

Commentary on Art. 5 FADP: Definitions

Function of the Definitions and the 2020 Change of System

Art. 5 FADP contains the statutory definitions on which the whole Act relies. They determine whether the FADP applies at all, since it covers personal data of natural persons processed by private persons or federal bodies (Art. 2 para. 1 FADP **Art. 2 FADP**). They also trigger heightened legal consequences, in particular under Art. 6 para. 7, Art. 22, Art. 24, Art. 30 and Art. 34 FADP. Those consequences are discussed under the relevant definitions below (sensitive personal data, profiling, breach of data security). Classification under Art. 5 therefore often decides the outcome of a case.

Art. 5 FADP has not changed since it entered into force on 1 September 2023. Later amendments to the Act concern other provisions. The amendment to the Information Security Act of 29 September 2023 inserts only Art. 24 para. 5bis FADP **BBi 2023 2296 Art. 24 FADP**. Subsequent federal legislation, such as the 2025 amendment to the Federal Personnel Act, refers to Art. 5 let. c FADP and its individual numbers as a fixed point of reference without amending it **BBi 2025 2028**.

The total revision restructured the catalogue compared with Art. 3 of the former FADP (fFADP). The Federal Council Dispatch names modernised terminology as the guiding principle, "insbesondere um die Vereinbarkeit mit dem Recht der Europäischen Union zu verbessern" (in particular to improve compatibility with European Union law) **BBi 2017 6941**. In detail:

- Protection of data relating to legal entities is abolished. The Dispatch says it had been "nur von geringer praktischer Bedeutung" (of only minor practical importance) **BBi 2017 6941**.
- The concept of a data file is dropped, because data "heute wie eine Datensammlung genutzt werden, auch wenn sie nicht zentral gespeichert sind" (are today used like a data file even if they are not stored centrally) **BBi 2017 6941**.
- The personality profile, a Swiss particularity, is replaced by profiling. The "controller of the data file" is replaced by the "controller" **BBi 2017 6941**.
- Genetic and biometric data become sensitive. The breach of data security and the processor are newly defined **BBi 2017 6941**.
- High-risk profiling (let. g) was not in the draft. It is a parliamentary compromise (see below under profiling).

According to the Dispatch, alignment with EU law means moving closer to Regulation (EU) 2016/679 (GDPR), not adopting it **BBi 2017 6941**. For the controller and the processor, the Dispatch expressly refers to the corresponding concepts in the GDPR and in the modernised Council of Europe Convention 108 **BBi 2017 6941**. The European concepts are therefore an aid to interpretation, but they do not override the Swiss wording, as let. g shows. On data security, the Zurich High Court used the GDPR as a benchmark. It held that companies meeting the GDPR's technical and organisational requirements also satisfy Swiss law **UE240472**.

Whether case law under the former Act still applies depends on the definition. The Federal Supreme Court applies Art. 5 let. a FADP using the established formula. With regard to the right of access, it holds that the case law under the fFADP "reste en principe valable" (remains valid in principle) **4A_504/2025**. Where the wording was carried over (personal data, processing, disclosure, federal body),

older decisions remain useful for interpretation. Where a definition was reformulated (profiling, genetic and biometric data), applying older case law needs its own justification. For the controller, the Dispatch treats the new concept as the successor to the controller of the data file, so the earlier case law remains relevant (see below under controller).

Personal Data (let. a)

Information Relating to a Person

Personal data means "any information" relating to an identified or identifiable natural person. The concept does not depend on the medium. Images are also personal data, "ohne dass es auf die Beschaffenheit des Datenträgers ankommt" (irrespective of the nature of the data carrier) **BGE 138 II 346**. Both facts and value judgements are covered. According to the Federal Supreme Court, personal data may "consister en des constatations de fait ou en des jugements de valeur se rapportant à la personne en cause" (consist of findings of fact or of value judgements about the person concerned) **4A_504/2025**.

In that case, statements in an internal investigation report about a professor's conduct were data of both the professor and the persons interviewed. Passages dealing only with the purpose or chronology of the investigation, or with third parties, were not the applicant's personal data **4A_504/2025**. The link to a person must therefore be assessed passage by passage, and the same item of information may relate to several data subjects.

The Geneva Court of Justice found no link to a person where an individual was mentioned only in a functional capacity. Naming the managing director as the company's representative in inspection reports contained no information about his personal situation. The data concerned the company itself, which acts through its organs **ACJC/1571/2025**. This cantonal application prevents the exclusion of legal entities from being circumvented through their organs.

Identifiability: the Relative Approach

A person is identifiable if they can be identified using additional information. However, "jede theoretische Möglichkeit der Identifizierung" (every theoretical possibility of identification) is not enough **BGE 136 II 508**. If the effort required is so great that, by general experience, no interested party would undertake it, the person is not identifiable **BGE 136 II 508**. What matters is the effort objectively required and the interest of the processor or a third party in identifying the person **BGE 136 II 508**.

The assessment is made "aus der Sicht des jeweiligen Inhabers der Information" (from the perspective of whoever holds the information). Where data are passed on, it is sufficient "wenn der Empfänger die betroffene Person zu identifizieren vermag" (if the recipient is able to identify the data subject) **BGE 136 II 508**. In the Logistep case, dynamic IP addresses were therefore personal data. The business model depended on rights holders later identifying the subscribers, and it was enough that a part of the stored information was identifiable **BGE 136 II 508**. The Telecommunications Act did not prevent the FADP from applying **BGE 136 II 508**.

Further case law shows the range of situations:

- Unique identifiers. In a sampling frame archived by the Federal Statistical Office (FSO), the information remained personal data because the FSO could link it to the address register through the social security (AHV) number. Archiving did not change this **1C_425/2020**.
- Pseudonymisation. It does not remove the link to a person if the recipient can identify the person from the data and their context. When employee and account data were sent to the US Department of Justice, the leaver list and the fact sheet naming the client adviser were enough. The Federal Supreme Court left open whether the US authorities' additional knowledge from SWIFT data also counted **4A_365/2017**.
- Images. In Street View, faces, vehicle number plates and images of houses, gardens and courtyards were sufficient, because a link to a person can easily be made **BGE 138 II 346**.
- Effective anonymisation. Anonymised invoices and medical records are not personal data under Art. 5 let. a FADP if they contain nothing that points to a particular insured person. The protective rules for health data then do not apply **BGE 151 V 30**. According to the Dispatch, the Act does not apply to anonymised data if re-identification by third parties is impossible **BBi 2017 6941**.

The decisions on the sampling frame **1C_425/2020** and on the anonymised invoices **BGE 151 V 30** do not conflict. In each case the decisive question is whether the specific holder or recipient has an identifier it can realistically use to link the data to a person. A party relying on anonymisation must therefore show that neither it nor the recipient holds such a key.

Data Subject (let. b)

Exclusion of Legal Entities and Transition

Only a natural person whose personal data is processed is a data subject. The Dispatch refers legal entities to other protective instruments, in particular protection of privacy under Art. 13 of the Federal Constitution, the personality protection of the Civil Code, and the Unfair Competition Act **BBi 2017 6941**.

The courts apply this exclusion consistently. According to the Federal Administrative Court, the new FADP abolished data protection for legal entities. Access requests under the FADP can now cover only the data of the natural person involved **a-1251-2024**. The Geneva Court of Justice applied the revised FADP immediately to pending civil proceedings, and the claimant company lost its standing to sue during the proceedings **ACJC/1571/2025**. For appeal proceedings, the Federal Administrative Court holds, referring to Art. 70 FADP, that the new law applies to pending appeals against first-instance decisions issued after it entered into force **a-1251-2024**.

A temporary transitional rule exists only for federal bodies. Provisions in other federal acts that relate to personal data continue to apply to data of legal entities for five years after entry into force, in particular to disclosures under Art. 57s paras. 1 and 2 of the Government and Administration Organisation Act **Art. 71 FADP**. The Dispatch explains that this avoids gaps in the law **BBi 2017 6941**. Art. 71 FADP provides no corresponding period for private controllers **Art. 71 FADP**.

Data of Deceased Persons

The FADP does not expressly regulate data of deceased persons. Ruling on cantonal data protection law, the Bern Administrative Court held that personality protection ends with death, so that "Informationen über Verstorbene" (information about deceased persons) is not personal data. Relatives may, however, rely on their own personality rights where the memory of the deceased is at stake or where the information also relates to living persons, for example in the case of hereditary diseases **100 2023 151**. The decision concerns cantonal law, but its reasoning turns on the natural person and is

consistent with let. a and b FADP.

Cantonal law may take a different approach. Geneva law (LIPAD) treats data of deceased persons as personal data with its own access regime. That regime requires a legitimate interest on the part of the relatives and a weighing against the known or presumed wishes of the deceased. Geneva law also covers legal entities under private law **ATA/229/2018**. Under the former federal law, the Federal Supreme Court held that the data protection right of access does not pass to the heirs. It left open whether the ordinance provision on access by close relatives of deceased persons had a sufficient legal basis **BGE 140 V 464**. Relatives therefore usually have to rely on access rights under special legislation or on their own personality rights.

Sensitive Personal Data (let. c)

Exhaustive List and Formal Classification

The list in let. c is exhaustive. On the current law, the Geneva Criminal Appeals Chamber holds that sensitive information is "énumérées, de façon exhaustive, à l'art. 5 let. c" (exhaustively listed in Art. 5 let. c) **ACPR/892/2024**. The Federal Supreme Court had already taken this view of Art. 3 let. c fFADP and concluded that information on income and assets is not covered **1P.79/2000**. Nor are a delivery address, the items purchased and the purchase price sensitive, even where the risk arises precisely from using the data in a particular context **SBE.2022.45/46**. According to the Zurich High Court, financial and address data do not call for a heightened security standard such as end-to-end encryption either **UE240472**.

Under Vaud case law, classification is abstract. It is enough that the data concern one of the listed subjects, regardless of the actual potential for harm **CREP pe23-017055-51/2024**. This does not rule out data from which indirect inferences can be drawn. The dividing line lies in the content of the information: data are sensitive only once they actually reveal something about the protected category.

The legal consequences are significant:

- consent must be express (Art. 6 para. 7 let. a FADP **Art. 6 FADP**);
- disclosure to third parties is presumed, as a rule, to violate personality rights (Art. 30 para. 2 let. c FADP), unless the data were made generally accessible under para. 3 **Art. 30 FADP**;
- federal bodies need a basis in a formal act of parliament (Art. 34 para. 2 let. a FADP), subject to the relief in paras. 3 and 4 **Art. 34 FADP**.

Art. 22 para. 2 let. a FADP presumes a high risk, which triggers a data protection impact assessment, in particular where such data are processed on a large scale. According to its wording, sensitivity alone is not enough **Art. 22 FADP**.

Views and Activities (no. 1)

The Federal Administrative Court applied no. 1 in the "Pfarrer-Check" case. A publicly accessible database listed members of the clergy with the status "erfasst" (recorded) or "angefragt" (asked) in relation to a questionnaire on their religious views. It processed sensitive data. The breach of the principles of proportionality, purpose limitation and transparency violated personality rights under Art. 30 para. 2 let. a and c FADP, and no justification applied **a-2941-2024**. The status alone allowed conclusions about a person's religious position.

Indirect information is sufficient if it reveals a person's views. The Federal Supreme Court classified membership of an association as sensitive because it expresses "eine bestimmte weltanschauliche sowie politische Haltung" (a particular philosophical and political stance). Systematic recording of such membership by a cantonal administration required a clear legal basis **BGE 122 I 360**. Conversely, not everything in a religiously coloured document is sensitive. According to the Geneva Constitutional Chamber, the complainants' religious experience as described was sensitive, but their names were not. Geneva law also covers cultural views and is broader than let. c

no. 1 in that respect **ACST/21/2019**.

Health, Private Sphere, Race and Ethnicity (no. 2)

Health data are data that allow direct or indirect conclusions about a person's physical, mental or psychological condition **ACPR/892/2024**. Purely administrative data of a clinic do not meet this requirement **ACPR/892/2024**.

The threshold shows in cases involving generic references to illness. According to the Ticino court, the entry "malattia" (illness) as a reason for absence on a duty roster says nothing about the condition, type or severity of the illness, so it is not sensitive data **60.2018.232**. Similarly, the Neuchâtel Cantonal Court doubted that a mere reference to "problèmes de santé" (health problems) was sensitive. It added that the result would be different if details of the nature of the problems had been disclosed **CCP.2010.17**. These decisions concern criminal provisions and the former law, but they follow a consistent line: what counts is what the information reveals about the state of health, not the keyword.

On the private sphere, the Basel-Stadt Court of Appeal held under cantonal law that investigations into sexual harassment directly affect the private sphere of both the accused persons and the alleged victims. Their sensitive nature did not rule out access as such, but led to a weighing of interests and to anonymisation **VD.2021.148**.

Genetic and Biometric Data (nos. 3 and 4)

The different wording of nos. 3 and 4 is intentional. The National Council wanted to cover only genetic data that uniquely identify a person **AB 2020 N 140**. The Council of States kept the broader wording, stating: "Genetische Daten sind immer besonders schützenswerte Personendaten, auch wenn sie nicht zur Identifikation einer Person führen." (Genetic data are always sensitive personal data, even if they do not lead to the identification of a person.) **AB 2020 S 291**. The Act therefore limits only biometric data to those that identify a person.

According to the Dispatch, biometric data are personal data obtained through a specific technical process relating to physical, physiological or behavioural characteristics, which allow or confirm the unique identification of a person **BBi 2017 6941**. The Federal Supreme Court classified data from automated facial recognition as sensitive data under Art. 5 let. c no. 4 FADP. It pointed to the risk of false positives where large groups of people are involved **BGE 151 I 137**. Under the former law, the Federal Administrative Court held that fingerprints and the minutiae extracted from them can be attributed to a specific person, whatever the storage format of the template. Central storage breached the principle of proportionality **2009-44**.

On DNA profiles from non-coding regions, the Federal Supreme Court held under Art. 13 para. 2 of the Federal Constitution that, like a fingerprint, they contain only identifying features that reveal nothing about personality. Creating and storing them is therefore a minor interference **BGE 128 II 259**. That decision concerns the seriousness of the interference with a fundamental right, not the category under Art. 5 let. c. It does not conflict with the legislature's choice to treat genetic data as always sensitive, but it may still carry weight when assessing whether processing is proportionate. Vaud practice shows that biometric data (AFIS) and DNA profiles (CODIS) are kept separately and linked only through a process control number, so that the DNA profiles remain anonymous **CREP 397/2026**.

Proceedings and Sanctions (no. 5)

Data relating to administrative and criminal proceedings or sanctions are sensitive. The former Federal Data Protection Commission concluded that a federal body may disclose to another authority only what that authority needs in the specific case for its statutory task. Handing over an entire criminal file, including deleted criminal record entries, was unlawful where answering two questions would have sufficed **150003905**.

Applying the former law by analogy, the Federal Supreme Court treated information about an administrative sanction (exclusion from public procurement) as sensitive data. It held that automatic publication in the official gazette was disproportionate, whereas time-limited publication on the supervisory authority's website was permissible **BGE 148 I 226**. The category thus extends beyond criminal proceedings.

The limit lies in the link to proceedings or a sanction. According to the Geneva Administrative Court, a police log that summarised statements made during a call-out in the conditional and mentioned no proceedings or sanction contained no sensitive data **ATA/1254/2024**. Where court files are evaluated for research, the Schaffhausen High Court required under cantonal law that offenders and victims not be identifiable in the publication **Nr. 95/2001/3**.

Social Assistance Measures (no. 6)

The scope of this category is illustrated mainly by cantonal practice on provisions with identical wording. The Geneva Administrative Court classified information about social assistance as sensitive, including a refusal to cooperate and the suspension of benefits. It held that passing the information to the supplementary benefits office, where this was not necessary, was unlawful **ATA/3/2026**.

Reviewing only for arbitrariness, the Federal Supreme Court confirmed that a child protection file contains sensitive data on the child's health, private sphere and assistance measures. It therefore upheld the refusal of access to the foster parents **1C_376/2022**. By contrast, according to the Bern High Court, an application for legal aid is not social assistance, because it is based on procedural law rather than social assistance law **BK 2018 240**. In 1997 the Federal Data Protection Commissioner also treated unemployment data as social assistance **150003584**. This broad administrative view under the former law should be relied on with caution.

Processing and Disclosure (let. d and e)

Broad Concept of Processing

Processing means "any handling" of personal data, irrespective of the means and procedures used. According to the Dispatch, the substance of the concept is unchanged; storage and deletion were added to the list **BBi 2017 6941**. Simply making recordings in public spaces on which persons or vehicle number plates are recognisable is processing. The Federal Supreme Court also held that dashcam recordings could not be noticed by other road users and were therefore covert, which made the recording unlawful **BGE 146 IV 226**. Publishing images on the internet is likewise processing **BGE 138 II 346**.

Disclosure: Transmitting or Making Accessible

Disclosure covers both actively transmitting data and passively making them accessible. Under the current law, the Federal Administrative Court held that publishing debtors' data on a website is disclosure under Art. 5 let. e FADP and therefore processing. The publication breached the principle of proportionality and was not justified **a-3891-2025**. In the Moneyhouse decision, the court extended disclosure to links that allowed premium users to combine private information about housing, neighbours and household members. The fact that search engines indexed the pages, and that data subjects could request deletion afterwards, did not replace consent **a-4232-2015**.

Disclosure requires a recipient who does not already know the data. The Federal Administrative Court found no disclosure where a military insurer merely told an office that two medicines it had reported would not be reimbursed. The office already had that information; the position would have been different for information about the insured illness **a-7372-2006**. According to the pension fund decision, third

parties are all those who do not need the data for their task. Sending pension certificates to employers unsealed was a disclosure, insofar as the certificates contained data the employers did not already know from their duty to pay contributions **2012-14**.

The legal independence of companies within a group does not exclude disclosure. When the supplementary insurer of the Helsana group obtained data from the group's basic insurers, this was "gleichzeitig eine Bekanntgabe von Daten" (at the same time a disclosure of data) by the basic insurers. Without valid written consent in the individual case, it was unlawful **a-3548-2018**. At cantonal level, the Zurich Administrative Court held that a municipal network operator passing addresses to private telecommunications providers was a disclosure without a legal basis, not outsourcing, because the providers pursued their own business purposes **VB.2020.00700**.

Profiling and High-Risk Profiling (let. f and g)

Profiling as Automated Evaluation

Profiling requires automated processing that evaluates personal aspects of a natural person. The Dispatch stresses that the concept was aligned with European terminology and covers "nur noch die automatisierte Bearbeitung von Personendaten" (only automated processing of personal data) **BBi 2017 6941**. Manual compilations therefore fall outside let. f, even if they could have been a personality profile under the former law.

The Federal Supreme Court described police use of automatic vehicle tracking to create movement profiles as an "Anwendungsfall des datenschutzrechtlich besonders heiklen" (instance of the, in data protection terms, particularly delicate) profiling. It also noted that the decision-making of complex algorithmic systems is hard to follow **BGE 151 I 137**. The decision rests on cantonal police law and Art. 13 of the Federal Constitution, not directly on let. f. Single images lie at the other end of the scale. Under Vaud case law, photographs of a person disposing of waste captured "un instant isolé de vie" (an isolated moment of life) and did not serve to create a profile **CREP pe23-017055-51/2024**.

For private persons, ordinary profiling has no special legal consequences. Federal bodies need express consent, where consent is the basis for the processing, and a basis in a formal act of parliament (Art. 6 para. 7 let. c FADP **Art. 6 FADP**; Art. 34 para. 2 let. b FADP **Art. 34 FADP**).

High-Risk Profiling as a Parliamentary Compromise

Let. g was the longest-running disagreement between the two chambers during the revision. The National Council regarded the category as a "Swiss Finish", because the GDPR draws no such distinction **AB 2020 N 140**. In the procedure to resolve differences, it deleted the provision by 98 votes to 88 **AB 2020 N 1598**. The Council of States deliberately based its definition on "der Definition des Persönlichkeitsprofils im geltenden Recht" (the definition of the personality profile in the current law) **AB 2020 S 291**. The Federal Council stated that this would achieve "ein vergleichbares Schutzniveau wie heute mit den Vorschriften zum Persönlichkeitsprofil" (a level of protection comparable to that currently provided by the rules on personality profiles) **AB 2020 N 140**. The conciliation conference followed the Council of States after being assured that, compared with the existing law and the Moneyhouse case law, the wording would bring "ni une complication des procédures ni une augmentation de la protection" (neither more complicated procedures nor an increase in protection) **AB 2020 N 1817**.

These legislative materials matter for interpretation. They suggest that let. g should be measured against the former personality profile, and in particular against the Moneyhouse decision. There, systematically linking data was enough, even if the data were publicly accessible or not sensitive, if the result provided "Aufschluss über einen oder

mehrere wesentliche Aspekte der Persönlichkeit" (insight into one or more essential aspects of the personality), for example a person's private housing and living situation **a-4232-2015**. In administrative practice, refining address profiles with donation behaviour was likewise treated as a personality profile **150001706**. By contrast, a single copy of an invoice with a delivery address and the items purchased did not allow essential aspects of the personality to be assessed **SBE.2022.45/46**.

Unlike the personality profile, however, let. g requires profiling and therefore automation. In addition, the high risk to personality or fundamental rights must result from the linking of data itself.

The Federal Council rejected a version that would have tied the high risk to the derivation of sensitive data, because the heightened consequences for such data apply in that case anyway **AB 2020 N 140**. For high-risk profiling by private persons, consent must be express where consent is required (Art. 6 para. 7 let. b FADP **Art. 6 FADP**). On credit ratings, the Bern High Court assessed a negative credit report solely under the justification of checking creditworthiness, without classifying it as profiling **BK 2024 170**.

Breach of Data Security (let. h)

A breach of data security exists where personal data are lost, deleted, destroyed or modified, or are disclosed or made accessible to unauthorised persons. According to the Dispatch, this applies "ungeachtet davon, ob der Vorgang mit Absicht geschieht oder nicht, ob er widerrechtlich ist oder nicht" (regardless of whether the event is intentional or not, and whether it is unlawful or not) **BBi 2017 6941**. The definition looks at the result: it describes an outcome, not a breach of duty.

For the Federal Administrative Court, the mere possibility that unauthorised persons can access the data is sufficient; whether anyone actually accessed them is irrelevant. In the case decided, URLs containing personal data had been indexed by a search engine **a-3790-2024**. Confidentiality was likewise missing where pension fund certificates were sent to employers unsealed and were thus "in keiner Weise gegen Einsichtnahme oder Kopieren geschützt" (in no way protected against inspection or copying) **2012-14**. By contrast, the Zurich High Court found no breach where an e-mail containing invoice and address data was sent without end-to-end encryption. The FADP and its ordinance prescribe no particular encryption method, and security measures are to be chosen according to the risk **UE240472**.

The definition triggers the duties under Art. 24 FADP, which are themselves graduated **Art. 24 FADP**:

- the FDPIC must be notified only where the breach is likely to result in a high risk;
- the processor must report every breach to the controller;
- the data subject must be informed where this is necessary for their protection or the FDPIC requests it.

Since the amendment of 29 September 2023, the FDPIC may, with the controller's consent, forward the notification to the National Cyber Security Centre for analysis (Art. 24 para. 5bis FADP) **BBi 2023 2296**. In the search engine case, the Federal Administrative Court found that the duty to inform applied because of the risk of misuse. A public announcement under Art. 24 para. 5 let. c FADP was nonetheless sufficient, because informing each person individually would have been disproportionate **a-3790-2024**.

Federal Body (let. i)

A Functional Concept

A federal body is an authority or service of the Confederation, or a person entrusted with public tasks of the Confederation. Private persons become federal bodies to the extent that such tasks have been assigned to them. The Federal Administrative Court asks

whether a private organisation can issue rulings, as recognised health insurers or accident insurers under the Accident Insurance Act can **a-7367-2006**. The Swiss Federal Railways (SBB) are a federal body because they perform public tasks **a-420-2007**.

Federal body status depends on the activity concerned. Where a federal body acts under private law, Art. 40 FADP applies the provisions for private persons **BBI 2020 7639**. On the former law, which was worded identically, the Federal Administrative Court held that the line is drawn by the nature of the underlying relationship. The SBB's collection of data in connection with issuing the SwissPass was governed by civil law, so there was no right to a formal ruling **a-5921-2020**. Likewise, transport contracts, the ticket shop and customer service fell within the jurisdiction of the civil courts, whereas data from the former employment relationship under public law could be challenged through administrative proceedings **a-420-2007**. Within a health insurance group, only the basic insurers are federal bodies, and only for mandatory health insurance. The supplementary insurer acts as a private person **a-3548-2018**.

The classification has significant consequences. Federal bodies are subject to the principle of legality, the disclosure rules in Art. 34 and 36 FADP, and the legal remedies under Art. 41 FADP **BBI 2020 7639**.

Distinction from Cantonal Bodies

Cantonal and municipal bodies are not federal bodies, "même s'ils sont chargés de l'exécution de tâches de la Confédération" (even if they are entrusted with implementing federal tasks). Cantonal data protection law therefore applies to the cantonal disability insurance office, and appeals do not go to the Federal Administrative Court **1C_125/2015**. The same applies to debt enforcement and bankruptcy offices. The Graubünden Administrative Court also held that Art. 8a of the Debt Enforcement and Bankruptcy Act governs the right to inspect records exhaustively and takes precedence over both the FADP and cantonal law **PVG 2020 27**. Federal law may, however, extend the FADP's scope through special legislation. Under Art. 54 of the Passenger Transport Act, the FADP applies to licensed transport companies even where a canton is the majority shareholder **ge-2023-0172**.

Controller and Processor (let. j and k)

Deciding on Purpose and Means

The controller is whoever, alone or jointly with others, determines the purpose and means of processing. According to the Dispatch, the controller corresponds to the former controller of the data file. The means include, for example, manual or automated processing and the software used **BBI 2017 6941**. Case law under the former law therefore remains relevant. The controller of the data file was whoever determined the purpose and the means of processing, "ohne zwingend über die einzelnen Daten selbst verfügen zu müssen" (without necessarily having to control the individual data themselves). Data bought from third parties and used unchanged also formed part of the data file of the platform operator, which decided how they were used **a-4232-2015**. Controller status can be inferred from business activity, for example from regularly disclosing address data for advertising purposes. A person who has data processed by third parties remains obliged to provide access **a-5225-2015**.

The distinction decides who can be sued. According to the Schwyz Cantonal Court, Art. 8 fFADP and Art. 25 FADP in principle oblige only the controller to provide information. A person who is not a controller need not even state whether they process data, subject to the rules on processors in the ordinance **ZK1 2023 22**.

Joint control ("jointly with others") is regulated in more detail only for federal bodies. The Federal Council regulates control and responsibility where a federal body processes data together with other federal bodies, cantonal bodies or private persons **Art. 33 FADP**. For private persons, the Moneyhouse decision on a jointly operated data

file shows the practical consequence under the former law: the right of access could be asserted against each controller, and a controller who was not responsible had to forward the request **a-4232-2015**.

Processor

A processor processes data "on behalf of" the controller and does not decide on the purpose. According to the Dispatch, the controller must actively ensure that the processor complies with the Act to the same extent as the controller itself. Storing data in a cloud is in principle a case of processing on behalf of a controller **BBI 2017 6941**.

Assigning processing to a processor is permitted if the data are processed only in the way the controller itself would be allowed to process them, and no duty of confidentiality prevents it. Sub-processing requires prior authorisation, and the processor may rely on the same justifications as the controller **Art. 9 FADP**. A person who hands over processing without meeting these conditions may be criminally liable under Art. 61 let. b FADP; the Schwyz Cantonal Court therefore set aside a decision not to open criminal proceedings **BEK 2024 84**.

A party pursuing its own purposes is not a processor. Moneyhouse's data suppliers were not processors, because the relationship was a sale **a-4232-2015**; the buyer itself became a controller.

Telecommunications providers that used the municipal fibre-optic network for their own retail services did not perform an auxiliary function. Under cantonal law, they were not processors but recipients of a disclosure **VB.2020.00700**. The decisive factor is therefore not what the contract calls the role, but who actually determines purpose and means.

Practical Consequences

- Document the link to a person. Before passing on data said to be anonymised, check whether the recipient has identifiers (AHV number, customer number, contextual knowledge). Pseudonymisation is not enough if the recipient can identify the person **4A_365/2017**.
- Assess sensitive categories by content. Whether data fall under let. c depends on what they reveal about the category. In cantonal practice, keywords such as "ill" are not enough, but details of the nature of the illness are **CCP.2010.17**.
- Treat intra-group flows as disclosure. Data flows between legally independent group companies must be assessed as disclosures and need their own justification (see above under disclosure) **a-3548-2018**.
- Define the roles. For each data flow, determine who decides on purpose and means. Data purchases and cooperation with partners pursuing their own purposes are not processing on behalf of a controller **a-4232-2015**.
- Separate public-law activities. Federal bodies and private persons entrusted with public tasks should classify their processing by the nature of the underlying relationship, because the legal basis and the legal remedies depend on it **a-5921-2020**.
- Check exposed data for a breach. Accessibility to unauthorised persons alone, for example through indexing, makes it necessary to examine the duty to notify **a-3790-2024**.