DeepL

Subscribe to DeepL Pro to translate larger documents.
Visit www.DeepL.com/pro for more information.

Aa Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner FDPIC

Data protection

FDPIC guidelines on data processing using cookies and similar technologies

22. January 2025

Contents

1 Terminology 3
1.1 Cookies and similar technologies 3
1.2 Person tracking and profiling 4
2 Legal sources 4
2.1 Requirements of the Telecommunications Act 4
2.2 Requirements of the DSG 5
3 Data protection requirements for the use of cookies 5
3.1 Relation of data processing to natural persons 5
3.1.1 Personal reference in general 5
3.1.2 Personal reference through the use of cookies 6
3.2 Responsibility 7
3.2.1 Order data processing 7
3.2.2 Data procurement by third parties 7
3.3 General information obligations 8
3.3.1 Content and form of the information 8
3.3.2 Time of information 9
3.4 Further information obligations 9
3.5 Application of the processing principles of the FADP to the use of cookies 9
3.5.1 Principle of good faith and transparency 10
3.5.2 Principle of proportionality 10
3.6 Permissibility of non-essential cookies 11
3.7 Justification of privacy-infringing cookie use, by overriding reasons private interests 12
3.7.1 Weighing up the use of non-essential cookies against the severity of the violation of privacy 12
3.7.2 Optional design reduces the severity of the intervention 12
3.8 Legal factual constellations a possible predominance of private that indicate interests 12
3.8.1 Use of cookies in direct connection with the conclusion or execution of a contract 13
3.8.2 Use of cookies for research and statistics 13
3.9 Granting the right to object and data protection default settings 13
3.10 Qualified use of cookies 14
3.10.1 Highly intrusive terms of personality and fundamental rightsuse of cookies in 14
3.10.2 Unexpected use of cookies 14
3.10.3 Special labeling and highlighting obligations 15
3.10.4 Structure of the statutory right to object and opt-out 15
3.10.5 Design of consent and opt-in 15
3.11 Use of cookies for personalized advertising 16
3.11.1 Usage of advertising cookies in a commercial processing context 16
3.11.2 Advertising tracking by means of "normal" profiling 16
3.11.3 High-risk advertising tracking by means of profiling 16
3.12 Legal requirements for obtaining consent and the granting of the right of Rights of revocation and objection 17

3.12.1 Application of the provisions on the right to object to cookies ..17
3.12.2 Informed consent 17

3.12.3 Specific consent 18
3.12.4 Voluntary consent 18
3.12.5 Form and structure of consent 19
3.12.6 Express consent 19
3.12.7 Revocation of consent 19
3.12.8 Consequences of legal deficiencies in the granting of the rights to consent and objection 19
3.13 Technical implementation 20
3.13.1 Implementation of timeliness 20
3.13.2 Consent banner 20

In this guide, the Federal Data Protection and Information Commissioner (FDPIC) describes the data protection requirements for the use of cookies and similar technologies by private controllers, with specific references to the special provisions applicable to federal bodies. The Commissioner derives these requirements from the Federal Data Protection Act (FADP SR 235.1), the Data Protection Ordinance (DPO SR 235.11), special statutory data protection provisions under federal law as well as federal court rulings, relevant doctrine and his supervisory practice to date.

1 Terminology

1.1 Cookies and similar technologies

Cookies are small text files that the operators of websites and third parties authorized by them store on the computers of website visitors in order to make user data available for further processing to fulfill specific functionalities, e.g. of online stores.

Based on the criterion of storage duration, the use of cookies can be differentiated as follows:
"Session" cookies are stored in the browser for a limited period of time and are automatically deleted when the browser is closed. Permanent cookies are stored in the browser for a longer period of time, for example to enable the website visitor to be recognized.

Cookies can also fulfill different functions. For example, a cookie can save the language setting, a login or, after a webshop visit, the selected products in the shopping cart. Cookies are also used for so-called "stateful tracking": Here, an "identifier" is stored locally in the client browser and retrieved by the provider at a later time, so that the end device can be recognized on a subsequent visit and thus information about the user behaviour of website visitors can be collected. In this way, it is possible to analyse the data traffic on a website and to personalize the content and advertising on a website.

A distinction can also be made between cookies that are set by a website provider itself (so-called "First-party cookies") and those that are not used by the website provider itself but by third parties, such as advertisers (so-called "third-party cookies"). In the first case, data is transferred between the website operator's system and the user's end device. In the second case, data records from third parties are stored in the user's browser when the user accesses the website. In other words, no data is actually transmitted by the website operator to third parties, but third parties obtain data from the data subject themselves at the instigation of the website operator. If a user then accesses content on another domain and the same third party is involved, he or she will be recognized. In many cases, third parties enrich the information obtained through cookies with further information that they have collected directly from users when using their services or which other third parties have made available to them, so that comprehensive user profiles can be created across domain boundaries.

The collection and analysis of data on surfing behavior is commonly referred to as
referred to as "tracking". However, this is not always based on the use of cookies. In the case of so-called "stateless tracking", no information is stored on the user's end device. In simple terms, data is not collected and analyzed via the user's browser, but via the server. Tracking technologies such as "browser fingerprinting", "ID graph", "user ID", "ETags", "pixels" or "authentication cache" are subsumed under the term "similar technologies" in these guidelines. Data processing in connection with the integration of third-party services such as "Like- and Share-

buttons" of online social platforms are referred to as "similar technologies" in this guide.

1.2 Person tracking and profiling

Personal tracking refers to the recording and evaluation of people's surfing behaviour, whereby the data obtained is used, for example, in connection with website analyses for optimization purposes. For example, as a basis for website performance evaluations or in connection with online advertising and marketing campaigns. Tracking can serve as a starting point for displaying personalized advertising offers to end users based on the user profiles created. The more comprehensive the tracking is, the more the advertised content can be tailored to individual people. This is based on the logic that the more data available about users, the better the algorithmic and self-learning computer programs used can predict their preferences. Therefore, the information on surfing behavior is often enriched with additional information from other sources (e.g. social media or other websites visited) or with machine-calculated predictions or information, which can create a user profile ("profiling").[1]

Profiling is to be assumed in accordance with Art. 5 lit. f FADP if the purpose of personal tracking is to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects relating to the work performance, economic situation, health, personal preferences, interests, reliability, location or relocation of that natural person.

If personal tracking leads to profiling with a high risk to the personality or fundamental rights of the data subject within the meaning of Art. 5 lit. g. FADP, in that it leads to a linking of data that an assessment of essential aspects of the personality of a natural person, the data controllers are required to examine the introduction of special protective measures, such as the preparation of a data protection impact assessment in accordance with Art. 22 FADP (see section 3.10.1).

2 Legal sources

2.1 Requirements of the Telecommunications Act

With regard to the use of cookies in apps and websites, it should be noted that the Telecommunications Act (TCA; SR 780.10) contains a special regulation regarding their storage on end devices such as smartphones or personal computers in Art. 45c, which has been in force since April 1, 2007.

This provision in the TCA relates to the technical processes for setting, reading and storing cookies. As these processes compromise the integrity of end devices by exchanging data with other computers unnoticed, the provision of Art. 45c TCA aims to protect the privacy and informational self-determination of the users of such end devices. In other words, Art. 45c TCA represents a special statutory, public-law norm for otherwise unnoticed "telecommunication" processes[2] which, as a norm of special federal data protection law, must be complied with cumulatively with the general data protection law in the FADP.[3]

Art. 45c lit. b TCA ensures that any data processing on third-party devices either serves the purpose of telecommunications transmission or, if this is not the case, can be controlled by the users of the devices.[4] According to Art. 45c TCA, website operators are obliged to inform website visitors about the use of corresponding technologies and to state the respective purposes. This must also indicated,

[1] Müller-Peltzer Philipp/Guttmann Philipp, "State of the art" web tracking - current developments, regulatory and judicial positions, DSB 2023 p. 233.

[2] Message on the amendment of the Telecommunications Act of November 12, 2003, BBl 2003 7951, p. 7987.

[3] See also FAC judgment A-3548/2018 of March 19, 2019, E. 5.4.

[4] Message on the amendment of the Telecommunications Act of November 12, 2003, BBl 2003 7951, p. 7987.

that and how the data subjects can object to the processing in question. How and in what form the data subjects should be informed is left open by the provision and must be specified in accordance with the FADP (see sections 3.7.1, 3.10.4 and 3.11.1 to 3.12.8).

2.2 Requirements of the DSG

The FADP regulates all aspects of personal data processing that is carried out using cookies and similar technologies. The provisions of the FADP, including their regulatory relationship to the special provision of Art. 45c TCA[5], are the subject of this guide.

3 Data protection requirements for the use of cookies

3.1 Relation of data processing to natural persons

3.1.1 Personal reference in general

Personal data is any information relating to an identified or identifiable natural person (Art. 5 lit. a FADP). A natural person is identified or at least identifiable if their identity can be inferred directly from the data itself or if their identity can be from the context of the data or by combining it with other data.[6] The way in which the reference to the data subject, i.e. the identification, is established, such as by means of a key, an AHV number, a file number or even a customer number, is generally irrelevant.[7]

According to Federal Supreme Court case law ("Logistep ruling "[8]), a person is "identified" if it is clear from the information itself that it is precisely this person. A person is "identifiable" if it can be inferred on the basis of additional information, whereby not every theoretical possibility of identification is sufficient. If the effort involved is so great that, according to general life experience, cannot be expected that an interested party will undertake it, there is no identifiability.[9] The question of whether identifiability exists must therefore be answered depending on the specific case taking into account in particular the possibilities of technology. However, it is not only important what effort is objectively required to be able to assign a certain piece of information to a person, but also what interest the data processor or a third party has in the identification.[10] This interest can change over time, as can the means to the data processor or a third party for identification. In other words, a person may be identifiable to certain people or entities based on their (additional) knowledge or ability to access further information, while this may not be the case for others who do not have this (additional) knowledge or ability[11]. In the case of the transfer of information between a data processor A, who cannot assign the data to a person with reasonable effort, and a data recipient B, who is able to identify the person with additional information, the FADP applies. This applies to both data recipient B and data processor A. To decide otherwise, according to the Federal Supreme Court, "would mean applying the Data Protection Act only to the individual recipients, but not to the person who obtains the data in question and disseminates it. This would run counter to the purpose of the law. "[12].

---

[5] See also FAC judgment A-3548/2018 of March 19, 2019, E. 5.4.

[6] Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7019.

[7] GABOR-PAUL BLECHTA, in: BLECHTA/VASELLA (ed.), Basler Kommentar, Datenschutzgesetz / Öffentlichkeitsgesetz, Art. 3 DSG N. 10.

[8] BGE 136 II 508 E. 3.2 et seq.

[9] Message on the Federal Act on Data Protection of March 23, 1988, BBl 1988 II 413, p. 444 f. and Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Legislation of September 15, 2017, BBl 2017 6941, p. 7019.

[10] BGE 136 II 508 E. 3.2 et seq.

[11] See BGE 136 II 508, E. 3.4; BEAT RUDIN, in: BAERISWYL/PÄRLI/BLONSKI (eds.), Stämpflis Handkommentar zum DSG, 2nd edition, Art. 5 N 11 f.

[12] BGE 136 II 508 E. 3.4.

However, a person can no longer be identified if personal data has been anonymized. Anonymized means that the personal reference is irreversibly removed in such a way that it is no longer possible to draw conclusions about individuals without disproportionate effort.

3.1.2 Personal reference through the use of cookies

Whether and to what extent the use of cookies or similar technologies results in a personal reference when processing data, or whether such a reference is strengthened, depends on the circumstances of the individual case. In particular, what information cookies transmit and what other data they are combined with. On the one hand, a personal reference may exist if the processed information itself has an identifying characteristic (e.g. the unique user ID for Android or Ad ID for Apple devices)[13]. On the other hand, a personal reference may arise due to the circumstances of the collection and subsequent evaluation of the data by the website operator or third parties, even if no identifying information was available at the time of collection and it was therefore (initially) only factual data.

A personal reference is created at the latest when the website owner or integrated third-party services can associate factual data with specific and identifying information on the basis of a log-in[14] or comparable online identifiers. For example, if the visitor selects a language when accessing a website for the first time. In this case, a cookie is stored on their end device together with the information that they wish to use the website in the selected language. If this information cannot be linked to the website visitor, the data processed using this text file is not considered personal data. If the website operator can link the language setting to a specific visitor, for example because they registered before or after in the website's online store, the data must be considered personal data[15].

If a person's data records are marked for the sole purpose of uniquely identifying them within an information system, without identifying characteristics of a natural person being assigned to them, this is referred to as singularization. Whether and to what extent such processing creates a personal reference is still largely unclear in doctrine[16] and case law[17] .

The FDPIC advises that in cases of doubt, where it is not possible to assess with sufficient certainty whether it is or could be possible to identify individuals with reasonable effort when using cookies, the potential processing of personal data should be assumed. If an identification that is difficult to assess could also be associated with high risks for the data subjects, the FDPIC recommends that the controller check whether the

---

[13] See final report of the FDPIC of April 11, 2024 in the matter of Ricardo AG and TX Group, point 128: https://www.edoeb.admin.ch/de/nsb?id=102867

[14] For the significance of customer accounts, see the FDPIC's final report of April 15, 2024 in the matter of Digitec Galaxus AG, point 85: https://www.edoeb.admin.ch/de/nsb?id=100736

[15] Austrian Data Protection Authority, FAQ Data Protection & Cookies: https://dsb.gv.at/faq/datenschutz-cookies

[16] Critical: David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16 November 2020, the same in digma, issue 4, December 2017; but in favor of the DPA in the matter of Google Analytics https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschwärzt.pdf; partial decision of the Austrian Data Protection Authority, GZ: D155.027 2021-0.586.257, dated 22 December 2021, in the matter of "Google Analytics", D.2. Point 2. a) and b). See also Philip Glass, Identification and Singularization, www.datalaw.ch, para. 9 f. (https://www.datalaw.ch/singularisierung-und-identifizierung/; as of 11 July 2024).

[17] In BGE 136 II 508 in the Logistep case, the Federal Supreme Court expressed in E. 3.6 that its interpretation of the concept of personal data under the FADP appeared to be in line with the legal situation in the European Union at the time by referring to Opinion 4/2007 of June 20, 2007 of the independent EU advisory body on data protection issues (Article 29 Working Party). Cf. p. 16 of the cited Opinion 4/2007*: "At this point, it should be noted that although in practice persons are mainly identified by their name, a name by no means always necessary to identify a person. For example, a can be singularized on the basis of other "characteristics". For example, computerized files for recording personal data usually assign a unique identifier to the persons recorded in order to avoid confusion between two persons in the file. The behavior of a device and thus the device user can also easily identified on the Internet with the help of Internet traffic monitoring tools. This gradually builds up a picture of the person's personality to which certain decisions can be attributed. The person can therefore be categorized and to certain decisions without knowing their name and address, based on socio-economic, psychological, philosophical or other criteria, as the person's point of contact (computer) no longer necessarily requires the disclosure of their identity in the strict sense. In other words, the identifiability of a person no longer requires knowledge of their name. This is reflected in the definition personal data."*

processing and the associated use of cookies should be subject to a data protection impact assessment (see section 3.9.1).

3.2 Responsibility

Pursuant to Art. 5 lit. j FADP, the person responsible under data protection law is the person who alone or jointly with others decides on the purposes and means of processing.

In the context of the website, the website owner is responsible for the use of cookies because he determines which data is processed via his website and for what purpose. As the controller, he must in particular ensure that the processing principles pursuant to Art. 6 and 8 FADP are complied with and that the data subjects are adequately informed about the data processing (see sections 3.3 and 3.5.1).

If a website owner integrates third-party services into his website, a distinction must be made with regard to his responsibility as to whether he uses the third-party services in the sense of commissioned data processing ("outsourcing") in accordance with Art. 9 FADP, or whether third parties use the services embedded on the website to (also) obtain data for their own purposes.

3.2.1 Order data processing

In the case of commissioned data processing ("outsourcing") within the meaning of Art. 9 FADP, the controller transfers the processing of personal data to a third party. The processing of information should be the main purpose or at least a central component of the contractual relationship. A commissioned data processor processes personal data on behalf of the controller and not for its own purposes. There is a contractual relationship between the controller issuing the order and its commissioned data processor.
"Internal relationship", so the transfer of data to a commissioned data processor does not constitute a disclosure of personal data to third parties[18]. The controller therefore does not need a special justification for the transfer of data processing. What is required, however, is a contract or a legal basis and compliance with the other requirements of Art. 9 FADP[19].

3.2.2 Data procurement by third parties

If, for example, social plug-ins from platforms such as Facebook, Twitter or Instagram or videos from platforms such as YouTube are integrated, website operators can use certain functionalities of social networks on their own websites. The integration of third-party products causes the browser of the visitor to the website in question to request content from the provider and to transmit the visitor's personal data to the third-party provider for this purpose. In this constellation of embedded services, third parties process the personal data obtained for their own purposes and therefore in their own interests. According to Art. 19 FADP, the procurement of personal data must be disclosed to the data subjects by both the website operator and the procuring third parties. According to para. 3 of this provision, the latter must also inform the data subjects of the categories of personal data that they obtain about them by setting cookies on a third-party website. This information then allows website visitors to exercise their right under Art. 45c TCA to refuse processing (see section 2.1).

Art. 5 lit. j FADP defines responsibility broadly insofar as the decision on the means used or the purpose of the processing can be made jointly by several controllers. The third party is initially responsible for its data processing, as it influences the processing of personal data out of its own interest and thus participates in the decision on the purposes and means of this processing. The website owner, on the other hand, only enables the third party to obtain data by integrating the third-party service on its website (means), even if it has little or no influence on the downstream data processing. From this

[18] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7023.

[19] Further information on our website: Outsourcing (order data processing)

it follows that joint or shared responsibility must be assumed for the process of obtaining data from the third party (as processing within the meaning of Art. 5 lit. d FADP) via the website[20].

As the website operator has control over which third-party services are integrated, it cannot assume that its responsibility ends where the third parties' terms of use apply. The website operator is responsible for ensuring that the website complies with data protection regulations. They must therefore inform themselves about the data processing of the integrated third-party services and ensure that the requirements of the law are complied with. In particular, the website operator must ensure that all information obligations towards the website visitors concerned are fulfilled.

3.3 General information obligations

3.3.1 Content and form of the information

According to the introductory sentence of Art. 19 para. 2 FADP, the data subject must be provided with all the information necessary to enable them to assert their rights under the FADP and to ensure transparent data processing. Art. 19 para. 2 lit. a - c as well as para. 3 and 4 FADP specify this principle through various minimum details that must be provided to the data subject. These general information obligations naturally also apply to the use of cookies and similar technologies.

The minimum information includes: the identity (i.e. the name or company) and contact details of the controller (Art. 19 para. 2 lit. a FADP), the purpose of the data processing (Art. 19 para. 2 lit. b FADP) and, if applicable, the recipients or categories of recipients to whom the personal data will be disclosed (Art. 19 para. 2 lit. c). When obtaining personal data, the controller must therefore inform the data subject that the data will be disclosed to a processor or a third party and the purpose of the data transfer or disclosure. Finally, if the personal data is disclosed abroad, information must also be provided about the respective state or international body and, if applicable, the guarantees pursuant to Art. 16 para. 2 FADP or the application of an exception pursuant to Art. 17 FADP (Art. 19 para. 4 FADP).[21]

The FADP does not specify how the data subjects must be informed. Art. 19 para. 1 FADP only stipulates that the information must be "appropriate". Adequacy depends on whether a data subject can make a conscious and self-determined decision on the basis of the information received and exercise their rights, such as consenting to personal data processing or the use of cookies or objecting to such processing, in a legally compliant manner (see sections 3.9 and 3.12). The more extensive and surprising the data processing is and the more seriously it encroaches on the personality of the data subject, higher the requirements for the accessibility of the information.[22]

Art. 13 GDPR specifies that the data controller must provide the data subject with information about the collection of personal data in a precise, transparent, comprehensible and easily accessible form. Neither the FADP nor the DPA specify formal requirements for the information. This means that data protection declarations, terms of use, notices or pictograms, for example, are possible. However, the information must be provided actively, which means that the data controller must provide this information and ensure that the data subject can actually take note of the complete information in a reasonable manner.[23] This means that

[20] Cf. judgment of the ECJ of July 29, 2019 C-40/17

[21] Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7051 f.

[22] BRUNO BÄRISWYL, in: BAERISWYL/PÄRLI/BLONSKI (eds.), Stämpflis Handkommentar zum DSG, 2nd ed., Art. 7 N 16 ff.

[23] BRUNO BÄRISWYL, in: BAERISWYL/PÄRLI/BLONSKI (eds.), Stämpflis Handkommentar zum DSG, 2nd ed., Art. 7 N 16 ff., Cf. dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Legislation of September 15, 2017, BBl 2017 6941, p. 7050

It is not possible to place the privacy policy somewhere in a hidden section of the website or that the information is only provided on request.

In order to meet the requirements of Art. 13 GDPR, the information must be provided in written form in a reader-friendly manner and tailored to the needs of the addressees. In the digital reality, a layered approach is essential, whereby the controller must ensure that the data subject always receives the most important information at the first level of communication when obtaining their personal data. For example, a data protection declaration drawn up according to this approach allows data subjects to obtain all essential information in summarized form at a glance, as well as specialists, investigative journalists and supervisory authorities with further information requirements to obtain detailed legal and information technology information by accessing a further level[24] (for the technical implementation of the requirements, see section 3.13). When integrating third-party services or in the case of commissioned data processing, the website operator can refer to further information from the third-party service or commissioned data processor for detailed information.

3.3.2 Time of the information

According to the wording of the law, the data subject must be informed when the personal data is obtained. This means that the controller who obtains personal data directly from the data subject must ensure that the data subjects are adequately informed at the latest at the time when they exercise their right to choose whether or not to obtain personal data or use cookies (see sections 3.12.2 and 3.13.1).

3.4 Further information obligations

With regard to the use of cookies and similar technologies, further information obligations may arise, as can be seen from the following explanations on the qualified forms of the unexpected or highly intrusive use of cookies and on informed consent (see Section 3.10 and Section 3.12.2).

3.5 Application of the processing principles of the FADP to the use of cookies

Art. 6 of the FADP sets out the principles that the controller must also follow when using cookies and similar technologies as soon as they expect the processing to establish a personal reference (see section 3.1). This standard stipulates that personal data may only be processed lawfully (para. 1) and that it must be processed in good faith and in a proportionate manner (para. 2). The collection of personal data and in particular the purpose of its processing must be recognizable to the data subject, and the personal data may only be processed in a way that is compatible with this purpose (para. 3). Controllers must ensure the accuracy of the processed personal data (para. 5). Paragraphs 6 and 7 regulate the conditions for the validity of the data 's consent, which must also apply mutatis mutandis to the right to object (see section 3.12.1). The principle of transparency is substantiated by the duty to provide information when obtaining personal data (Art. 19 FADP). The principles of proportionality and data security are substantiated by the obligation to make data protection-friendly default settings (Art. 7 para. 3 FADP) and the obligation to data minimization (Art. 6 para. 4).

Private individuals may process personal data unless they thereby unlawfully violate the privacy of the data subjects. Since Art. 30 para. 2 lit. a FADP states that a violation of personality rights occurs when private individuals process personal data contrary to the statutory processing principles, the principles set the legal limits for data processing by private individuals. According to Art. 31 para. 1 FADP, if the principles are violated, this constitutes a

[24] Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7050 f.; Federal Office of Justice, Explanatory Report on the Revision of the Ordinance on Data Protection of August 31, 2022, p. 37

unlawful infringement of personality rights, unless it is justified by one of the justification grounds under Art. 31 FADP (consent of the data subject, overriding private or public interest or law).

When processing personal data, federal bodies must observe the principles of the FADP in the same way as private controllers, but are also subject to the principle of legality in accordance with Art. 34 para. 2 FADP, according to which there must be a sufficient legal basis for any processing. As part of the processing of personal data, which is regulated by law and always in the public interest, federal bodies use technically necessary cookies in accordance with the principle of proportionality. Any further use of text files is possible, provided it is also in the public interest and is based on a sufficiently specific legal basis.

3.5.1 Principle of good faith and transparency

The principle of good faith pursuant to Art. 6 para. 2 FADP and the aforementioned information obligations pursuant to Art. 19 FADP ensure the transparency of personal data processing. The latter is an indispensable prerequisite for the data subjects to be able to assert their rights under the FADP and thus, in particular, to exercise their rights of design such as consent to or objection to the personal use of cookies in a legally compliant manner (for the content, form and timeliness of the information obligations under Art. 19 FADP see Section 3.3 and on the qualified forms of cookie use and qualified consent, see Sections 3.9 and Sections 3.12 and 3.13).

3.5.2 Principle of proportionality

In accordance with the principle of proportionality pursuant to Art. 6 para. 2 FADP, only data that is suitable and necessary for the purpose of processing may be processed. In addition, there must be an appropriate relationship between the purpose and the means used.[25] This principle is specified in Art. 7 para. 3 FADP, which obliges the controller to ensure by means of suitable default settings that only as little personal data processed as necessary for the intended purpose, unless the data subject specifies otherwise[26].

Cookies that are limited to the essential functions of the website are referred to as "technically necessary" cookies in the IT sense. In principle, their use is to be regarded as proportionate, because without them a website cannot be used for its actual function - is desired by visitors. An objection to such necessary cookies in application of Art. 45c TCA (see section 2.1) is therefore only possible indirectly, in which case the application as a whole is dispensed with.

Cookies used for information technology security are also considered technically necessary. The following is an exemplary list of cookies that are considered technically necessary and for which the corresponding data processing can therefore generally be regarded as proportionate:

- Shopping cart cookie: The storage of selected products in an online store;
- User input: The temporary storage of data in an online form;
- Login: The authentication of a logged-in user;
- Language selection: Saving the choice of language that suits the website visitor;
- Cookie opt-in and cookie opt-out: It is necessary to save the cookie consent or opt-out so that the "cookie banner" does not appear each time the page is accessed.

[25] Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7024.

[26] Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7030.

- Load distribution ("load balancing"): Cookies that serve to distribute the load of a website evenly;
- Cookies to prevent so-called brute force attacks through repeated login attempts;
- Cookies to distinguish humans from computer bots (Captcha);
- Cookies to prevent the overloading of websites.

The criterion of necessity is to be applied both to the content of the cookies and to their storage duration and any disclosure of data to third parties. In terms of content, it may be necessary for cookies to be set to store consent or for load balancing. They may only be stored with a unique ID if and as long as this is necessary to fulfill the functionality. The same applies to the storage of language or background color settings. This does not require a unique identifier such as a unique user ID, but it is sufficient to store non-identifying information such as
"background-color: black" or "language: de".

3.6 Permissibility of non-essential cookies

In addition to the necessary cookies, cookies are often used that are not required for the secure technical operation of an application, but are used, for example, to optimize the user's experience when surfing the website (so-called functional or convenience cookies). The use of such cookies collides with the principle of proportionality under data protection law in accordance with Art. 6 para. 2 FADP, as it goes beyond what is necessary.

If personal data is processed by a private controller contrary to the general processing principles in accordance with Art. 6 and 8 FADP, this processing violates the privacy of the persons concerned in accordance with Art. 30 para. 2 lit. a. Pursuant to Art. 31 para. 1 FADP, private controllers must refrain from violating personal data unless they can justify this on the basis of an overriding private or public interest, the law or the consent of the data subjects.

Private controllers therefore have the following instruments at their disposal to lawfully use non-essential cookies:

- Firstly, as part of a balancing of interests, they can check whether the data processing carried out using such cookies can be justified by overriding private interests (see section 3.7);

- Secondly, data controllers have the option of obtaining the consent of the data subjects (see section 3.12).

As a further possibility, data controllers can optionally structure data processing that violates personal data by granting a right of objection in accordance with Art. 30 para. 2 lit. d FADP, which is in any case mandatory with regard to the use of non-essential cookies due to the special legal requirement in Art. 45 c TCA (see sections 2.1, 3.7.2 and 3.9).

3.7 Justification of privacy-infringing cookie use by overriding private interests

In practice, advertisers often try to justify the commercial use of cookies beyond the limits of the principle of proportionality by arguing that their private interests prevail, because by providing evidence of such, they can refrain from obtaining consent from the data subjects, which does not alter the fact that they are entitled to a cookie under Art. 45c TCA.

right of objection.

3.7.1 Weighing up the use of non-essential cookies against the severity of the infringement of privacy

Whether the private interests of the data processor outweigh a specific infringement of personality rights and thus justify it depends on the balance between the interests of the controller and the data subject in each individual case.[27] Website operators must therefore first examine which private interests are served by the cookies or similar technologies they use beyond the limits of the principle of proportionality, what benefits and disadvantages they have for the data subjects and how serious the infringement of the data subjects' personality rights resulting from the disadvantages is. It must then be weighed up whether the infringement is reasonable for the data subjects, so that the private interests of the website operators prevail. Elements such as the storage period of the information collected with cookies or any data disclosure to third parties must be included in the assessment.

3.7.2 Optional design reduces the severity of the intervention

In most cases[28] , the controller can reduce the severity of the interference associated with data processing that violates personal data to a level that is compatible with data protection by granting the data subjects the right to object to the processing guaranteed by Art. 30 para. 2 lit. b FADP. For the use of non-essential cookies, this optional arrangement is prescribed by Art. 45c TCA, meaning that the controller must always give the data subject the option of rejecting the use of such cookies.

3.8 Legal factual constellations that indicate a possible predominance of private interests

As part of the balancing of interests, private controllers will first try to invoke the constellations listed in Art. 31 para. 2 lit. a - f FADP. On the one hand, this non-exhaustive catalog indicates a possible predominance of the constellations of interests described there. On the other hand, according to the case law of the Federal Supreme Court, an overriding private interest can only be affirmed with caution.[29] It can be concluded from the legislator's exemplary list that the controller is subject to limits in all constellations in which he can assert a legitimate private interest, in that he must determine a clear processing purpose and proportionately restrict the scope of the data to be processed in terms of time, content and accessibility. This is in order to keep the interference with the personality of the data subjects as low as possible so that it remains reasonable for them.

For a private interest in the use of non-essential cookies to considered overriding, the relationship between the purpose and the means must be appropriate. This is not the case if there are milder means to achieve the same purpose or if the interference with the personality of the data subjects for the fulfillment of these purposes is so serious that it is unreasonable for the data subjects. For example, the private interest of the website operator in an analysis of visitor flows supported by cookies cannot justify personal data evaluations if this purpose can be fulfilled with an anonymized evaluation.

3.8.1 Use of cookies in direct connection with the conclusion or execution of a contract

With the use of cookies, private controllers support a variety of functionalities in the practice of e-commerce that serve to conclude or process contracts. For example, cookies that enable the selection of items in the shopping cart of an online order or of

[27] Cf. BGE 136 II 508 p. 521, E. 5.2.5

[28] If the use of non-essential cookies takes place in the context of processing operations that associated with serious interference or high risks to the personality and fundamental rights of the data subjects, the optional use cannot bring about this reduction to a legally sufficient extent (Section 3.10).

[29] BGE 136 II 508, E. 5.2.4 and 6.3.3.

payment modalities and also serve commodities as home deliveries based on address data, which are not absolutely necessary for technical reasons. In Art. 31 para. 2 lit. a. FADP, the legislator has indicated a possible overriding private interest in such uses.

3.8.2 Use of cookies for research and statistics

The justification for non-personal data processing such as research and statistics pursuant to Art. 31 para. 2 lit. e FADP also proves to be particularly relevant with regard to the use of non-necessary cookies. This is because the analysis of website visitor flows is often carried out using cookies and it is an important concern of operators to find out how their website is used and can be optimized.

To achieve this purpose, the legislator has already weighed up the interests and defined three conditions for affirming an overriding private interest of the private individual. Accordingly, the processing of personal data for non-personal statistical purposes is justified if the following three conditions are met:

a. The data is anonymized as soon as the processing purpose allows this. In the context of websites, this usually means immediately. If this is impossible or requires a disproportionate effort, appropriate measures are taken to prevent the data subject from being identifiable.

b. If the personal data is particularly sensitive, it shall disclose it to third parties in such a way that the data subject cannot be identified; if this is not possible, it must be ensured that the third parties only process the data for non-personal purposes.

c. The results are published in such a way that the persons concerned cannot be identified.

By complying with these legal requirements, the website operator can justify the analysis of visitor flows on the basis of overriding private interests. These requirements can also be met when using external analysis tools, provided that their providers do not process the data for their own purposes, but only on behalf of the website operator.

3.9 Granting the right to object and data protection default settings

Insofar as the use of non-essential cookies does not require express consent, the controller must structure the legally prescribed granting of the statutory right to object to the use of such cookies (section 3.7.2) in such a way that the granting of this right complies with the basic principle of good faith in accordance with Art. 5 para. 2 FADP (see section 3.10.4). In addition, the website operator must ensure that the use of cookies is limited to the minimum necessary for the intended purpose by means of appropriate buttons with suitable default settings in accordance with Art. 7 para. 3 FADP.

Furthermore, the controller must prominently display the right to object to the use of non-essential cookies on the website so that the opt-out option can be easily recognized by users who are interested in it, both on their first and subsequent visits, and can be selected and exercised with just a few clicks.

3.10 Qualified use of cookies

If the use of non-essential cookies occurs unexpectedly or in the context of processing operations that associated with serious interference or high risks to the personality and fundamental rights of the data subjects, the private interests of the data controllers are generally not able to outweigh the personality violations of the data subjects (a schematic overview can be found in Appendix A).

on the risk levels of the use of cookies).

3.10.1 Highly intrusive use of cookies in terms of personal rights and fundamental rights

The use of non-essential cookies is associated with a high degree of intrusion if it takes place in the context of processing that involves particularly sensitive personal data within the meaning of Art. 5 lit. c. FADP or result in high-risk profiling within the meaning of lit. g. of this provision. High-risk profiling leads to a combination of data that allows an assessment of key aspects of a natural person (see section 1.2). For example, the collection of geolocation data supported by cookies and similar technologies may result in high-risk profiling depending on the duration and radius of the data collection.

For the use of non-essential cookies in the context of highly intrusive processing, the controller can neither rely on the overriding nature of their private interests nor on the optional nature of the processing. Rather, he must obtain express consent from the data subject before carrying out the processing. This also applies in cases in which such intrusive operations are expected due to a general public perception[30]. In this context, consent must also be obtained for the disclosure of sensitive personal data or high-risk profiles to third parties.

Data controllers must assume a potentially high level of intrusion if profiling involves a large number of different data sets and they cannot rule out the possibility that the result could have serious consequences for the personality and fundamental rights of the data subjects. In such cases, data controllers are required to prepare a data protection impact assessment in accordance with Art. 22 FADP[31].

3.10.2 Unexpected use of cookies

The use of dispensable cookies must be considered unexpected or unusual if they serve purposes that are in obvious contrast to the purposes of the main personal processing in the context of which they are used. Such unusualness may exist, for example, if cookies are set for the linking and marketing of address and telephone data in the website-supported provision of charitable or friendly services or in certain online games. If, based on the specific circumstances, it can be assumed that such uses contradict the expectations of a significantly high proportion of website visitors, those responsible must make it particularly clear on the website that such cookies are set and that they can be objected to.

The contrast between purpose and expectation has a more serious impact on data subjects if cookies are used for commercial purposes on websites with sensitive content of a political[32], trade union or religious nature. Due to the connection with the processing of particularly sensitive personal data, the operators of such websites must obtain express consent from the data subjects before the unexpected use of cookies (see section 3.10.1).

3.10.3 Special labeling and highlighting obligations

In accordance with the principle of good faith, the controller must inform the data subject in a prominent place on the website, separately and with particular clarity, of the high level of intrusiveness or unusual nature of personal data processing or the associated use of unnecessary cookies. For example, in the case of qualified processing with a high level of intrusiveness, it is advisable that an automatic

---

[30] In the case of applications used by transport companies for the purpose of billing chargeable passenger transportation, the recording of position data is common practice today, but not the sale of sensitive data to third parties.

[31] In the event of an investigation, the FDPIC may order a data protection impact assessment to be carried out.

[32] Cf. the guidelines of December 15, 2022 of the federal and cantonal data protection authorities on the application of data protection law to the digital processing of personal data in connection with elections and votes in Switzerland: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/internet_technologie/leitfaden-wahlen.html

notice ("pop-up window") appears on the particularly intrusive or unusual use of cookies or that attention is drawn to this use by means of a conspicuous font size or font in an unmistakable manner (for technical implementation, see section 3.13).

These special labeling and highlighting obligations also extend to the generally mandatory obtaining of express consent (opt-in) and, in some cases, the sufficient granting of a right to object (opt-out) in the case of qualified cookie use:

3.10.4 Design of the statutory right to object and opt-out

An optional design of the processing may be appropriate, for example, if an unexpected use of cookies occurs without a high level of intrusion (see Section 3.10.2, first paragraph). When granting the right to object to such qualified cookie use, the controller must ensure, in addition to data protection-friendly default settings, prominent website placement and clearly visible display of the possibility to object (see section 3.9), that the latter is marked with a degree of conspicuousness that corresponds to the unusual nature of the cookie use in question. This degree is reached if, when the data subject first visits the website, it is impossible to overlook the fact that a qualified use of cookies is pending due to particularly conspicuous notices, which they can object to with just a few clicks.

3.10.5 Design of consent and opt-in

To justify highly intrusive processing and the associated use of cookies, the data controller must obtain explicit consent from the data subjects.
within the meaning of Art. 6 para. 7 FADP. For federal bodies, lit. c. of this standard already requires explicit consent to be obtained if the use of cookies results in profiling that has not yet exceeded the threshold of high risk.

The legally sufficient obtaining of an opt-in presupposes that the controller requires the data subject to actively click on or set a sign when visiting the website for the first time before they make use of the corresponding web offer. Once consent has been given, the website must prominently inform the data subjects on each visit that they can withdraw their consent to the use of cookies in question at any time. The website must then guide visitors who wish to withdraw their consent to the corresponding button by means of simple navigation (for the technical implementation of these requirements, see section 3.13).

3.11 **Use of cookies for personalized advertising**

3.11.1 Use of advertising cookies in a commercial processing context

It is generally common and known that many private companies use cookies in e-commerce practice for the purpose of delivering personalized advertising, so that this mode of use cannot be considered unexpected or unusual in a commercial context. Depending on the circumstances of the specific offer, comparable expectations may also exist for free online services such as the provision of contact opportunities on social networks (see section 3.10.2).

Even if a significantly high proportion of website visitors expect advertising tracking and the controller designs the legal opt-out option to be sufficiently data protection-friendly (see section 3.9), the controller's private interest in the use of cookies for online advertising purposes may not always outweigh this. In this respect, a distinction must be made between advertising tracking with profiling and qualified profiling or with a medium and high risk (for profiling, see section 1.2 and for the schematic risk classification, see Appendix A).

3.11.2 Advertising tracking by means of "normal" profiling

Advertisers use cookies to record the behavior and interests of visitors to their websites.

website in order enable a personalized presentation of offers or to send personalized advertisements for our own products on the basis of this data. The data collected and the analyses based on it thus result in profiling within the meaning of Art. 5 lit. f FADP, which allows conclusions to be drawn about certain aspects of the user's personality and consumer behavior.

For the use of advertising cookies that within the limits of this "normal" profiling, private controllers must ensure, as a minimum requirement, that it is immediately apparent to users of the website on their first and subsequent visits how they can exercise their right to object (opt-out) with just a few clicks when they search for the corresponding button (see section 3.9).

In contrast to private controllers, federal bodies must obtain express consent for the use of cookies that lead to "normal" profiling within the meaning of Art. 5 lit. f FADP. However, it should be noted that federal bodies can act under both sovereign and private law. When using advertising cookies, the latter should generally apply, meaning that the FADP provisions on data processing by private parties apply to their use.

3.11.3 High-risk advertising tracking by means of profiling

Website operators often use cookies to record the behaviour and interests of visitors in order to enable third parties to place personalized advertising on the basis of this data or to sell them the placement of personalized advertisements by auction. In order to create as comprehensive a picture as possible of the consumer behavior of users, such tracking is usually carried out several websites using cookies. This can exceed the intensity of normal profiling, so that it leads to high-risk profiling within the meaning of Art. 5 lit. g FADP. If this threshold is exceeded, data controllers must comply with the requirements for processing operations that are characterized by a high level of intrusiveness with regard to labeling and highlighting obligations as well as obtaining consent (see sections 3.10.3 and 3.10.5). As long as controllers cannot rule out the possibility that the threshold of "normal" profiling is exceeded due to the lack of the necessary analysis, they must assume a potentially high risk (see section 3.10.1).

In the final report of 11 April 2024 on a clarification of facts concluded under the old FADP of 19 June 1992, the FDPIC qualified processing within the meaning of the old legal concept of "personality profile" under Art. 3 lit. d aFADP, from which the legislator of 2020 derived the new legal concept of "high-risk profiling" under Art. 5 lit. g FADP[33]. The clarification was directed against a company that had processed its customers' usage data on its own platform using cookies and linked it with data from other companies in the same group of companies in order to analyze user behavior across all offers. The FDPIC qualified the processing as a "personality profile" based on the following circumstances: Firstly, the economic operators participating in the tracking were active in different sectors. Secondly, the personal data in question was collected over a longer period of time, and thirdly, publicly available data and data from third-party providers could also be used to improve the database[34].

3.12 Legal requirements for obtaining consent and granting rights of revocation and objection

Neither the FADP nor Art. 47c TCA provide for the obtaining of consent as a mandatory requirement for the lawfulness of data processing using non-essential cookies. The consent of the data subject is only one of several reasons for justifying data processing that violates personal data, which the legislator lists in Art. 31 para. 1 FADP.

---

[33] BEAT RUDIN, in: BAERISWYL/PÄRLI/BLONSKI (ed.), Stämpflis Handkommentar zum DSG, 2nd edition, Art. 5 N 52.

[34] S. Final report of the FDPIC of April 11, 2024 in the matter of Ricardo AG and TX Group: https://www.newsd.admin.ch/newsd/message/attachments/90124.pdf

Even in constellations in which it would be possible to obtain the consent of a wider group of people, this can prove to be time-consuming and costly. For practical reasons, consent is therefore usually only obtained by private controllers when it becomes apparent that the resulting disadvantages for the data subject outweigh the private interest in the use of non-essential cookies if a mere right to object is granted.

3.12.1 Appropriate application of the provisions on the right to object to cookies

The central requirements for valid consent to the use of non-essential cookies or similar technologies are, in accordance with Art. 6 para. 6 FADP, appropriate information about the data processing to which consent is to be given and the voluntary nature of the declaration of consent.

Consent to the processing of personal data, objection to such processing and the revocation of consent granted or an objection lodged are four rights that are legally related in nature. The requirements explained in the following chapters for obtaining legally valid consent and for granting a valid revocation thereof must therefore apply mutatis mutandis with regard to the granting of the right to object and the revocation thereof in good faith (see sections 2.1, 3.7.1 and 3.9).

3.12.2 Informed consent

According to the case law of the Federal Administrative Court, the requirement of adequate information aims to ensure that the data subject gives their consent in full knowledge of the facts, i.e. that they only have to decide once they have been able to form an impression of the possible negative consequences of their consent. It is ultimately necessary, but also sufficient, for the data subject to be aware of what they are consenting to, i.e. what the implications of their decision are. [35] The requirement of adequate information is thus closely linked to the principle of recognizability and the information obligations under Art. 19 FADP (see section 3.3). If data processing that violates personal data is to be justified by the data subject's consent, the requirements for transparency must be set high because the controller wants to transfer joint responsibility for the consequences that violate personal data to the data subject by demanding consent. The data subject must therefore be able to understand which data processing is to be carried out on the basis of their consent and for what purpose. Only in this way can they assess the consequences or risks of data processing in relation to their personal rights and make a legally valid declaration of intent. In application of the principle of proportionality, the more sensitive the personal data concerned, the clearer the information must be.[36]

The Federal Administrative Court states that, depending on the situation, it will be necessary to provide information that not only refers to the circumstances of the data processing, but also to the most important potential risks or consequences for the data subject.[37] This is because the form of appropriate information depends on the person or group of persons who are to be informed.[38] If the target audience of data processing is minors who are capable of judgment and who their right to informational self-determination independently,[39] the data processor is expected to use simple and unambiguous language and to specifically point out the possible risks or consequences of the corresponding data processing.

As explained above in section 3.3.2, information about the imminent use of cookies must always be provided before the declaration of consent is issued.[40]

---

[35] See BVGE 2009/44 E. 4.2.

[36] LUKAS BÜHLMANN/MICHAEL SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, para. 52 and 54 KLAUS SAMUEL/THOMANN KENZO in: BIERI/POWELL (eds.), Orell Füssli Kommentar zum DSG, 1st ed., Art. 6 DSG N. 21.

[37] See BVGE 2009/44 E. 4.2.

[38] TOBIAS FASNACHT, Consent in data protection law, Zurich 2017, N 263

[39] In the case of children, the parents exercise this right on behalf of the children to the extent of their parental custody.

[40] MONIKA PFAFFINGER in: BAERISWYL/PÄRLI/BLONSKI (eds.), Stämpflis Handkommentar zum DSG, 2nd ed., Art. 31 DSG N. 33; TOBIAS FASNACHT, Consent in data protection law, Zurich 2017, N 252.

3.12.3 Specific consent

Consent to the use of non-essential cookies must be clear from the circumstances as an expression of the data subject's will that he or she agrees to the data processing about which he or she was previously informed. Furthermore, this expression of will must relate to clear, specified and legitimate data processing.[41] General clause-like declarations of consent or blanket consent are thus excluded (e.g. the frequent formulation "for marketing purposes").[42]

3.12.4 Voluntary consent

Consent must be given voluntarily in accordance with Art. 6 para. 6 FADP. Consent given on the basis of deception or under duress is invalid. Deception can occur if the controller deliberately misrepresents facts or withholds important information in order to influence the data subject's decision.[43] Misleading representations and formulations (so-called "dark patterns" or "nudging") can therefore lead to the invalidity of consent.[44]

It can be inferred from the case law of the Federal Supreme Court that consent is to be considered involuntary in particular if refusal to give it would result in disadvantages that are unrelated to or disproportionate to the purpose of the data processing. [45] Consent is therefore voluntary if the data subject has a genuine or free choice or is in a position to refuse or withdraw consent without disproportionate disadvantages.

In the context of websites, the question of voluntariness arises in particular if access to the website or a characteristic main service is denied as long as consent has not been given to one or more data processing operations that are not necessary for the main service, such as the setting of third-party cookies. Whether consent can be validly granted under these circumstances depends on whether or not the waiver of the main service can be considered reasonable for the data subject in the specific case. If the waiver is not reasonable, the controller must provide an equivalent alternative so that consent can be considered voluntary. A reasonable waiver is more likely to be denied if there is a relationship of dependency and the consequence is a lack of or poor [alternatives46]. It is easier to refrain from participating in a one-off competition than from ordering a product from a dominant online retailer or from using an online job portal or social network. It should be noted that the importance of social networks and online portals for participation in social life is [likely] to increase further as digitalization progresses47.

3.12.5 Form and form of consent

The legislator of the FADP has not tied consent to any legal [form48]. However, the form in which consent is obtained can be relevant to its validity. For example, if the controller obtains consent for several data processing operations with different purposes. If different types and functionalities of cookies are combined, users must be given the option of individually selecting or deselecting data processing with different purposes. A dialog box that only allows users to either accept "everything" or to completely refrain from displaying the content of the website cannot be understood as a clear declaration of consent. This is particularly the case if processing that is carried out without the consent of the data subject

---

[41] Art. 5 para. 4 ER-Conv 108+; Message on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Further Data Protection Ordinances of September 15, 2017, BBl 2017 6941, p. 7027.

[42] BRUNO BÄRISWYL, in: BAERISWYL/PÄRLI/BLONSKI (eds.), Stämpflis Handkommentar zum DSG, 2nd ed. Art. 6 N 86.

[43] TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, Zurich 2017, N 276 et seq.

[44] "Dark Patterns. Documenting the unknown". Report of the Federal Council in fulfillment of Postulate 22.3190, Michaud Gigon Sophie, 16. March 2022, p. 30 ff. Available at: https://www.newsd.admin.ch/newsd/message/attachments/88176.pdf

[45] BGE 138 I 331 E. 7.4.1.

[46] TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, Zurich 2017, N 295 ff.

[47] See EDPB, Opinion 08/2024 on "Effectiveness of consent in the context of "Consent or Pay" models of large online platforms" of April 17, 2024.

[48] According to Art. 6 para. 7 FADP, however, consent must be given expressly for: the processing of particularly sensitive personal data; high-risk profiling by a private individual; or profiling by a federal body.

may be mixed with those for which the controller must obtain authorization. On the other hand, it may be permissible to combine different data processing operations that serve the same purpose.

3.12.6 Express consent

In order to obtain consent, for which the FADP requires an express declaration or opt-in in Art. 6 para. 7 FADP, data controllers must always require active behavior from the data subjects, with which they must manifest their express consent. The situation is different when granting rights of objection and revocation, which represent options for the data subjects that they can, but do not have to, exercise by actively selecting buttons or setting signs (for technical implementation, see section 3.13).

3.12.7 Revocation of consent

Consent to the use of non-essential cookies must be revocable at any time, informally and without justification. The responsible website owner must offer website visitors simple options for exercising their right of withdrawal. If the website owner makes it more difficult to withdraw consent, for example by installing administrative chicanery that leads to an unreasonably higher effort than granting it, this violates the requirement of voluntariness. If data controllers make the revocation dependent on the deselection of a large number of data processing operations, this constitutes an inadmissible "dark pattern". Even if the granting of the right of withdrawal is so complicated that an average user cannot be expected to the time to make a conscious decision, this must lead to the invalidity of the consent.

By analogy, data processing may not be considered lawful if the controller disregards the principles of good faith when implementing the statutory right to object or to withdraw it.

3.12.8 Consequences of legal deficiencies in the granting of the rights to consent and objection

Legal deficiencies for the controller is solely responsible, which lead to the fact that consent to the use of cookies was given due to a lack of information or will or that declarations of objection were not made, cannot have any legal effect to the detriment of the declarants or the data subjects affected by the data processing.

3.13 Technical implementation

The general and more extensive information obligations for the setting of non-essential cookies as well as the requirements for obtaining consent and granting rights of revocation and objection were presented above. The following information is intended to support the responsible website operators in the technical implementation of these data protection requirements, which are largely left open by the Swiss legislator:

3.13.1 Implementation of timeliness

In order to comply with the legal requirements for obtaining consent with regard to the use of cookies, the website must be technically set up in such a way that the data processing in question only takes place after the data subjects have had the opportunity to take note of it. For example, if cookies are used so that third parties can collect data from visitors and this data processing is based on the consent of the data subject, then this data processing must not be activated by default at the time the website is accessed. In order to enable prior information, the implementation of a two-click solution is indicated, which ensures that the JavaScript is only activated after the visitor has been informed and has given their consent. This applies in particular to the integration of social plugins, tracking pixels and other third-party services.

3.13.2 Consent banner

For the technical implementation of the information and self-determination rights of website visitors (see section 3.10.3), the obtaining of consent (opt-in) and the subsequent storage of permitted cookies or blocking of non-essential cookies by

In practice, so-called "cookie banners" or CMPs[49] are commonly used for opting out.

Users are informed by means of such banners about the options for activating or deactivating individual aspects and functionalities of a website and can make informed and self-determined decisions in this regard, which they communicate to the operator of the website and any third parties. This can be done, for example, by checking or unchecking the relevant boxes or by clicking on the relevant buttons.

In the technical implementation of "consent banners" to obtain express consent within the meaning of Art. 6 para. 7 FADP, controllers must always use buttons or fields that require users to actively click on or set signs with which the latter must visualize their express consent (see section 3.12.6). If the website operator decides to preset certain processing and processing modalities for which the law does not require express consent[50] by default, he may not make the deselection of an already checked box more complicated than the selection of the same.

If the website operator decides to display both data processing operations for which consent is obtained and those for which this is not the case in the consent banner, it must be clear to the data subjects which fields mandatory and which are optional. When visually implementing the "consent banner", data controllers must also ensure that the use of fonts, images and colors does not lead to confusion, errors or omissions when exercising design rights (see section 3.12.4).

[49] "Consent management platform"

[50] According to Art. 6 para. 7 FADP, consent must be given expressly for: a. the processing of particularly sensitive personal data; b. high-risk profiling by a private individual; or c. profiling by a federal body.

Risk factors of cookie use		Risk values 1-3
Personal reference	No	0
	Yes	1
Technically necessary	Yes	1
	No	2
Expected by users	Yes	1
	No	2.5
Profiling	No	1
	Yes	2
Profiling with high risk	Yes	3
Particularly sensitive personal data	No	1
	Yes	3

Rights of the data subjects	
For risk values 0 - 1 (necessary cookies)	Acceptance or waiver for entire offer
For risk values 1 - 2.5 (functional cookies and cookie inserts with "normal" profiling)	Opt-out mandatory
For risk values> 2.5 (qualified cookie inserts)	Opt-in mandatory

