

Commentary on Art. 6 FADP: Principles of Data Processing

Function, Scope and Legislative History

Art. 6 FADP brings together the substantive processing principles: lawfulness (para. 1), good faith and proportionality (para. 2), purpose limitation and recognisability (para. 3), storage limitation (para. 4), accuracy (para. 5) and the validity of consent (paras. 6 and 7)

Art. 6 FADP. According to the Federal Council's Dispatch, the Act gives concrete form to the right to informational self-determination under Art. 13(2) of the Federal Constitution, i.e. the right to decide, in principle, whether and for what purposes data about oneself are processed **BBI 2017 6941**.

Scope. The principles apply to every processing of personal data of natural persons by private persons and federal bodies. Excluded are in particular processing exclusively for personal use and the deliberations of the Federal Assembly; for court proceedings and proceedings under federal procedural codes, the relevant procedural law governs **Art. 2 FADP**. Cantonal bodies are subject to cantonal data protection law; decisions on cantonal law are therefore cited here only as parallel assessments. "Processing" covers any handling of personal data, from collection through storage to erasure **Art. 5 FADP**.

Cumulative application. According to the Federal Administrative Court, Art. 6 FADP contains the essential substantive principles for private processors and federal bodies alike; these "müssen kumulativ eingehalten werden und sind unabhängig voneinander zu prüfen" (must be complied with cumulatively and are to be examined independently of one another) **a-2941-2024**. Processing that complies with one principle may therefore fail on another. In the case of a publicly accessible database that, as part of a campaign involving a questionnaire on religious topics, listed contacted persons with the status "recorded" or "contacted", the Court found violations of proportionality, purpose limitation and transparency side by side **a-2941-2024**.

Former law. Paras. 1, 2, 6 and 7 derive from Art. 4 of the former FADP in the version of 24 March 2006, para. 5 from Art. 5 of the former FADP; para. 3 combines the former principles of purpose limitation and recognisability **BBI 2006 3547 BBI 2017 6941**. Case law on Art. 4 and 5 of the former FADP therefore remains relevant for interpretation, but must in each case be measured against the new wording. On the legislative history of the consent rules, see below under paras. 6 and 7. The text of Art. 6 as adopted on 25 September 2020 corresponds to the wording in force **BBI 2020 7639**, and the wording has remained unchanged since entry into force on 1 September 2023 **DSG (2025-07-07)**.

Transitional law. For ongoing processing, Art. 69 FADP exempts only Arts. 7, 22 and 23, not Art. 6; the principles have therefore applied since 1 September 2023 also to processing begun earlier **Art. 69 FADP**. Investigations by the Federal Data Protection and Information Commissioner (FDPIC) pending at entry into force remain subject to the former law **Art. 70 FADP**. The decisive point is the formal opening of the investigation: in the database case, prior correspondence and informal enquiries did not suffice, so that the new law applied **a-2941-2024**.

Breach of Principles, Justification and Legal Basis

Private processors: breach as a violation of personality

For private persons, Art. 6 FADP must be read together with Arts. 30 and 31 FADP. A violation of personality exists in particular where personal data are processed contrary to the principles of Arts. 6 and 8 FADP **Art. 30 FADP**. It is unlawful unless justified by consent, an overriding private or public interest, or law **Art. 31 FADP**. The breach of a principle thus establishes the violation; justification is a second, separate stage of the analysis.

The Federal Supreme Court held under the former law that justification of processing contrary to the principles is not excluded in general, but that grounds of justification "nur mit grosser Zurückhaltung bejaht werden können" (can be accepted only with great restraint) in the specific case **BGE 136 II 508 BGE 138 II 346**. In the Logistep case, concerning the covert collection of IP addresses in peer-to-peer networks for transmission to rights holders, even the interest in effectively combating copyright infringements could not outweigh the breach of purpose limitation and recognisability **BGE 136 II 508**. Under the new law, the Federal Administrative Court likewise examines Art. 31 FADP once a breach of Art. 6 FADP has been established, and in two internet publication cases it rejected every ground of justification. In the publication of alleged debtors, consent and a legal basis were lacking, and the Court gave no weight to the interests in warning the public and in debt collection, because criminal prosecution and debt enforcement law are available for those purposes **a-3891-2025**. In the religious database case, Art. 31(2)(f) FADP did not cover the disclosure to third parties **a-2941-2024**. A person who breaches a principle can therefore rely on overriding interests only exceptionally.

Federal bodies: legal basis and principles side by side

Federal bodies may process personal data only on the basis of a legal provision; for sensitive personal data, profiling and potentially serious interferences with fundamental rights, a formal statute is in principle required **Art. 34 FADP**. Consent in the individual case is here only an exceptional ground (Art. 34(4)(b) FADP) **Art. 34 FADP**. The Federal Supreme Court accepted, for an entry in the military medical information system MEDISA, a basis in a formal statute, the Armed Forces Act; that the data subject had not known of the entry did not affect its lawfulness **1C_524/2024**. The legal basis does not, however, release the body from Art. 6 FADP: in a RIPOLE alert, the Federal Administrative Court examined storage limitation under Art. 6(4) FADP and proportionality and held storage until the limitation period for enforcement expired to be suitable, necessary and reasonable **a-7720-2025**.

Lawfulness (Para. 1)

Para. 1 covers every processing, not only collection **BBI 2003 2101**. Its reach is nonetheless limited. According to the Federal Administrative Court, processing for an unlawful purpose is unlawful in

data protection terms only "wenn dabei gegen eine Norm verstossen wird, die zumindest auch, direkt oder indirekt, den Schutz der Persönlichkeit einer Person bezweckt" (if a norm is thereby breached that is intended, at least also, directly or indirectly, to protect a person's personality) **a-3548-2018**. In the *Helsana+* bonus programme case, a possible breach of the premium rules of the Health Insurance Act (KVG) therefore did not render the processing unlawful, because those rules serve the principle of mutuality in social health insurance and not the protection of personality **a-3548-2018**.

The same decision shows the opposite direction: collecting data from compulsory health insurance was unlawful because the consent required by the special statute was lacking **a-3548-2018** (on the formal requirements see below under para. 7). Special statutory requirements for consent and disclosure thus feed into the FADP through para. 1. The decision was rendered under Art. 4(1) of the former FADP, whose wording Art. 6(1) FADP adopts.

Good Faith, Transparency and Purpose Limitation (Paras. 2 and 3)

Recognisability of collection and purpose

Para. 3 requires a specific purpose that the data subject can recognise. According to the Dispatch, both the collection and the purpose of processing must be recognisable, and vague, undefined or imprecise purposes do not suffice **BBi 2017 6941**. The transparency principle is closely linked to good faith (para. 2): according to the Federal Supreme Court, in order to enforce data protection, data subjects must first know whether data about them are being processed **BGE 148 II 349**. The duty to inform under Art. 19 FADP gives concrete form to this and requires at least information on the identity of the controller, the purpose and the recipients **Art. 19 FADP**. Where collection and purpose are obviously recognisable from the specific circumstances, no additional information is necessary according to the materials of the 2006 revision **BBi 2003 2101**.

Case law sets concrete requirements for recognisability:

- Timing. "Eine nachträgliche Information genügt den Anforderungen an die Transparenz nicht." (Subsequent information does not satisfy the requirements of transparency.) **a-3891-2025** Nor does it suffice that data subjects contact the processor themselves after a publication **a-3891-2025**.
- Specificity. A mere link to a website did not make the publication of status data recognisable **a-2941-2024**. In *Google Street View*, the visibility of the camera vehicles did not suffice: "Ob ein vorbeifahrendes Google-Fahrzeug gerade Aufnahmen tätigt, ist für die Anwesenden nicht erkennbar." (Whether a passing Google vehicle is currently taking pictures is not recognisable to those present.) **BGE 138 II 346** Internet information one week in advance about the areas to be filmed did not sufficiently ensure recognisability **BGE 138 II 346**.
- Covert recordings. Dashcam recordings are not readily recognisable to other road users: "Die Datenbearbeitung ist damit als heimlich im Sinne von Art. 4 Abs. 4 DSG zu qualifizieren." (The data processing is therefore to be qualified as covert within the meaning of Art. 4(4) FADP.) **BGE 146 IV 226** (referring to the former FADP). Notices on the vehicle do not change this, because drivers cannot be expected to look out for such notices **BGE 146 IV 226**.

Limits. Transparency may also be established by statute. In tax administrative assistance, the duty of prior information did not apply to data transmissions because the special statutory provisions make sufficiently clear to third parties not directly concerned that data may be collected and transmitted **BGE 148 II 349**. The new law provides corresponding exceptions to the duty to inform, for example where processing is provided for by law or where the information would defeat the purpose of the processing **Art. 20 FADP**. In an employment relationship, transparency was established through usage regulations

and repeated warning notices when blocking impermissible websites; an anonymous, statistical analysis of internet log data was permissible under those conditions **a-6453-2014**.

Foreseeability of subsequent use (cantonal parallel). That recognisability may follow from the factual context even without express information is illustrated by a judgment of the *Vaud Cour de droit administratif et public* under the cantonal data protection act (LPrD), which does not apply Art. 6 FADP. A municipality requested from the cantonal energy authority the list of buildings in its territory that had received energy subsidies from 2022 to 2024, in order to check compliance with building and fire safety permits. The Court examined recognisability in the individual case and found it given, because the subsidy is applied for in respect of works on the building "pour lesquels le requérant ne peut pas ignorer qu'une autorisation communale pourrait être nécessaire" (for which the applicant cannot be unaware that a municipal permit might be required) **ge-2026-0008**. It also considered the municipality's control purpose to be compatible with the original purpose of collection, so that the disclosure violated neither purpose limitation nor transparency **ge-2026-0008**. The Court drew the line at proportionality: a "recherche généralisée et indéterminée de moyens de preuve" (a general and indeterminate search for evidence) would be impermissible, which was not the case here given the temporal, territorial and subject-matter limits of the request **ge-2026-0008**. Whether and how the data subjects must be informed subsequently and whether they have a right to object, the Court did not decide itself but remitted to the cantonal data protection authority **ge-2026-0008**. As a parallel assessment, the decision supports the idea that a subsequent use foreseeable for the data subject may be recognisable, but it does not answer the question of the duty to inform.

Compatibility of further processing

Further processing must be compatible with the purpose of collection. According to the Dispatch, it is impermissible if the data subject "berechtigterweise als unerwartet, unangebracht oder beanstandbar erachten kann" (may legitimately regard it as unexpected, inappropriate or objectionable) **BBi 2017 6941**. Incompatible on this basis is, for example, the advertising use of addresses recorded while collecting signatures for a political campaign; compatible, by contrast, is a company's advertising to an address given for a customer card or an order **BBi 2017 6941**. A change of purpose may also be covered by statute or another ground of justification such as consent **BBi 2017 6941**.

Publicly accessible data are not a free pass. Art. 30(3) FADP excludes a violation of personality only as a rule where the data subject has made the data generally accessible and has not expressly prohibited processing **Art. 30 FADP**. The Federal Administrative Court held that this covered contacting the data subjects, but not further processing in a new context, namely the public display of their status as "recorded" or "contacted" **a-2941-2024**. As a counter-example, the unaltered and temporally unlimited redistribution of commercial register data by a private provider remained within the statutory purpose of the commercial register **2008-16**. The decisive question is therefore whether the new context of use is still carried by the originally recognisable purpose.

Proportionality (Para. 2)

According to the Dispatch, only data that are suitable and necessary for the purpose may be processed; the rights of data subjects must be preserved as far as possible, and data avoidance and data minimisation are expressions of this principle **BBi 2017 6941**. Art. 7 FADP implements this organisationally: processing must be designed from the planning stage so that, in particular, the principles of Art. 6 are complied with, and default settings must limit processing to the minimum necessary for the purpose **Art. 7 FADP**.

The analysis follows the three-step test of suitability, necessity (choice

of the least intrusive of several suitable means) and proportionality in the narrower sense **BGE 130 II 425**. In practice, necessity is usually decisive:

- Publishing alleged debtors on the internet was not the least intrusive means of achieving the purpose, because debt enforcement law and criminal prosecution were available **a-3891-2025**.
- In the religious database case, the public display of the status was "nicht aussagekräftig" (not meaningful) for achieving the objective **a-2941-2024**.
- For application forms for rental apartments, the Federal Data Protection Commission examined each individual item: the name of the previous management and the current rent were not necessary for the decision to conclude the lease and collecting them was disproportionate, whereas there was an overriding interest in information on the residence permit and on debt enforcement within the statutory limits **150006365**.

Proportionality is often achieved through conditions rather than a prohibition. In *Street View*, the Federal Supreme Court accepted an error rate of about 1 % in automatic anonymisation, but required complete anonymisation in front of sensitive facilities such as women's shelters, retirement homes, prisons, schools, courts and hospitals, and prohibited the publication of private areas filmed from a camera height of more than 2 m that remain closed to an ordinary passer-by **BGE 138 II 346**.

Monitoring and Video Surveillance under Paras. 2 and 3

Monitoring in the employment relationship

In the employment relationship, the employer may process data only insofar as they concern the employee's suitability for the job or are necessary for performing the employment contract; otherwise the FADP applies **Art. 328b OR**. In addition, there is a prohibition of monitoring systems intended to monitor employees' behaviour at the workplace **Art. 26 ArGV 3**. The Federal Supreme Court interprets this prohibition restrictively: prohibited are systems that exclusively or mainly monitor behaviour as such; systems used for legitimate reasons such as safety or work organisation are permissible, provided they are proportionate and the employees have been informed in advance **BGE 130 II 425**. A GPS system in company vehicles was accordingly permissible because the monitoring was only indirect (via the vehicles), limited to movements and not permanent; continuous real-time tracking, by contrast, could have been disproportionate **BGE 130 II 425**.

The counter-examples show the limits. The covert installation of spyware that recorded an employee's entire computer activity for more than three months was disproportionate, because a summary analysis of existing log files and a warning would have sufficed **BGE 139 II 7**. A Zurich labour court held GPS monitoring of a company car also usable for private purposes to be impermissible, although the employee had been informed of the GPS, because the device recorded all movements without distinguishing between business and private use and the employer had taken no protective measures **AH180153-L**. Informing employees about the system thus does not cure disproportionality.

Video surveillance by private persons

Private video surveillance of identifiable persons is subject to the FADP and must respect good faith, proportionality and recognisability **6B_768/2022**. The Federal Supreme Court requires that persons be informed before they enter the camera's field of view and holds: «Un système de vidéosurveillance privé qui filme l'espace public sera généralement jugé disproportionné et, donc, illicite.» (A private video surveillance system that films public space will generally be held disproportionate and therefore unlawful.) **6B_768/2022** Because the lower court had investigated neither the visibility of the camera and

the notice before entering the recorded area nor less intrusive measures, the Federal Supreme Court remitted the case **6B_768/2022**.

The Geneva Criminal Appeals Chamber refers to the FDPIC's practice whereby, for reasons of practicability, private persons may also capture a small part of public space if the private property cannot otherwise be protected; it too remitted for lack of fact-finding on purpose and recognisability **ACPR/685/2023**. The Vaud Cantonal Court, by contrast, held unlawful a camera that captured the shared forecourt of a housing development and the privacy screen of the neighbour's garden; the short storage period of 24 hours did not change this, and less intrusive means such as shutters or an alarm system had not been shown to be unsuitable **CACI pp20-043408-542/2022**. These decisions were rendered under the former FADP.

Storage Limitation and Anonymisation (Para. 4)

Personal data must be destroyed or anonymised as soon as they are no longer required for the purpose of processing **Art. 6 FADP**. According to the Dispatch, compliance with this duty requires "dass der Verantwortliche Aufbewahrungsfristen festlegt" (that the controller sets retention periods) **BBI 2017 6941**. According to the wording ("as soon as"), the duty must be fulfilled by the controller on its own initiative and does not presuppose a request by the data subject **Art. 6 FADP**.

Statutory retention obligations. Retention periods under special legislation are reserved **BBI 2017 6941**. Thus, business accounts and accounting vouchers must be kept for ten years **Art. 958f OR**, and logs under Art. 4 of the Data Protection Ordinance (DPO) must be kept for at least one year and may be used only to verify data protection and data security **Art. 4 DPO**. Such obligations define the purpose of further retention and at the same time limit the permissible use of the data.

Standard of necessity. Case law assesses necessity functionally. According to the Federal Supreme Court, the decisive question for police data is whether they "in nachvollziehbarer Weise noch nützlich sein können und die weitere Aufbewahrung im öffentlichen Interesse ist" (can still be useful in a comprehensible manner and further retention is in the public interest); discontinuation of criminal proceedings therefore does not compel immediate deletion where the entry clearly shows the discontinuation and automatic deletion is foreseeable **1C_439/2011**. The European Court of Human Rights, by contrast, held that retaining for years the unsubstantiated designation "prostituée" in a Geneva police file was not necessary in a democratic society, because the suspicion was vague and not supported by concrete facts **16188/07**. For cantonal police data, the Administrative Courts of Zurich (ten-year deletion period in domestic violence protection proceedings) and Bern (five-year retention of a journal entry) confirmed retention under cantonal law as proportionate **VB.2024.00039 100 2023 166**. For federal bodies, para. 4 applies directly, as the RIPOL case shows (above) **a-7720-2025**.

Requirements for anonymisation. According to the Federal Supreme Court, anonymisation is any measure that ensures that the identity of the data subject can no longer be determined, or only with extraordinary effort **1C_425/2020**. Data containing an AHV (social security) number that could be linked via an address directory were therefore not anonymised **1C_425/2020**. Pseudonymisation suffices only if it is not reversible; whoever relies on the effectiveness of pseudonymisation bears the burden of proof **4A_365/2017**. According to the Dispatch, only data that cannot be re-identified, or only with an effort that no interested party would undertake, fall outside the scope of the Act; this also applies to pseudonymised data **BBI 2017 6941**. Where the data are still needed in personal form, anonymisation is not a suitable less intrusive means **100 2023 166**.

Accuracy (Para. 5)

Duty to verify and appropriate measures

Any person who processes personal data must satisfy themselves that the data are accurate and take all appropriate measures to correct, delete or destroy incorrect or incomplete data; appropriateness depends in particular on the form and extent of processing and on the risk to personality or fundamental rights

Art. 6 FADP. Compared with Art. 5 of the former FADP, deletion and this risk-based standard are now expressly mentioned **BBI 2006 3547**. According to the Dispatch, the extent of the duty to verify must be determined in the individual case, and data that cannot be corrected or completed must be deleted or destroyed **BBI 2017 6941**.

How far the duty can extend is shown by the Moneyhouse decision: the Federal Administrative Court required the operator of a business information platform to check the accuracy of its data stock in a ratio of 5 % of the queries made **a-4232-2015**. For mass processing with high risk, para. 5 thus requires systematic sample checks. Data are incorrect if they do not correspond to reality, are outdated or incomplete; an entry that correctly reflects the state of knowledge at the time of recording is not incorrect according to the Zurich Administrative Court **VB.2024.00039**.

Limits. According to the Dispatch, statutory obligations may stand in the way of correction, deletion or updating, and the principle must be viewed in a differentiated way for archives, museums and other memory institutions **BBI 2017 6941**. The right to rectification under Art. 32(1) FADP is excluded where a statutory provision prohibits the change or the data are processed for archiving purposes in the public interest **Art. 32 FADP**. According to the Aargau Administrative Court, the files of concluded judicial proceedings can be changed only under procedural law; party allegations in written submissions are not subject to a data protection right to rectification **WBE.2022.152**.

Burden of proof, rectification and dispute notice

For federal bodies, the Federal Administrative Court has allocated the burden of proof: the applicant must prove the accuracy of the requested change, and the federal authority, if contested, the accuracy of the data it processes **d-3102-2025 a-5104-2024**. If neither party succeeds, the more probable data must be entered or retained and marked with a dispute notice under Art. 41(4) FADP **d-3102-2025 Art. 41 FADP**. The two ZEMIS/SYMIC decisions on dates of birth show the range: in one case, the date claimed by the applicant appeared at least not less probable, so that the State Secretariat for Migration (SEM) was ordered to enter it **d-3102-2025**; in the other, the requested date remained unproven, the entry was retained but marked with a dispute notice **a-5104-2024**. For holdings of memory institutions, rectification and a dispute notice are excluded **Art. 41 FADP**.

Against private persons, the claimant may request a dispute notice if neither accuracy nor inaccuracy can be established **Art. 32 FADP**. The Geneva Court of Justice held in a banking case that the processor must prove that it took the necessary measures to ensure accuracy, while the applicant must prove inaccuracy; because the entry as beneficial owner was correct and there was no reasonable doubt, rectification and a dispute notice were refused **ACJC/805/2025**. A dispute notice therefore presupposes a genuine evidentiary impasse.

Consent (Paras. 6 and 7)

Function: a validity rule, not a general consent requirement

Para. 6 presupposes that consent is "required" and governs only its validity **Art. 6 FADP**. The FADP does not make consent a general precondition for every processing. For private persons, it is one of several grounds justifying a violation of personality **Art. 31 FADP**; for federal bodies, it replaces the legal basis only exceptionally in the individual case **Art. 34 FADP**. Consent becomes required where

without it there would be an unlawful violation of personality, or where a special statute requires it, as the KVG did in the Helsana+ case **a-3548-2018**. According to the Dispatch, consent must cover the purpose for which it serves as a ground of justification; processing for further purposes requires another justification **BBI 2017 6941**.

Specificity and appropriate information

Consent must relate to one or more specific instances of processing. The Federal Administrative Court infers from this: "Eine globale Einwilligung in Bezug auf unbestimmte Bearbeitungen oder Bearbeitungen für beliebige Zwecke ist damit ungültig." (A global consent relating to unspecified processing or processing for any purposes is therefore invalid.) **a-2941-2024** As to information, it suffices that the data subject "im Klaren darüber sein kann, worin sie einwilligen soll, d.h. was die Tragweite ihrer Entscheidung ist" (can be clear about what she is to consent to, i.e. what the scope of her decision is) **a-3908-2008**. According to the materials of the 2006 revision, this also includes information on possible negative consequences of refusal **BBI 2003 2101**. The requirements increase for sensitive data: for biometric data, the information would have to be comprehensive; an information sheet that had not been properly handed over did not suffice **a-3908-2008**.

General terms and conditions do not exclude valid consent. The Federal Supreme Court held a user's consent to data processing by Instagram through terms of use and a privacy policy to be valid because it was based "auf hinreichend zur Kenntnis gebrachten und für ihn genügend erkennbaren Angaben" (on information sufficiently brought to his attention and sufficiently recognisable to him) **6B_219/2022**. Conversely, the Vaud Cantonal Court held a general power of attorney in social assistance invalid because the data subject could not sufficiently assess the circle of persons and bodies authorised to provide information **ps-2008-0073**. Both decisions were rendered under the former law.

Voluntariness, coupling and dependency

Consent is voluntary only if the data subject has "eine - mit nicht unzumutbaren Nachteilen behaftete - Handlungsalternative" (an alternative course of action not burdened with unreasonable disadvantages) **a-3908-2008**. If an alternative is offered only after refusal, voluntariness is lacking **a-3908-2008**.

Coupling a service to consent is not impermissible per se. In the Helsana+ case, consent was voluntary because the disadvantage of refusal, namely being unable to participate in the bonus programme, was directly related to the data whose processing was consented to **a-3548-2018**. The decisive factor is thus the substantive connection between the service withheld and the data processing.

In relationships of dependency, voluntariness is regularly denied. Apprentices who knew that refusing a drug test would be treated as a breach of contract did not give truly voluntary consent; the Federal Data Protection Commission left open whether this would be assessed differently before the apprenticeship began, but excluded it for tests during the apprenticeship **150006614**. Apartment seekers are de facto restricted in their freedom to refuse the collection of certain data, so that filling in an application form does not constitute valid consent **150006365**. The threat of a 25 % reduction of social assistance until a power of attorney was signed likewise excluded free consent **ps-2008-0073**. In the employment relationship, the Geneva Court of Appeal for labour matters required unambiguous consent of the employee before the employer contacted the future employer; a mere reference in a witness statement did not suffice **CAPH/19/2023**. In such constellations, processing should therefore be based on another ground of justification, such as Art. 328b of the Code of Obligations (CO).

Form: tacit, explicit and special statutory consent

Outside para. 7, consent is not subject to any form. According to the

Dispatch, it may also be given tacitly, but "blosses Schweigen oder Untätigkeit" (mere silence or inactivity) does not constitute valid consent to a violation of personality **BBI 2017 6941**. The Federal Council's draft additionally required "unambiguous" (eindeutig) consent; the National Council deleted this word by adopting the majority proposal under which consent must be "nach angemessener Information freiwillig erteilt" (given voluntarily based on appropriate information), without the debate recording any specific reason for the deletion **AB 2019 N 1775**. The passages of the Dispatch on "unambiguousness" are therefore of only limited use; the deletion does not change the exclusion of mere silence, given the statutory wording requiring consent to be "given" **BBI 2020 7639**.

Explicitness under para. 7. Explicit consent is required for sensitive personal data (let. a), for high-risk profiling by a private person (let. b) and for any profiling by a federal body (let. c) **Art. 6 FADP**. Where explicit consent is required, it cannot be given tacitly **BBI 2017 6941**. A separate form is not necessary, however: the Federal Administrative Court accepted explicit consent given by signing a contractual clause **b-5181-2018**. On explicit consent through cookie banners, see below under cookies and similar technologies.

Special statutory formal requirements go further. In the *Helsana+* case, the KVG required written consent in the individual case for the disclosure of data from basic insurance; clicking a button in the app did not suffice for lack of a handwritten signature **a-3548-2018**.

High-risk profiling (para. 7 lets. b and c)

Profiling is any automated processing used to evaluate personal aspects of a natural person (Art. 5 let. f FADP); high-risk profiling exists where it leads to a combination of data "die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt" (that allows an assessment of essential aspects of the personality of a natural person) (Art. 5 let. g FADP) **Art. 5 FADP BBI 2020 7639**. The rule is a compromise: the Federal Council's draft required explicit consent for profiling generally **BBI 2017 6941**; the National Council wanted it in no case; the Council of States imposed a risk-based approach **AB 2019 S 1240**. The conciliation conference adopted this solution after the Federal Council, the administration and the FDPIC had given assurances that it would not tighten the law compared with the previous legal situation and the application of the Moneyhouse case law **AB 2020 N 1817**. The committee rapporteur stated that "bei der Bemessung" (in the assessment) one should not go beyond the Moneyhouse judgment **AB 2020 N 1817**.

The Moneyhouse decision thus becomes the interpretive anchor for let. b. There, under the former concept of the personality profile, the Federal Administrative Court held that the systematic combination of identification data with information on private living and housing circumstances, partly with former places of residence and professional data, resulted in a personality profile for which the necessary explicit consent had not been shown **a-4232-2015**. For federal bodies, explicitness applies to any profiling (let. c), which corresponds to the requirement of a basis in a formal statute for profiling under Art. 34(2)(b) FADP **Art. 34 FADP**. High-risk profiling moreover excludes the justification for creditworthiness checks under Art. 31(2)(c) FADP **Art. 31 FADP**.

Withdrawal

Consent is not final. An opinion under the former law already held: «Il peut être retiré en tout temps.» (It may be withdrawn at any time.) **150001781** Consent may be restricted from the outset or subsequently; in the case of withdrawal at an inopportune time, for example shortly before a broadcast, damages remain reserved **150001781**. After withdrawal, further processing is no longer covered by the consent **150001781** and may moreover contravene an express declaration of intent within the meaning of Art. 30(2)(b) FADP **Art. 30 FADP**. Special statutes may require that the data subject be informed of the possibility of withdrawal; in employment placement law, the Federal Administrative Court ordered a corresponding

supplement to a contractual clause **b-5181-2018**.

Capacity to consent

Consent presupposes capacity of judgement. For consent to medical treatment, the Federal Supreme Court held that minors with capacity of judgement exercise strictly personal rights themselves and are represented by their parents only if they lack capacity of judgement: «Le mineur ne sera donc représenté par ses parents que s'il est incapable de discernement» (The minor will therefore be represented by his parents only if he lacks capacity of judgement) **BGE 134 II 235**. This judgment does not decide whether data protection consent is always a strictly personal right in this sense; it does, however, support obtaining the minor's own consent where the minor has capacity of judgement, at least where the processing substantially affects their personality.

Cookies and similar technologies

For cookies, Art. 45c of the Telecommunications Act (TCA) applies alongside the FADP: processing data on third-party devices is permissible outside telecommunications services only if users are informed about the processing and its purpose and are told that they may refuse it **Art. 45c TCA**. According to the FDPIC's guidelines, this provision does not replace the requirements of the FADP; for non-essential cookies with high intrusiveness, in particular for sensitive data or high-risk profiling, explicit consent must be obtained before processing

EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies

. For such explicit consent, the FDPIC requires buttons or boxes that call for active clicking

EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies

. The FDPIC does not regard a dialogue box offering only the choice between accepting all cookies and leaving the website as a valid declaration of intent

EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies

. These statements reflect the supervisory authority's practice and do not bind the courts.

Legal Consequences and Enforcement

Civil claims

Against private persons, actions are governed by Arts. 28 et seq. of the Civil Code; the claimant may in particular request a prohibition of processing or disclosure and the deletion or destruction of the data, as well as rectification of incorrect data and notification or publication of the judgment to third parties **Art. 32 FADP**. Against federal bodies, the claimant may request that unlawful processing be refrained from, its consequences be remedied or its unlawfulness be established; instead of deletion, processing must be restricted in certain cases, and the procedure is governed by the Administrative Procedure Act **Art. 41 FADP**.

Supervisory measures and criminal law

The FDPIC opens an investigation ex officio or upon report if there are sufficient indications of a breach; it may refrain from doing so in cases of minor importance **Art. 49 FADP**. If it finds a breach, it may order processing to be adapted, suspended or terminated and the data to be deleted or destroyed; if the processor has restored lawful conditions during the investigation, it may limit itself to a warning **Art. 51 FADP**. In both internet publication cases, the Federal Administrative Court upheld corresponding orders **a-3891-2025 a-2941-2024**.

A breach of Art. 6 FADP is not punishable as such. The criminal provisions cover only certain breaches of duty, in particular intentional breaches of the duties to inform, to provide access and to cooperate, of certain duties of diligence and of professional confidentiality **Art. 60 FADP Art. 61 FADP Art. 62 FADP**. Indirectly, however,

non-transparent processing may become punishable where the duty to inform under Art. 19 FADP is at the same time intentionally breached **Art. 60 FADP**.

Admissibility of evidence obtained in breach of the principles

Data collected in breach of Art. 6 FADP have been obtained unlawfully. In civil proceedings, they are taken into account only if the interest in establishing the truth prevails **Art. 152 CPC**. The Federal Supreme Court requires restrictive application and upheld the exclusion of a transcript of a secret audio recording because, in a purely financial private dispute, the financial interests did not outweigh the protection of privacy; it reviews the lower court's balancing only with restraint **4A_133/2024**. In criminal proceedings, the Federal Supreme Court admits evidence unlawfully obtained by private persons only if the authorities could have obtained it lawfully and a balancing of interests favours its use **6B_768/2022**; dashcam recordings of traffic offences that are not serious crimes therefore remained inadmissible **BGE 146 IV 226**. Substantive grounds of justification under data protection law do not change the unlawfulness under criminal procedure, because admissibility is governed primarily by the State's interest in prosecution and the right to a fair trial **BGE 146 IV 226**.

In employment law, inadmissibility had substantive consequences: covert spyware monitoring remained inadmissible, so that the summary dismissal lacked a basis **BGE 139 II 7**, and GPS data from a company car also usable privately could not be used as the basis for a salary deduction **AH180153-L**. That the balancing may also favour admissibility is shown by a decision of the Federal Administrative Court: a personalised analysis of internet log data was procedurally irregular because the employee had not been informed in writing in advance of the specific suspicion, but remained admissible because the interference was limited to log data and the employer had drawn attention to the prohibition through regulations and warning notices **a-6453-2014**.

Practical Notes

- Define and communicate the purpose before collection. Subsequent information does not cure a lack of recognisability **a-3891-2025**; notices must be specific and perceptible before data are captured, and for cameras before the recorded area is entered **6B_768/2022**.
- Document less intrusive means. Courts regularly examine whether log files, technical blocks, shutters or remedies under debt enforcement law would have sufficed **BGE 139 II 7 a-3891-2025 CACI pp20-043408-542/2022**.
- Set retention periods and align them with statutory retention obligations **BBI 2017 6941 Art. 958f OR**.
- Check accuracy in proportion to risk and record the measures taken in a provable form, since the processor must prove them **ACJC/805/2025 a-4232-2015**.
- Draft consent narrowly and specifically, offer alternatives without unreasonable disadvantages, consider another ground of justification in relationships of dependency and obtain an active declaration for para. 7 **a-2941-2024 a-3908-2008 150006614**.
- Factor in evidentiary risk. Data collected in breach of the principles may be inadmissible in proceedings and thereby deprive dismissals or claims of their basis **BGE 139 II 7 4A_133/2024**.