art. 24 FADP (see below).

The risk-based standard: protection needs, risk, state of the art and costs

Art. 1 FADPO gives concrete form to para. 1 in two steps. First, the need for protection of the data must be determined, based on the type of data and on the purpose, nature, extent and circumstances of the processing (para. 2). Second, the risk to the personality or fundamental rights of the data subject must be assessed. The relevant factors are the causes of the risk, the main threats, the measures taken or planned, and the likelihood and severity of a breach despite those measures (para. 3). The state of the art and the implementation costs must also be taken into account when choosing measures (para. 4). The duty is ongoing: the need for protection, the risk and the measures must be reviewed «über die gesamte Bearbeitungsdauer hinweg» (throughout the entire duration of the processing), and the measures must be adjusted where necessary (para. 5) **Art. 1 DPO**.

The state of the art and implementation costs limit the scope of the duty only within what is appropriate. According to the Explanatory Report, it suffices to take measures «die bereits zur Verfügung stehen und sich entsprechend bewährt haben» (that are already available and have proven themselves accordingly). Costs include staff and time resources. The controller cannot, however, «nicht mit der Begründung von der Pflicht einer angemessenen Datensicherheit befreien, dass damit übermässige Kosten verbunden sind» (release itself from the duty of appropriate data security on the ground that it involves excessive costs)

EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) - Erläuternder Bericht

. Costs thus determine which means is chosen, not whether measures are taken at all. The report is an administrative explanation; it does not bind the courts, but it is consistent with the wording of Art. 8(1) FADP.

The law does not prescribe binding technical standards. The Third Criminal Chamber of the Zurich High Court held: «Das Datenschutzgesetz und die Datenschutzverordnung enthalten keine verbindlichen Vorgaben für Daten- bzw. Informationssicherheitsstandards.» (The Data Protection Act and the Data Protection Ordinance contain no binding requirements for data or information security standards.) **UE240472**. For an e-mail containing financial and address data, enforced TLS transport encryption was therefore sufficient. The court rejected the demand for end-to-end encryption, partly because such data are not sensitive personal data **UE240472**. The decision was issued in criminal proceedings (a decision not to open proceedings), so it should be transferred to the civil or supervisory standard with caution. The assessment is stricter where the need for protection is high: for telecommunications metadata, the Federal Supreme Court relied on the facts that transmission takes place only by previously

authenticated staff and in encrypted form, and that system access is limited to registered and verified users **BGE 144 I 126**.

Cantonal practice applies the same proportionality reasoning. For cantonal case-management software, the Bern Administrative Court held that the required measures are assessed according to the principle of proportionality and the specific risks. It did not, however, rule on the alleged lack of two-factor authentication, for want of a current interest **100 2017 72**. For video surveillance, the Vaud Cantonal Court required manual logging of access to the recordings. But it held: «il serait toutefois disproportionné d'exiger le renouvellement des installations pour ce seul motif» (it would, however, be disproportionate to require the installations to be replaced on that ground alone) **ge-2012-0139**. Both decisions were issued under cantonal law and are relevant to Art. 8 FADP only by analogy.

Security objectives and the catalogue of measures

Art. 2 FADPO sets out four security objectives: confidentiality, availability, integrity and traceability **Art. 2 DPO**. Art. 3 FADPO assigns measures to them. Confidentiality covers access control, physical access control and user control. Availability and integrity cover data carrier, storage and transport control, recovery, reliability and system security, which includes closing known critical vulnerabilities. Traceability covers input and disclosure control as well as the rapid detection and remedying of breaches **Art. 3 DPO**. The measures must be taken «ihrem Schutzbedarf entsprechend» (according to their need for protection) **Art. 2 DPO**. The catalogue is therefore a checklist for assessment, not a list that must be fully implemented in every case.

Access control and need-to-know. The Federal Administrative Court applied the principle that authorised persons may only access the data they need for their tasks (now Art. 3(1)(a) FADPO) already under the former law. A pension fund sent pension certificates in unsealed envelopes to employers for forwarding. This violated the principle of data security under former Art. 7 FADP, because employers do not need to know an employee's individual pension situation. The court required direct mailing or at least sealed envelopes, addressed by name and marked confidential **a-4467-2011**. The decision shows that simple organisational measures may also be owed.

Hospitals and patient records. The Geneva Administrative Chamber found lawful an access model that limits access by profile, area of activity and treatment time window. For emergencies, an exceptional access that must be justified («vitre brisée», break-glass access) is available, and all access is logged and checked afterwards. By contrast, access by a doctor who was not treating the patient and falsely claimed to be responsible was unlawful **ATA/663/2024**. The case separates the system design, which was sufficient, from the abusive individual access, which amounted to an infringement of personality. The Geneva Criminal Appeals Chamber saw no manifest breach of the minimum requirements in a clinic's billing staff accessing the medical record. Those staff needed access for invoicing and are also bound by professional secrecy. Whether the organisation of access was proportionate was, in the chamber's view, essentially a civil-law question **ACPR/239/2025**.

Video surveillance and circles of authorised persons. The Fribourg Cantonal Court objected to a communal video surveillance regulation because the circle of persons with access was «trop étendu et trop imprécis» (too wide and too imprecise), and because password protection alone is not sufficient to secure the data **601 2014 46**.

Missing formal security testing. The Federal Administrative Court allowed a smart meter to remain in use under transitional law even though the data security test required by sector-specific law (Art. 8b of the Electricity Supply Ordinance) was missing. The grid operator nevertheless remains bound by the substantive security requirements, and there were no concrete indications of insecure processing **a-2372-2021**. The decision thus requires concrete indications before a

complaint of a data security breach can succeed.

Logging and processing regulations

Art. 4 FADPO, in the version in force since 1 December 2025, governs logging. Private controllers and their private processors must keep logs where sensitive personal data are processed automatically on a large scale or high-risk profiling is carried out, and preventive measures cannot ensure data protection. At a minimum, storage, alteration, disclosure, deletion and destruction, as well as access, must be logged. Federal bodies must always log in certain cases. For other automated processing, they decide whether and to what extent to log on the basis of a prior written risk assessment, which must be communicated to the FDPIC on request (paras. 2 and 2bis). Logs must be kept for at least one year, separately from the production system, and may be used only for control and security purposes (para. 5) **Art. 4 DPO**. For processing by federal bodies that was planned or begun before the amendment, the assessment must be carried out by 31 December 2026. Any logging that is needed must be implemented by 31 December 2029; this does not apply to cases in which logging is mandatory in any event **Art. 46 DPO**.

The purpose limitation of logs matters in practice. Under cantonal law, the Geneva Administrative Chamber held that badge access logs collected for the security of premises may not be used to monitor working time. It ordered the relevant files to be destroyed **ATA/1316/2024**. This matches the purpose limitation that Art. 4(5) FADPO expressly lays down under federal law **Art. 4 DPO**.

Private persons must draw up processing regulations for automated processing if they process sensitive personal data on a large scale or carry out high-risk profiling. The regulations must describe in particular the internal organisation, the processing and control procedures, and the security measures, and must be updated regularly **Art. 5 DPO**. For federal bodies the list is broader. It includes, among other things, any processing of sensitive data, any profiling, making data accessible to third parties and linking data sets **Art. 6 DPO**. Such regulations may contain security-relevant information, for example on user and access rights and on data security. For the regulations of the Federal Intelligence Service, access under the Freedom of Information Act was therefore excluded by the special statute **a-4286-2022**.

Notification and information after a breach

Art. 8 FADP is preventive. Art. 24 FADP governs what happens after an incident. The controller must notify the FDPIC as soon as possible of a breach that is likely to result in a high risk for the data subject. The processor must report every breach to the controller. Data subjects must be informed where this is necessary for their protection or the FDPIC so requests (paras. 1, 3 and 4). A notification may be used in criminal proceedings against the person required to notify only with that person's consent (para. 6). Since 1 April 2025, the FDPIC may, with the controller's consent, forward the notification to the Federal Office for Cybersecurity (para. 5bis) **Art. 24 FADP**. Art. 15 FADPO sets out the minimum content of the notification. It also requires every breach to be documented, with the facts, effects and measures taken, and the documentation to be kept for at least two years **Art. 15 DPO**. In the crawler case, the Federal Administrative Court upheld the FDPIC's order to inform the data subjects. Where individual information is impossible or disproportionate, a public announcement may take its place **a-3790-2024**.

Enforcement by the FDPIC

The FDPIC opens an investigation where there are sufficient indications of a violation. It may refrain from doing so if the violation is of minor importance (Art. 49(1) and (2) FADP) **Art. 49 FADP**. If the party concerned fails to cooperate, the FDPIC may order, among other things, access to premises and facilities and expert

examinations (Art. 50 FADP) **Art. 50 FADP**. In particular, it may order that the measures under Arts. 7 and 8 FADP be taken (Art. 51(3)(b) FADP). If the party concerned restores compliance itself during the investigation, the FDPIC may limit itself to issuing a warning (para. 5) **Art. 51 FADP**. Wilful failure by a private person to comply with an order issued with reference to the penalty is a criminal offence (Art. 63 FADP) **Art. 63 FADP**. Under the former law, the FDPIC could not, in action proceedings, demand technical and organisational measures going beyond its recommendation **a-5225-2015**. That limit has largely been superseded by the power to issue orders under Art. 51 FADP.

A person who reports a violation has no right to an investigation. The Federal Administrative Court held: «la personne concernée ne bénéficie pas d'un droit subjectif à ce qu'une procédure d'enquête soit ouverte» (the data subject has no subjective right to the opening of an investigation). The notice under Art. 49(4) FADP is not an appealable decision **a-8391-2025**. Data subjects must therefore enforce their rights through the civil courts (see below).

Criminal consequences: Art. 61(c) FADP

Private persons who wilfully fail to comply with the minimum data security requirements issued by the Federal Council under Art. 8(3) FADP are liable, on complaint, to a fine of up to CHF 250,000

Art. 61 FADP. This results in three limits. Federal bodies are not covered. Negligence is not punishable, as the Explanatory Report on the FADPO confirms

EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -

. And the offence is prosecuted only on complaint. Prosecution and adjudication are the responsibility of the cantons; the FDPIC may file a criminal complaint and exercise the rights of a private claimant

Art. 65 FADP. Within businesses, Arts. 6 and 7 of the Federal Act on Administrative Criminal Law apply. For fines of up to CHF 50,000, the business may be convicted instead of the responsible persons where identifying them would be disproportionate **Art. 64 FADP**. Prosecution is time-barred after five years **Art. 66 FADP**.

The offence was contested in Parliament. The National Council initially deleted the criminal provision (Art. 55(c) D-FADP)

AB 2019 N 1805. In the procedure to resolve differences, a minority again moved for deletion on the ground of vagueness. The Federal Council replied: «Der Bundesrat ist also in der Festlegung der Mindestanforderungen nicht einfach frei.» (The Federal Council is therefore not simply free in setting the minimum requirements.) The National Council followed the majority by 137 votes to 51, and the criminal provision was retained **AB 2020 N 140**.

Cantonal practice resolves the tension between a blanket criminal provision and an open, risk-based standard in the ordinance through narrow interpretation. The Geneva Criminal Appeals Chamber holds: «seuls des cas manifestes - par exemple l'absence totale de mesures de protection - pourraient constituer une infraction pénale» (only manifest cases - for example the complete absence of protective measures - could constitute a criminal offence) **ACPR/239/2025**. The Zurich High Court upheld a decision not to open proceedings because no wilful violation was apparent where an e-mail had been sent with TLS encryption **UE240472**. The Vaud Criminal Appeals Chamber considered that a hospital sending letters to a wrong address amounted at most to non-punishable negligence; it left open the data security question **CREP pe22-008518-471/2023**. These cantonal decisions follow a consistent line, but they are not binding beyond their respective cantons.

Civil consequences and liability

Where private persons process personal data, there is an infringement of personality in particular where personal data are processed contrary to the principles in Arts. 6 and 8 FADP (Art. 30(2)(a) FADP) **Art. 30 FADP**. Data security is thus expressly a processing principle whose disregard infringes personality. The infringement is unlawful unless justified by consent, an overriding

interest or law (Art. 31(1) FADP) **Art. 31 FADP**. Actions are governed by Arts. 28, 28a and 28g to 28l of the Civil Code. Claimants may seek in particular a ban on processing, a prohibition of disclosure, and erasure or destruction, as well as notification or publication of the judgment (Art. 32(2) and (4) FADP) **Art. 32 FADP**. Through the reference in Art. 32(2) FADP, damages and compensation for non-material harm are governed by the Civil Code.

In damages claims, causation is often the decisive obstacle. The Glarus Administrative Court found that a partly impermissible disclosure of data by the road traffic office was unlawful, but rejected the state liability claim: «Damit mangelt es diesbezüglich an der erforderlichen Kausalität.» (The necessary causation is therefore lacking in this respect.) **VG.2016.00090**. The case concerned an impermissible disclosure under cantonal state liability law, not a failure of security measures under Art. 32 FADP. It shows, however, that a finding of a data protection violation does not by itself give rise to a claim for compensation.

Practical guidance

- Assess the need for protection and the risk under Art. 1 FADPO in writing and give reasons for the measures chosen, especially where the state of the art or costs played a role. This documentation shows, in supervisory proceedings and in response to a criminal allegation, that the measures were chosen on a risk basis.
- Align access rights with need, require justification for exceptional access and log it, and use logs only for their intended purpose.
- Bind processors by contract to security measures, the data life cycle, audits and authorisation of sub-processing, because Art. 61(b) FADP penalises wilful handover without the controller having satisfied itself of the processor's ability.
- For federal bodies, monitor the transitional deadlines in Art. 46 FADPO for assessing and implementing logging (see Logging above).
- After an incident, document the breach under Art. 15(4) FADPO and check whether the high-risk notification threshold is met; blocks put in place afterwards do not replace this assessment (see Data security breaches above).