Art. 19 FADP: Duty to Provide Information When Collecting Personal Data

Function and Place in the FADP

Art. 19 FADP requires the controller to give information actively. It must inform on its own initiative, without waiting for the data subject to ask **RBOG 2025 Nr. 10**. The duty is triggered by the collection of personal data. It applies whether the data is collected from the data subject or from a third party **a-3891-2025**.

According to the Federal Administrative Court, Art. 19(1) FADP supplements the general principle of transparency **a-2941-2024**. Under that principle, personal data may be collected only for a specific purpose that the data subject can recognise (Art. 6(3) FADP) **Art. 6 FADP**. Ruling on Art. 18a of the former FADP,the Federal Supreme Court held that the information is meant to let data subjects assess whether the collection is lawful. Its function is therefore preventive protection **BGE 148 II 349**.

Para. 2 uses the same general clause as the right of access in Art. 25(2) FADP.Access is the later counterpart: it is granted only on request, and for disclosure abroad it refers expressly to the information under Art. 19(4) FADP **Art. 25 FADP**.

Consent also depends on information. It is valid only if given "nach angemessener Information" ("after appropriate information"; Art. 6(6) FADP) **Art. 6 FADP**. Defective information under Art. 19 FADP can therefore invalidate a consent on which the controller seeks to rely.

Automated individual decisions are additionally subject to their own duty to inform under Art. 21 FADP **Art. 21 FADP**.

Legislative History: Extension of the Duty to Private Controllers

The core of the revision is the extension of the duty. Under Art. 14 of the former FADP,private persons had to inform only when they collected sensitive personal data or personality profiles. Federal bodies were already obliged under Art. 18a of the former FADP to inform on every collection **BBl 2017 6941**. According to the Federal Council's Dispatch, the duty now applies to all processing by private controllers, subject to certain exceptions. The aim is generally better transparency **BBl 2017 6941**.

Comparing similar cases shows how significant this step is:

- Former law: The Criminal Appeals Chamber of the Canton of Bern held that a GPS tracker fitted to a vehicle triggered no duty to inform at all. A vehicle's movement profile contained no sensitive personal data and was not a personality profile. Art. 34 of the former FADP was therefore clearly not fulfilled **BK 2017 358**.
- Current law, Thurgau: The Thurgau High Court regards retrieving AirTag location data of another person's vehicle as, in principle, a collection that triggers Art. 19 FADP **RBOG 2025 Nr. 10**.
- Current law, Fribourg: The Fribourg Cantonal Court upheld a conviction under Art. 19(1) and (2) in conjunction with Art. 60(1)(b) FADP for a GPS tracker placed on the brother's vehicle **501 2025 197**.

Older decisions on private persons' duty to inform therefore cannot be transposed to the current law insofar as they rest on the former limitation to sensitive data.

In Parliament, the Federal Council's draft (Art. 17 draft FADP) remained essentially unchanged **BBl 2017 7193**:

- "Appropriate" in para. 1: The National Council inserted the word ("angemessen") **AB 2019 N 1805**.
- Para. 4: A minority sought to delete the information on disclosure abroad as too detailed and disproportionate. It was defeated by 157 votes to 39 **AB 2019 N 1805**.
- Para. 2(d) and (e): The Council of States added a list of the data subject's rights and a notice of creditworthiness checks **AB 2019 S 1240**. The National Council deleted both again **AB 2020 N 140**, and the Council of States concurred **AB 2020 S 291**.

An abstract list of data subjects' rights is thus not part of the statutory minimum content. The general clause in para. 2 nonetheless remains decisive: the information must enable data subjects to exercise their rights. The cross-references in para. 4 to Arts. 16(2) and 17 FADP reflect the renumbering of the draft's Arts. 13(2) and 14 (**BBl 2017 7193**; **BBl 2020 7639**).

Temporal Application

Art. 19 FADP has applied unchanged since 1 September 2023. The transitional provision for ongoing processing exempts only Arts. 7, 22 and 23 FADP,and only where the purpose remains unchanged and no new data is collected **Art. 69 FADP**. Art. 19 FADP is not exempted. Every new collection is therefore subject to the new law.

By contrast, FDPIC investigations pending at entry into force are governed by the former law (Art. 70 FADP) **Art. 70 FADP**:

- The FDPIC therefore still assessed the privacy notice of Ricardo and TX Group under Art. 4(4) and Art. 14 of the former FADP **EDÖB Schlussbericht vom 11. April 2024 i.S. Ricardo AG und TX Grou** .
- In the "Pfarrer-Check" (pastor check) case, the investigation was opened only after entry into force. The Federal Administrative Court therefore applied the new FADP **a-2941-2024**.

Who Is Bound and Scope of Application

Only the controller is bound, i.e. whoever, alone or jointly with others, determines the purpose and means of the processing (Art. 5(j) FADP) **Art. 5 FADP**. The processor is not itself subject to the duty to inform. According to the explanatory report on the Data Protection Ordinance (DPO), Art. 13 DPO is addressed solely to the controller. The controller must, however, disclose when data is passed to a processor **EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -** . The Valais Cantonal Court cites processors as an example of recipients within the meaning of para. 2(c) **P3 25 9**.

Within corporate groups, allocating roles is delicate. In the Ricardo case **EDÖB Schlussbericht vom 11. April 2024 i.S. Ricardo AG und TX Group A** :

- Processing by TX Group for purposes determined by Ricardo was processing on behalf of Ricardo.
- For processing for its own and group-wide purposes, TX Group was itself the controller or a joint controller.
- The FDPIC objected that this allocation of roles was not clear from the privacy notice.

The report still concerns the former law. It shows, however, that an unclear allocation of responsibility is itself a transparency deficiency.

The scope of application has the following limits:

- Natural persons only: The FADP applies only to personal data of natural persons (Art. 2(1) FADP) **Art. 2 FADP**. Legal entities are no longer protected by the revised Act or its criminal provisions (**HG220030**; **BK 2025 65**).
- Personal use: Data processed by a natural person exclusively for personal use is excluded (Art. 2(2)(a) FADP) **Art. 2 FADP**. The Valais Cantonal Court refused to apply this exception to a camera at a restaurant. It covered the customer car park and thus data outside the owner's private sphere **P3 25 9**.
- Proceedings: In court proceedings and in proceedings under federal procedural codes, procedural law prevails. By contrast, the FADP applies to first-instance administrative proceedings (Art. 2(3) FADP) **Art. 2 FADP**.
- Cantonal bodies: Cantonal law applies to them, in the Canton of Vaud for instance Art. 13 LPrD **ge-2026-0008**.
- Territorial scope: The Act covers situations that have an effect in Switzerland, even if they originate abroad. Private-law claims are governed by the Private International Law Act (Art. 3 FADP) **Art. 3 FADP**.

Trigger: The Concept of Collection

Collection is a form of processing (Art. 5(d) FADP) **Art. 5 FADP**. The Thurgau High Court understands it as the activity by which someone intentionally gains knowledge of the data or acquires control over it. It requires "ein aktives, gezieltes Vorgehen des Verantwortlichen" ("an active, targeted course of action by the controller"), which calls for "eine gewisse Planmässigkeit" ("a certain degree of planning") **RBOG 2025 Nr. 10**. On this definition, merely incidental knowledge does not trigger the duty, whereas targeted retrieval does.

In the Thurgau case, retrieval via the "Find My" ("Wo ist?") function sufficed. The location data was personal data of the appellant, because the vehicle was suspected to be used exclusively by him **RBOG 2025 Nr. 10**.

Collection from third parties is also covered. The Federal Administrative Court applied this to a debt collection company that collected the data of alleged debtors mostly from third parties and published it. The fact that the data subjects could react afterwards did not replace the information **a-3891-2025**.

Content of the Information: General Clause and Minimum Information

Para. 2 operates on two levels. The general clause requires the information necessary for data subjects to exercise their rights and for processing to be transparent. The list in letters (a)-(c) sets out the minimum content:

- the controller's identity and contact details,
- the purpose of processing,
- where applicable, the recipients or categories of recipients.

Further information is therefore owed where the particular case requires it for transparency. As regards recipients, the Dispatch highlights categories **BBl 2017 6941**. The Act allows either individual recipients or categories to be named.

According to case law, the yardstick is the processing actually carried out. Two cases illustrate this:

- "Pfarrer-Check": An association had sent pastors a questionnaire by e-mail and stated that the answers would be published. For further information it referred to its website. The Federal Administrative Court objected on two counts. The reference to the website was insufficient to ensure transparent processing. Moreover, data subjects could not recognise that their data would be published even if they did not complete the questionnaire **a-2941-2024**. The information was thus incomplete precisely regarding the processing that most affected the data subjects.
- Ricardo: The FDPIC required the privacy notice to show for which purposes which personal data is processed and which platforms are involved in tracking. It must also reflect the processing actually carried out **EDÖB Schlussbericht vom 11. April 2024 i.S. Ricardo AG und TX Grou** .

According to cantonal case law, how "appropriate" the information must be depends on the context. The Valais Cantonal Court examined video surveillance against Art. 19(2) FADP.A sign on the entrance door sufficed, although it stated neither the purpose nor the controller. The purpose was clearly recognisable to anyone using a restaurant car park, and only the owner could obviously be the controller **P3 25 9** . The reasoning comes close to the exception in Art. 20(1)(a) FADP (the data subject already has the information) **Art. 20 FADP**. It should, however, be read as a case-specific assessment by a cantonal court. It does not license a general waiver of the minimum information.

Form: Precise, Comprehensible, Easily Accessible

Under Art. 13 DPO, the information must be communicated "in präziser, transparenter, verständlicher und leicht zugänglicher Form" ("in a precise, transparent, comprehensible and easily accessible form") **Art. 13 DPO**. The Act prescribes no particular form. The Dispatch states that the information may be given "in einfacher, standardisierter Weise" ("in a simple, standardised manner") **BBl 2017 6941**.

The explanatory report on the DPO specifies **EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -** :

- The data subject should receive the essential information at the first level of communication.
- Further information may be made available in a structured overview.
- Pictograms were deleted from the draft because businesses would not have been able to implement them in the required form.

In the Ricardo case, the FDPIC recommended a layered approach: a concise overview at the top level, with a link to the detailed notice. The privacy notice must be easy to find, comprehensible and clearly structured **EDÖB Schlussbericht vom 11. April 2024 i.S. Ricardo AG und TX Group A** . Combined with the "Pfarrer-Check" judgment, this means: a link to further information is permissible if the first level itself contains the essential information. A link is not sufficient, however, where it is meant to replace information about processing that significantly affects the data subject **a-2941-2024**.

Collection from Third Parties: Data Categories and One-Month Deadline

Where data is not collected from the data subject, the Act tightens the duty in two respects:

- Content: The categories of personal data processed must also be communicated (para. 3). In this situation, data subjects do not know from their own involvement which data has been collected **a-2941-2024**.
- Timing: The information must be provided at the latest one month after receipt of the data, or, if the data is disclosed earlier, at the latest at the time of disclosure (para. 5).

The Federal Administrative Court applied the one-month deadline in the debt collection case. The data subjects should have received the necessary information at the latest one month after receipt of the data. No exception under Art. 20 FADP applied **a-3891-2025**. The rule on earlier disclosure is particularly significant in such a case: whoever publishes data must inform at the latest upon publication and may not use up the one-month period.

The Dispatch mentions the one-month deadline for third-party collection without elaborating on when it begins to run **BBl 2017 6941**. In the National Council, a minority proposed that the deadline should cover only the information under paras. 2 and 3. Consistently with its motion to delete para. 4, it was defeated **AB 2019 N 1805**. The deadline therefore also applies to the information on disclosure abroad.

For cantonal bodies, cantonal law sets its own timing. Vaud law requires written information, in the case of third-party collection, at the latest when the data is recorded **ge-2026-0008**. The Vaud Administrative Court concluded that the information need not precede the collection but may be deferred **ge-2014-0110**.

Disclosure Abroad

Where personal data is disclosed abroad, para. 4 requires the following additional information:

- the State or the international body,
- where applicable, the guarantees under Art. 16(2) FADP or the application of an exception under Art. 17 FADP.

The Dispatch stresses that the data subject must, in particular, know the name of the third State **BBl 2017 6941**. On the failed motion to delete para. 4, see the section on legislative history.

The structure follows from Arts. 16 and 17 FADP.Without an adequacy decision by the Federal Council, disclosure is permitted only with appropriate guarantees, such as standard data protection clauses or binding corporate rules **Art. 16 FADP**. Otherwise, an exception is required, such as express consent or a direct connection with a contract **Art. 17 FADP**. The information under para. 4 must therefore match the legal basis chosen. Where the Federal Council has recognised the State as adequate, naming the State suffices according to the wording, since guarantees and exceptions must be communicated only "if applicable".

For the USA, the FDPIC requires additional guarantees under Art. 16(2) FADP as long as no adequacy decision applies **EDÖB 31. Tätigkeitsbericht 2023/2024** In such cases, the guarantees must consequently be stated.

Exceptions and Restrictions (Art. 20 FADP)

Art. 20 FADP distinguishes two types of situations **Art. 20 FADP**.

The duty lapses (paras. 1 and 2) if

- the data subject already has the information,
- the processing is provided for by law,
- the private controller is bound by a statutory duty of confidentiality,
- the conditions of Art. 27 FADP are met.

In the case of third-party collection, it also lapses if providing the information is impossible or requires disproportionate effort.

The controller may restrict, defer or dispense with the information (para. 3) if

- overriding interests of third parties so require,
- the information would defeat the purpose of the processing,
- for private controllers: overriding own interests exist and the data is not disclosed to third parties; group companies are not deemed third parties for this purpose (para. 4),
- for federal bodies: overriding public interests so require or proceedings would be jeopardised.

The legislative history shows how narrowly the legislature intended the exceptions. The National Council had wanted to extend the disproportionate-effort exception to direct collection. It abandoned this in the procedure to resolve differences, because the draft and European law allow it only for third-party collection. On the group privilege, a compromise from the Council of States prevailed **AB 2020 N 140**. The wording therefore deliberately confines disproportionate effort to para. 2.

On processing provided for by law, there is a leading Federal Supreme Court decision under the former law (Art. 18a(4)(a) former FADP). In administrative assistance in tax matters, the Tax Administrative Assistance Act (StAhiG) expressly governs the transmission of third parties' data and the information to be given to them. The general prior duty to inform under the FADP therefore lapses. The Federal Supreme Court reserved, however, that prior information may be required in individual cases involving sensitive data **BGE 148 II 349**. For Art. 20(1)(b) FADP this implies: the special provision must provide for the processing with sufficient specificity, and for particularly sensitive data a case-by-case assessment remains reserved. This transposition rests on a decision under the former law.

The Federal Administrative Court's case law on FINMA shows that an exception is not readily assumed. For the appellant's own data, no restriction under Art. 18b of the former FADP was apparent. The failure to inform was unlawful **2024iv-2**.

There is a cantonal example of deferral on account of overriding interests. Under cantonal law, the Vaud Administrative Court accepted that a municipality considering concluding a contract could initially collect data about the prospective contracting party through a detective agency without that party's knowledge. It later informed him of the purpose and supplemented the information at his request **ge-2014-0110**. The decision illustrates the logic of deferral: the information is provided later, not withheld permanently.

A Federal Supreme Court decision on cantonal police law shows how strict the standard for such reservations is. The Court annulled a provision under which subsequent notification of preventive covert investigation could be deferred or omitted across the board "wenn dies zum Schutz überwiegender öffentlicher oder privater Interessen notwendig ist" ("if this is necessary to protect overriding public or private interests"). Notification is a precondition of legal protection **1C_39/2021**. The decision does not concern the FADP.By analogy, however, it supports the view that dispensing with information under Art. 20(3) FADP requires specifically substantiated interests.

In criminal law: whoever legitimately refrains from informing on the basis of Art. 20 FADP does not commit an offence **RBOG 2025 Nr. 10** . The exceptions must therefore already be examined when assessing the elements of the offence. In the Thurgau case, the matter had to be referred back to the public prosecutor because Art. 20(1) and (3)(a)-(c) FADP had not been investigated **RBOG 2025 Nr. 10**.

Recognisability in Video Surveillance and Covert Collection

Private video surveillance is an important field of application. Case law developed here under the principle of recognisability (Art. 4(4) former FADP,now Art. 6(3) FADP) and today links it with Art. 19 FADP.

Timing of the information: According to the Federal Supreme Court, persons must be informed before they enter the camera's field of view. In the case at hand, stickers that were merely visible "von aussen" ("from outside") were not sufficient without further inquiry. The Court referred the case back for the facts to be supplemented **6B_768/2022**. The Valais Cantonal Court adopted this standard under the new law and supplemented it with the minimum information under Art. 19(2) FADP **P3 25 9**. Recognisability is a question of fact that must be investigated. The Geneva Criminal Appeals Chamber therefore referred a case back for examination of whether the surveillance was "reconnaissable, visible, apparente et suffisamment discernable" ("recognisable, visible, apparent and sufficiently discernible") to users

ACPR/685/2023.

Unrecognisable recording: According to the Federal Supreme Court, continuous dashcam recording is not recognisable to those affected. Absent justification, it was unlawful. Following a balancing of interests, the recordings were not admissible in the criminal proceedings **BGE 147 IV 16**.

Justification despite a transparency deficiency: Several decisions leave recognisability open because an overriding interest justifies the processing in any event:

- For an ATM camera, the Federal Supreme Court accepted a security interest in preventing and solving crimes **7B_797/2023**.
- The Bern Criminal Appeals Chamber accepted justification for event-related surveillance of one's own parking space after repeated damage. Decisive were the limitation to what was necessary and a recording time initially of 34 minutes per day. The court stressed that grounds of justification for breaches of the processing principles may be accepted only with great restraint **BK 2021 532**.

Covert surveillance in employment: According to the Federal Supreme Court, a general notice of possible monitoring does not cover the covert use of spyware. The employee had been informed of the possibility of monitoring, "ma certamente non delle modalità invasive e sproporzionate" ("but certainly not of the invasive and disproportionate methods"). The expert report was inadmissible, and the dismissal fell away **BGE 139 II 7**. The decision is based on employment law (Art. 26 ArGV 3) and public-service staff law. For Art. 19 FADP it follows by analogy that the information must cover the specific type of processing.

A Geneva decision under cantonal law points in the same direction. Badge data collected under the notice "en cas de soupçon de malversation" ("in case of suspected misconduct") could not be used to monitor working time. The purpose was not recognisable, and the data had to be destroyed **ATA/1316/2024** In private employment, Art. 328b CO additionally refers to the FADP **Art. 328b OR**.

Consequences of a Breach

Civil-Law Protection of Personality

A violation of personality occurs in particular where personal data is processed contrary to the principles of Art. 6 FADP (Art. 30(2)(a) FADP) **Art. 30 FADP**. It is unlawful unless justified by consent, an overriding private or public interest, or law (Art. 31(1) FADP) **Art. 31 FADP**. Actions are governed by Arts. 28 et seq. Civil Code. In particular, a claimant may request that processing be prohibited or data deleted (Art. 32(2) FADP) **Art. 32 FADP**.

Art. 30(2)(a) FADP does not mention Art. 19 FADP expressly. An information deficiency can, however, be captured through the transparency principle. In the debt collection case, the Federal Administrative Court based the violation of personality on Art. 6(3) FADP alone. It left open whether Art. 19 FADP was also breached **a-3891-2025**. Justification for breaches of the processing principles is not excluded, but may be accepted only with great restraint. In the Logistep case, neither the economic interest nor the interest in combating copyright infringements sufficed to justify the covert collection of IP addresses **BGE 136 II 508**. For video surveillance cases in which justification was accepted, see the section on recognisability in video surveillance and covert collection.

An information deficiency does not automatically lead to deletion. In relation to FINMA, the Federal Administrative Court found the failure to inform unlawful. It nonetheless refused to delete the entry, because the processing was otherwise permissible **2024iv-2**. Whether the deficiency justifies deletion thus depends on whether the processing is also substantively unlawful.

Supervision by the FDPIC

The FDPIC opens an investigation ex officio or upon notification if there are sufficient indications of a breach. It may refrain from doing so for breaches of minor significance (Art. 49(1) and (2) FADP) **Art. 49 FADP**. In particular, it may order the controller to inform the data subjects in accordance with Art. 19 FADP (Art. 51(3)(c) FADP). If the controller has taken the necessary measures during the investigation, the FDPIC may confine itself to a warning (Art. 51(5) FADP) **Art. 51 FADP**. In both Federal Administrative Court judgments under the new law, the transparency deficiency served as grounds for further-reaching measures: cessation of publication and deletion of the data (**a-3891-2025**; **a-2941-2024**).

Criminal Liability

Private persons are liable, on complaint, to a fine of up to CHF 250,000 if they wilfully fail to inform in accordance with Art. 19(1) FADP or to provide the information under Art. 19(2) FADP.Wilfully providing false or incomplete information is also punishable (Art. 60(1) FADP) **Art. 60 FADP**. The omission offence expressly mentions only paras. 1 and 2. The additional information under paras. 3 and 4 and the deadline under para. 5 are not listed there. Federal bodies are not covered.

The Geneva Criminal Appeals Chamber emphasises intent and the complaint requirement **ACPR/239/2025**. Legal entities are not entitled to file a complaint, as they are no longer protected **BK 2025 65**. On the exclusion of criminal liability where information is legitimately withheld under Art. 20 FADP,see the section on exceptions.

The Fribourg Cantonal Court upheld a conviction for a GPS tracker attached for a few days. It reduced the fine, however, from CHF 20,000 to CHF 4,000. Decisive was that the violation and its consequences remained limited and that it was a one-off offence **501 2025 197**.

Further rules:

- Business undertakings: Offences within business undertakings are governed by Arts. 6 and 7 of the Federal Act on Administrative Criminal Law. For fines up to CHF 50,000, the undertaking may be convicted instead of the responsible persons (Art. 64 FADP) **Art. 64 FADP**.
- Jurisdiction: Prosecution and adjudication are the responsibility of the cantons. The FDPIC may file a complaint and exercise the rights of a private claimant (Art. 65 FADP) **Art. 65 FADP**.
- Limitation: The right to prosecute becomes time-barred after five years (Art. 66 FADP) **Art. 66 FADP**.

Practical Guidance

- Clarify roles: First determine who the controller is. In group settings, disclose the allocation of roles in the information.
- Align the information with the actual processing: Processing with significant impact, such as publication, must be stated expressly at the first level. A mere reference to a website does not suffice.
- Third-party collection: State the data categories. Monitor the one-month deadline and inform at the latest at the time of any earlier disclosure.
- Disclosure abroad: State the State and, depending on the legal basis, the guarantees or the exception relied on.
- Document exceptions: Anyone relying on Art. 20 FADP should record the specific interests involved. The civil, supervisory and criminal assessment depends on them.
- Video surveillance: Place notices so that they are perceptible before persons enter the area covered.