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

with additions dated 6 October 2025

Version	Date	Description
1.0	22.01.2025	First finalised version
1.1	06.10.2025	Addition to footnote 5; addition of a sentence to paragraph 3 in section 3.1.2.; addition to the last sentence of section 3.2.2; clarifying addition in section 3.5.2; clarifying additions in section 3.6; addition to section 3.8.1; addition of a reference in the last sentence of the first paragraph in section 3.9., clarifying additions in section 3.10.1; additions and clarifications in section 3.11.1; clarification of the first sentence in section 3.11.3 regarding embedded third parties; addition of a second paragraph in section 3.12.3; clarification in section 3.12.4 regarding free services and cookie paywalls.

Contents

In these guidelines, 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 authorities. The FDPIC has drawn up these requirements based on the Federal Data Protection Act (FADP; SR 235.1), the Data Protection Ordinance (DPO; SR 235.11), special statutory data protection provisions within federal law, judicial precedent from the Federal Supreme Court, relevant academic opinion, and the Commissioner's own supervisory practice to date.

1 Terms

1.1 Cookies and similar technologies

Cookies are small text files that website operators and third parties that they authorise save on website visitors' computers in order to collect user data. These data are then made accessible for further processing with the aim of fulfilling specific functionalities, e.g. for online shops.

Based on duration of storage, the use of cookies can be categorised as follows: session cookies are saved in the visitor's browser for a limited time and are automatically deleted when the browser is closed. Permanent cookies are saved in the browser for a longer period of time – for example, to enable the website visitor to be recognised on future visits.

Cookies fulfil a range of different functions. For example, they can store language settings, a login or, after an online shop visit, the products saved in the visitor's shopping basket. Cookies are also used for a process known as stateful tracking: 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 recognised on subsequent visits and information about website visitors' user behaviour can be collected. This makes it possible to analyse the data traffic on a website and to personalise its content and advertising.

Cookies can also be differentiated according to whether they are set by a website provider itself (known as first-party cookies) and whether they are set not by the website provider itself, but by third parties such as advertisers (known as third-party cookies). In the former case, data are transferred between the website operator's system and the user's end device. In the latter case, datafiles from third parties are stored in the user's browser when the user accesses the website. In other words, the website operator does not actually transfer any data to third parties. Instead, third parties obtain data directly from the data subject with the website operator's permission. If a user then accesses content on another website where the same third party is integrated, the user will be recognised. In many cases, third parties combine information obtained through cookies with additional information gathered directly from users of their own services or shared by other third parties. This allows them to create comprehensive user profiles across different websites.

The collection and analysis of data on surfing behaviour is commonly referred to as tracking. However, tracking is not always based on the use of cookies. With stateless tracking, no information is stored on the user's end device. Put simply, data are not collected and analysed via the user's browser, but via the server. In these guidelines, tracking technologies such as browser fingerprinting, ID graphs, user IDs, ETags, pixels and authentication caching are all included under the term 'similar technologies'. These guidelines also use the term 'similar technologies' to refer to data processing related to integrated third-party services, such as 'Like' and 'Share' buttons from online social platforms.

1.2 Personal tracking and profiling

Personal tracking refers to the process of recording and evaluating individuals' surfing behaviour. The data collected are used for various purposes, such as analysing websites for optimisation potential. For example, they can form the basis for website performance evaluations, online advertising and marketing campaigns. Tracking can serve as a starting point for displaying personalised promotional offers to end users based on the user profiles created. More comprehensive tracking enables advertised content to

be tailored more precisely to individual people. The logic is that the more data that are available about users, the better the algorithms predict their preferences. For this reason, information on surfing behaviour is often supplemented with information from other sources (e.g. social media or other websites visited) or with predictions or information calculated by algorithms, which can create user profiles (profiling).[1]

Profiling is to be assumed in accordance with Article 5 letter f FADP if the purpose of personal tracking is to evaluate specific personal aspects relating to a person, in particular to analyse or predict that person's work performance, economic situation, health, personal preferences, interests, reliability, location or movements.

Personal tracking may lead to profiling that poses a high risk to the data subject's personality or fundamental rights as laid down in Article 5 letter g FADP. This occurs when data is linked in ways that allow essential aspects of a person's personality to be assessed. In cases of this kind, controllers must consider introducing special protective measures, such as carrying out a data protection impact assessment in accordance with Article 22 FADP (see section 3.10.1).

2 Legal sources

2.1 Provisions of the Telecommunications Act

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

The provision of the TCA relates to the technical processes for setting, reading and storing cookies. As these processes compromise the integrity of end devices by sharing data with other computers unnoticed, Article 45*c* TCA aims to protect the privacy and informational self-determination of users of these end devices. In other words, Article 45*c* TCA constitutes a special public-law standard for otherwise unnoticed 'telecommunications' processes[2]. As a provision of federal data protection law specific to this case, it must be complied with alongside the general data protection law contained in the FADP.[3]

Article 45*c* letter b TCA ensures that all data processing on third-party devices is either used for telecommunications transmission or, if this is not the case, can be controlled by the device users.[4] Under Article 45*c* TCA[5], website operators are obliged to inform website visitors about the use of technologies of this kind and to state their purposes. In addition, website operators must remind data subjects that they may refuse to allow the processing of their data and inform them how they can do so. The way in which data subjects are to be informed is not stipulated by the provision and must be specified in accordance with the FADP (see section 3.7.1, section 3.10.4 and sections 3.11.1. to 3.12.8).

2.2 Provisions of the FADP

The FADP governs all aspects of personal data processing that is carried out using cookies and similar technologies. These guidelines cover the provisions of the FADP, including their regulatory relationship to the special provision of Article 45*c* TCA[6].

[1] Müller-Peltzer, Philipp/Guttmann, Philipp, 'State of the art' Webtracking – aktuelle Entwicklungen, aufsichtsbehördliche und gerichtliche Positionen, DSB 2023, p. 233.

[2] Dispatch on the Amendment of the Telecommunications Act of 12 November 2003, BBl 2003 7951, p. 7,987.

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

[4] Dispatch on the Amendment of the Telecommunications Act of 12 November 2003, BBl 2003 7951, p. 7,987.

[5] Wilful or negligent violations of this provision are punishable by a fine of up to CHF 5,000 in accordance with Art. 53 TCA.

[6] See also FAC decision A-3548/2018 of 19 March 2019, consid. 5.4.

3 Data protection requirements for the use of cookies

3.1 Personal identifiability of persons during data processing

3.1.1 Personal identifiability in general

Personal data are any information relating to an identified or identifiable person (Article 5 letter a FADP). A person is deemed identified or at least identifiable if their identity can be inferred directly from the data itself, from the context of the data or by combining the data with other information.[7] The relationship to the data subject (i.e. personal identifiability) may be established in various ways, such as by means of a key, an OASI number, a reference number or even a customer number, but this is generally irrelevant.[8]

According to judicial precedent from the Federal Supreme Court ('Logistep decision'[9]), a person is deemed identified if the information itself clearly refers to precisely that person. A person is deemed identifiable if they can be identified through additional information, although not all theoretical possibilities for identification are sufficient. If the effort required to identify the person is so great that, based on general life experience, no interested party could be expected to undertake this task, the person is not deemed identifiable[10]. Identifiability must therefore be determined on a case-by-case basis, with particular consideration given to the technological options available. However, it is important to establish not only what effort is objectively required to link a specific piece of information to a person, but also what interest the processor or a third party has in identifying that person.[11] This interest may change over time, as may the means of identification available to the processor or a third party. In other words, a person may be identifiable to specific people or organisations 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[12]. If information is passed from data processor A, who cannot link the data to a person with a reasonable amount of effort, to data recipient B, who is able to identify the person using additional information, the FADP applies to both data recipient B and data processor A. According to the Federal Supreme Court, to decide otherwise "would mean applying the Data Protection Act only to the individual recipients, but not to the person who obtains and disseminates the relevant data. This would be contrary to the purpose of the Act."[13]

However, a person is no longer deemed identifiable if personal data has been anonymised. Anonymised means that personal references have been irreversibly removed in such a way that it is no longer possible to link the data to individuals without disproportionate effort.

3.1.2 Personal identifiability through the use of cookies

Whether and to what extent the use of cookies or comparable technologies results in personal identifiability when processing data, or whether such identifiability is increased, depends on the circumstances of the individual case – in particular, the information transmitted by the cookies and the other data they are combined with. Personal identifiability may exist if the processed information itself contains an identifying characteristic, e.g. a unique user identification (UID) for Android or ad ID for Apple devices[14]. In addition, personal identifiability may arise due to the circumstances in which the data was

[7] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,019.

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

[9] Federal Supreme Court decision 136 II 508, consid. 3.2 ff.

[10] Dispatch on the Federal Act on Data Protection of 23 March 1988, BBl 1988 II 413, p. 444 f. and Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,019.

[11] Federal Supreme Court decision 136 II 508, consid. 3.2 ff.

[12] See Federal Supreme Court decision 136 II 508, consid. 3.4; BEAT RUDIN, in: BAERISWYL/PÄRLI/BLONSKI (ed.), Stämpflis Handkommentar zum DSG, 2nd edition, Art. 5 N 11 f.

[13] Federal Supreme Court decision 136 II 508, consid. 3.4.

[14] See the FDPIC's final report of 11 April 2024 re Ricardo AG and TX Group, section 128: https://www.edoeb.admin.ch/en/nsb?id=102867 (de)

collected and analysed by the website operator or third parties, even if no identifying information was available at the time of collection and therefore only non-personal data was (initially) collected.

Personal identifiability is created at the latest when the website owner or integrated third-party services can link factual data with specific and identifying information based on a login[15] or comparable online identifiers. For example, when a visitor selects a language when accessing a website for the first time. In this case, a cookie and the information that the visitor wishes to use the website in the selected language will be stored on their end device. If this information cannot be linked to the website visitor, the data processed using this text file are not considered personal data. If the website operator can link the language setting to a specific visitor, e.g. because they registered for the website's online shop beforehand or afterwards, the data must be considered personal data[16].

If records on a person are labelled for the sole purpose of being uniquely identifiable within an information system, but no identifying characteristics of a person are assigned to the records, this is known as singularisation. Whether and to what extent processing of this kind establishes personal identifiability is still largely unresolved by legal doctrine[17] and judicial precedent[18] and depends on the context of the processing in each individual case. In practice, a high probability of personal identifiability can be presumed when collecting location data if the processing generates profiles of data subjects' movements. If these profiles are used to identify places where people regularly spend time, such as offices, shops or people's homes, inferences can be made about specific people's real identities.[19]

In cases of doubt where, when using cookies, it cannot be determined with sufficient certainty whether it is or could be possible to identify persons with a reasonable amount of effort, the FDPIC advises assuming that personal data may potentially be processed. If it is difficult to determine whether identification is possible, but identification could also pose high risks for the data subjects, the FDPIC recommends that controllers check whether the processing in question and the related cookie usage should be subject to a data protection impact assessment (see section 3.9.1).

3.2 Responsibility

As specified in Article 5 letter j FADP, persons who decide on the purpose and means of processing, either alone or in conjunction with others, are deemed to be responsible under data protection law.

In the context of websites, the website owners are responsible for cookie usage, because they determine which data is processed via their website and for what purpose. As controllers, they must in particular

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

[16] Austrian Data Protection Authority (ADPA), FAQ on data protection & cookies: https://dsb.gv.at/faqs/datenschutz-cookies (de)

[17] Critical opinion: David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16 November 2020, idem in digma, Heft 4, December 2017; however, favourable decision from ADPA re 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, of 22 December 2021, re 'Google Analytics', D.2. Spruchpunkt 2. a) und b). See also Philip Glass, Identifizierung und Singularisierung, www.datalaw.ch, para. 9 f. (https://www.datalaw.ch/singularisierung-und-identifizierung/; as at: 11 July 2024).

[18] In the Federal Supreme Court decision 136 II 508 re Logistep, the Federal Supreme Court stated in consid. 3.6 that its interpretation of the concept of personal data under the FADP appeared to be in line with the legal position in the European Union at the time. Specifically, it referred to Opinion 4/2007 of 20 June 2007 adopted by the independent EU advisory body on data protection and privacy (Article 29 Data Protection Working Party). See also p. 16 of Opinion 4/2007: *"At this point, it should be noted that, while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other 'identifiers' are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects this fact."*

[19] The profiles based on a person's movements can in turn be used to make sensitive inferences about the data subject's private life by analysing locations that are visited repeatedly, such as other persons' homes or doctors' and lawyers' practices. This may also intrude on the privacy of other persons.

ensure that the processing principles under Articles 6 and 8 FADP are complied with and that data subjects are adequately informed of the data processing (see sections 3.3 and 3.5.1).

If website owners integrate third-party services into their website, it is important in terms of their responsibility to distinguish whether they use the third-party services for the purpose of commissioned data processing (outsourcing) as set out in Article 9 FADP, or whether the third parties use the services embedded on the website to obtain data (also) for their own purposes.

3.2.1 Commissioned data processing

In the case of commissioned data processing (outsourcing) as defined in Article 9 FADP, the controller transfers the processing of personal data to a third party. Information processing 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 an 'internal relationship' between the controller issuing the commission and its commissioned data processor, which means that transfer of data to a commissioned data processor does not constitute disclosure of personal data to third parties[20]. As such, the controller does not need a special justification to transfer data processing. However, a contract or a statutory provision and compliance with the other provisions of Article 9 FADP are required[21].

3.2.2 Data collection by third parties

If social plug-ins from platforms such as Facebook, X and Instagram or videos from platforms such as YouTube are integrated, website operators can use specific social network functions on their own websites. When third-party products are integrated into a website, the visitor's browser will be prompted to request the provider's content and to transfer the visitor's personal data to the third-party provider for this purpose. In this configuration of embedded services, third parties process the personal data collected for their own purposes and thus in their own interests. As specified in Article 19 FADP, collection of personal data must be disclosed to the data subjects by both the website operator and the third parties collecting the data. As per paragraph 3 of that provision, the latter must also inform the data subjects of the categories of personal data they collect about them through use of cookies on a third-party website. This information then allows website visitors to exercise their right under Article 45*c* TCA to refuse processing (see section 2.1).

Article 5 letter j FADP defines responsibility broadly insofar as the decision on the means used to process data or the purpose of the processing can be made jointly by multiple controllers. The third party is primarily responsible for its data processing, as it influences the personal data processing in its own interests and thus participates in the decision on the purposes and means of processing. The website owner, meanwhile, enables the third party to collect data by integrating the third-party service on its website (means), even if it has little or no influence on the downstream data processing. It follows that joint or shared responsibility must be assumed for the third party's data collection process ('processing', as defined in Article 5 letter d FADP) via the website[22].

As website operators control which third-party services are integrated, they cannot assume that their responsibility ends where third parties' terms of use apply. They are responsible for ensuring that websites comply with data protection regulations. They must therefore familiarise themselves with the data processing carried out by integrated third-party services and ensure that legal requirements are met. In particular, website operators must ensure that they fulfil all duties to provide information to the relevant website visitors and, if necessary, that they obtain sufficiently specific consent (see sections 3.10.1 and 3.12.3).

---

[20] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,023.

[21] Further information on our website: Outsourcing of data processing

[22] See CJEU judgment of 29 July 2019 C-40/17.

3.3 General information obligations

3.3.1 Form and content of information

According to the introductory sentence of Article 19 paragraph 2 FADP, data subjects must be provided with all the information necessary for them to assert their rights under the FADP and to ensure transparent data processing. Article 19 paragraph 2 letters a–c, paragraph 3 and paragraph 4 FADP expand upon this principle by specifying the minimum information that must be communicated to data subjects. These general information obligations naturally also apply to the use of cookies and similar technologies.

The minimum information includes: the controller's identity (i.e. the name or company) and contact details (Article 19 paragraph 2 letter a FADP), the purpose of the data processing (Article 19 paragraph 2 letter b FADP) and, if applicable, the recipients or categories of recipients to whom the personal data is disclosed (Article 19 paragraph 2 letter c). When collecting personal data, therefore, controllers must inform data subjects that their data will be disclosed to a processor or a third party and communicate the purpose of the data transfer or disclosure. Finally, if personal data are disclosed abroad, data subjects must also be informed of the state or international body with which the data have been shared. If applicable, they must also be informed of the guarantees under Article 16 paragraph 2 FADP or the application of an exception under Article 17 FADP (Article 19 paragraph 4 FADP).[23]

The FADP does not specify the way in which data subjects must be informed. Article 19 paragraph 1 FADP stipulates only that information must be provided in an "appropriate manner". Appropriateness depends on whether data subjects can make a conscious and self-determined decision based on the information they receive and exercise their rights of alteration, such as consenting to or rejecting personal data processing or cookie usage in a legally compliant manner (see sections 3.9 and 3.12). The more extensive and unexpected the data processing is and the more seriously it intrudes on the data subject's personality rights, the higher the requirements for the accessibility of the information.[24]

Article 13 DPO specifies that the controller must provide the data subject with information on personal data collection in a precise, transparent, comprehensible and easily accessible form. Neither the FADP nor the DPO stipulate requirements as to the precise form in which the information must be provided. Possible options therefore include privacy policies, terms of use, notices and pictograms. However, data subjects must be informed actively, which means that controllers must provide this information unprompted and ensure that data subjects can actually take note of the full information in a reasonable manner.[25] It is therefore not enough to place a privacy policy somewhere in a remote corner of the website or to provide the information only on request.

In order to fulfil the requirements of Article 13 DPO, information in written form must be reader-friendly and tailored to its audience's needs. In the digital reality, a layered approach is essential. This means controllers must ensure that data subjects always receive the most important information at the first level of communication when their personal data are collected. For example, a privacy policy drawn up using this approach allows data subjects to obtain a summary of all essential information at a glance, while specialists, investigative journalists and supervisory authorities with more in-depth information requirements can obtain detailed legal and information technology information by accessing an additional level[26] (for the technical implementation of the requirements, see section 3.13). When integrating third-

[23] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,051.

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

[25] BRUNO BÄRISWYL, in: BAERISWYL/PÄRLI/BLONSKI (eds), Stämpflis Handkommentar zum DSG, 2nd ed., art. 7 N 16 ff.; see also Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment to Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,050.

[26] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,050 f.; Federal Office of Justice, Explanatory Report on the Revision of the Ordinance of 31 August 2022 on Data Protection, p. 37.

party services or outsourcing data processing, website operators can refer to further information from the third-party service or commissioned data processor for detailed information.

3.3.2 Moment at which the information is provided

According to the wording of the FADP, data subjects must be informed at the moment when their personal data are collected. This means that controllers who collect personal data directly from data subjects must ensure that the data subjects have been adequately informed by the time they choose whether to consent to or reject processing of their personal data and/or cookie usage (see sections 3.12.2 and 3.13.1).

3.4 Further information obligations

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

3.5 Application of FADP processing principles to the use of cookies

Article 6 FADP sets out the principles that controllers must also follow when using cookies and similar technologies if they expect the processing to establish personal identifiability (see section 3.1). This Article stipulates that personal data must be processed lawfully (paragraph 1), in good faith, and proportionately (paragraph 2). Personal data may only be collected for a specific purpose that the data subject can recognise, and the personal data may be processed only in a way that is compatible with this purpose (paragraph 3). Controllers must ensure the accuracy of the personal data processed (paragraph 5). Paragraphs 6 and 7 govern the requirements for the data subject's consent to be deemed valid. These requirements must also apply in a similar way to the right to refuse consent (see section 3.12.1). The principle of transparency is expressed in the duty to provide information when collecting personal data (Article 19 FADP). The principles of proportionality and data security are expressed in the obligation to ensure data protection-friendly default settings (Article 7 paragraph 3 FADP) and the obligation to ensure data minimisation (Article 6 paragraph 4).

Private individuals may process personal data unless doing so would unlawfully breach the data subjects' personality rights. Article 30 paragraph 2 letter a FADP specifies that personality rights are breached when private individuals process personal data contrary to the processing principles set out in Articles 6 and 8 FADP. As such, these principles set the statutory limits for data processing by private individuals. If the principles are violated, this constitutes an unlawful breach of personality rights as defined in Article 31 paragraph 1 FADP, unless the breach is justified by one of the grounds under Article 31 FADP (consent of the data subject, overriding private or public interest, or legal provision).

When processing personal data, federal bodies must comply with the principles of the FADP in the same way as private controllers, but they are also subject to the principle of legality under Article 34 paragraph 2 FADP, which stipulates that there must be a sufficient statutory basis for any processing. In accordance with the principle of proportionality, federal authorities use only the cookies that are technically required in order to carry out the data processing that is required by law in the public interest. Supplementary use of text files is possible, provided it is also in the public interest and there is a sufficiently specific statutory basis.

3.5.1 Principle of good faith and transparency

The principle of good faith as set out in Article 6 paragraph 2 FADP and the above-mentioned information obligations under Article 19 FADP ensure the transparency of personal data processing. Transparency is an indispensable prerequisite for data subjects to be able to assert their rights under the FADP and thus, in particular, to be able to exercise their rights of alteration, such as by consenting to or objecting to personally identifiable cookie usage, in a legally compliant manner (for the content, form and timing of the information obligations under Article 19 FADP, see section 3.3, and for qualified forms of cookie usage and qualified consent, see section 3.9 and sections 3.12 and 3.13 respectively).

3.5.2 Principle of proportionality

In accordance with the principle of proportionality set out in Article 6 paragraph 2 FADP, only data that are suitable and required for the intended purpose may be processed. There must also be an adequate relationship between the purpose and the means used.[27] This principle is set out in Article 7 paragraph 3 FADP, which obliges the controller to use suitable default settings to ensure that only as much personal data are processed as are necessary for their intended use, unless the data subject specifies otherwise[28].

Cookies are considered 'technically necessary' if they enable a website or app to be provided to the extent, technically speaking, that users require. This term therefore also refers to cookies and similar technologies without which:

- a website cannot be used for its actual function – or for the function required by visitors (functional aspect of technical necessity); or
- the requested processing cannot meet the minimum requirements for technical security as defined by Article 8 FADP (security aspect of technical necessity).

Technically necessary use of cookies and similar technologies based on functional criteria

The question of which cookies and similar technologies are technically necessary to ensure functional feasibility of the required processing depends on the purpose for which the data controller is processing the data in each specific case and cannot be answered in general terms.[29] An assessment of the circumstances of each individual case is used to determine whether data processing using cookies and similar technologies is appropriate, necessary and proportionate for a specific purpose. The assessment of proportionality will depend on the severity of the intrusion and the legitimate expectations of the data subjects using the website or app in question.[30]

In an online shop, for example, the use of shopping basket cookies that store the items customers have selected in the shop is necessary and therefore considered proportionate under data protection law. Cookies of this kind enable customers to add products to a digital shopping basket and complete the purchase process only once they have had the opportunity to find all the products they are interested in. They also prevent customers from having to spend time searching for all the products again if they do not manage to complete their purchase within a single browser session.

Technically necessary use of cookies and similar technologies based on security criteria

If data controllers wish to justify using cookies and similar technologies for security purposes, they must prove that this usage is necessary to ensure a level of data security appropriate to the risk, as defined in Article 8 paragraph 1 of the FADP.

The following is an example[31] list of cookies that are considered technically necessary and generally proportionate with regard to data subjects; data processing using these cookies can therefore generally also be regarded as proportionate:

---

[27] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,024.

[28] Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,030.

[29] In this respect, the proportionality test overlaps with the overriding private interest test, particularly as defined in Art. 31 para. 2 let. a FADP. Data processing that is absolutely necessary to provide an app service is justified by an overriding private interest on the part of the data processor and is also proportionate with respect to data subjects. See Federal Supreme Court decision 2C_369/2021 of 22 September 2021, consid. 6.1 and Federal Supreme Court decision 143 I 403, consid. 5.6.3; consid. 9.2.2 and Häfelin/Müller/Uhlmann, Allgemeines Verwaltungsrecht, 8th ed., N 555 ff.

[30] In applications used by transport companies to bill for passenger transport services, it is now common practice to collect location data. Users can avoid having to enter their starting point and destination manually by allowing the application to access their location. As the application can fulfil its purpose of selling tickets without collecting any location data, this use of data processing – which entails significant data protection risks – is not necessary or proportionate. Consequently, it must be justified by obtaining the user's consent.

[31] The following examples are intended as a guide to the cases in which data processing is very likely to be considered proportionate. However, there is no binding list of necessary cookies.

Technically necessary uses of cookies and similar technologies	
based on functional criteria	based on security criteria
• Shopping basket cookie: Storage of selected products in an online shop; • User input: Temporary storage of data in an online form; • Login: Authentication of a logged-in user (on a website that contains a protected area accessible only to logged-in users); • Language selection: Storage of the website visitor's chosen language (on websites available in multiple languages); • Cookie opt-in and cookie opt-out: Storage of cookie consent or rejection is required so that the cookie banner does not appear each time the page is accessed (on websites with a CMP[32]).	• Load balancing: Cookies that are used to evenly distribute a website's load; • Cookies to prevent brute force attacks through repeated login attempts; • Cookies to distinguish humans from computer bots (Captcha).

The criterion of necessity must be applied to cookie content, storage duration and any disclosure of data to third parties. In terms of content, it may be necessary to set cookies in order to store the visitor's consent or for load balancing. When associated with a unique user ID, they may be stored only if and as long as necessary to fulfil the website's functionality. A similar rule applies to storing language or background colour settings. These do not require a unique identifier such as a unique user ID; all that is needed is storage of a non-identifying specification such as 'background-colour: black' or 'language: de'.

As such, it is only possible to indirectly reject necessary cookies in application of Article 45*c* TCA (see section 2.1), and doing so will prevent access to the application as a whole.

3.6 Permissibility of non-essential cookies

In addition to the technically necessary cookies described in section 3.5.2, website operators often use cookies that help to optimise the user's experience when surfing the website. These are known as functionality or functional cookies. Use of these cookies conflicts with the data protection law principle of proportionality under Article 6 paragraph 2 FADP, as it exceeds what is necessary.[33]

If personal data are processed by a private controller contrary to the general processing principles set out in Articles 6 and 8 FADP, this constitutes a breach of the data subjects' personality rights as described in Article 30 paragraph 2 letter a. According to Article 31 paragraph 1 FADP, private controllers must not breach personality rights unless they can justify doing so by providing evidence of an overriding private or public interest, of relevant legal provisions or that they have obtained the data subject's consent.

As such, private controllers may use non-essential cookies[34] lawfully in the following ways:

- Firstly, when balancing interests, they can check whether the data processing carried out using these cookies can be justified by overriding private interests (see section 3.7);

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

Alternatively, controllers can make data processing that breaches personality rights optional for users by granting a right of rejection in accordance with Article 30 paragraph 2 letter b FADP. This is already

[32] Consent Management Plattform

[33] See above, section 3.5.2.

[34] The term 'non-essential cookies' refers to all cookies that do not fulfil the criteria to be considered technically necessary, as set out in section 3.5.2.

mandatory for the use of non-essential cookies due to the special legal requirement in Article 45*c* TCA (see sections 2.1, 3.7.2 and 3.9).

3.7 Overriding private interests as justification of cookie usage that breaches personality rights

In practice, advertisers often try to justify commercial cookie usage beyond the limits of the proportionality principle by claiming that their private interests prevail. If they provide evidence of such interests, they do not have to obtain consent from data subjects. However, this does not alter the fact that data subjects must be granted a right to reject cookies in accordance with Article 45*c* TCA.

3.7.1 Balancing the use of non-essential cookies against the severity of the personality rights breach

Whether the processor's private interests can justify a specific breach of personality rights depends on the balance of the controller's and data subject's interests in the individual case[35]. To this end, website operators must first consider the following points: which private interests are served by the use of cookies or similar technologies beyond the limits of the proportionality principle? What benefits and disadvantages does use of the cookies entail for the data subjects? And how severe is the breach of the data subjects' personality rights that arises from these disadvantages? It is then necessary to assess whether the breach is acceptable to the data subjects, such that the website operators' private interests prevail. Information such as the storage period of the information collected via cookies or any disclosure of data to third parties must be included in the assessment.

3.7.2 Opt-out feature reduces the severity of the intrusion

In most cases[36], controllers can take steps to address data processing that breaches personality rights. By giving data subjects the option to reject data processing, a right guaranteed by Article 30 paragraph 2 letter b FADP, controllers can reduce the severity of the intrusion, making the processing compatible with data protection legislation. When using non-essential cookies, this opt-out feature is mandatory under Article 45*c* TCA, which means that controllers must always give data subjects the option to reject the use of these cookies.

3.8 Specific circumstances set out in law that may indicate an overriding private interest

When balancing interests, private controllers will first try to appeal to the specific circumstances listed in Article 31 paragraph 2 letters a–f FADP. This non-exhaustive catalogue indicates circumstances in which private interests may prevail. However, according to judicial precedent from the Federal Supreme Court, an overriding private interest may only be affirmed with reservations.[37] Based on the legislator's list of examples, it can be concluded that controllers are subject to restrictions in all circumstances in which they can claim a legitimate private interest. They must define a clear processing purpose and proportionately limit the scope of the data to be processed in terms of time, content and accessibility. The aim of this is to minimise the violation of data subjects' personality rights as much as possible, so that it remains acceptable to them.

For a private interest in the use of non-essential cookies to be considered overriding, there must be a reasonable balance between the purpose and the means of processing. This is not the case if there are milder means available to achieve the same purpose, or if the violation of the data subjects' personality rights when fulfilling this purpose is so severe that it is unacceptable to the data subjects. For example, the website operator's private interest in analysing visitor streams through the use of cookies does not justify personal data evaluations if an anonymised evaluation could produce the same result.

[35] See also Federal Supreme Court decision 136 II 508 p. 521, consid. 5.2.5.

[36] If non-essential cookies are used in the context of processing operations that involve severe violation or pose high risks to the data subjects' personality and fundamental rights, giving users the option to reject these cookies does not reduce the severity of the violation to a legally acceptable level (see section 3.10).

[37] Federal Supreme Court decision 136 II 508, consid. 5.2.4 and 6.3.3.

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

Private controllers in the e-commerce sector use cookies to support a variety of functionalities that help them to conclude or fulfil contracts. These include cookies that remember items selected in an online shopping basket, those that store payment methods, and those that support services such as home deliveries based on address data, none of which are absolutely necessary for technical reasons. In Article 31 paragraph 2 letter a FADP, the legislator has indicated that a private interest may be considered overriding when cookies are used in such ways.

3.8.2 Use of cookies for research and statistics

The grounds for justification of non-personal data processing (e.g. processing for research and statistical purposes) as per Article 31 paragraph 2 letter e FADP are particularly relevant with regard to the use of non-essential cookies. This is because website visitor streams are often analysed using cookies, and it is important for operators to find out how their websites are used and how they can be optimised.

To this end, the legislator has already balanced the competing interests and has defined three prerequisites for affirming that private controllers have an overriding private interest. Accordingly, personal data processing for non-personal statistical purposes is justified if the following three conditions are met:

a. The data are anonymised as soon as the purpose of processing permits. In the context of websites, this usually means immediately. If this is impossible or would require disproportionate effort, appropriate measures must be taken to prevent the data subject from being identifiable.

b. If the matter involves sensitive personal data, the controller shall disclose such data to third parties in such a manner that the data subject is not identifiable; if this is not possible, it must be guaranteed that the third parties only process the data for purposes unrelated to the data subject's person.

c. The results are published in such a manner that data subjects are not identifiable.

By complying with these legal requirements, website operators can justify visitor stream analyses on the basis of overriding private interests. These requirements can also be met when using external analysis tools, provided that the suppliers of these tools process the data only on the website operator's behalf and not for their own purposes.

3.9 Granting the right to reject cookies and default settings under data protection law

In cases where express consent is not required for the use of non-essential cookies, the controller must comply with the legal requirement to enable visitors to reject these cookies (section 3.7.2). This opt-out must be implemented in line with the basic principle of good faith, as stipulated in Article 6 paragraph 2 FADP (see section 3.10.4).

In addition, as the website operator, the controller must ensure, in accordance with Art. 7 para 3 FADP that the use of cookies – until it is actually possible to obtain information about the data processing and exercise the right to object by means of a corresponding button (see section 3.13.2) – is limited to the minimum necessary for the purpose of use (see section 3.13.1).

3.10 Qualified use of cookies

If non-essential cookies are used unexpectedly or in the context of processing operations that involve serious intrusion or high risks to data subjects' personality and fundamental rights, controllers' private interests do not generally override breaches of data subjects' personality rights (see Appendix A for a diagram illustrating the risk levels of cookie usage).

3.10.1 Use of cookies involving a serious intrusion on personality and fundamental rights

Non-essential cookie usage involves severe intrusion if it occurs while processing sensitive personal data as defined in Article 5 letter c FADP or results in high-risk profiling as defined in Article 5 letter g FADP. High-risk profiling links data in such a way that key aspects of a person can be assessed (see section 1.2). For example, collection of geolocalisation data supported by cookies and similar technologies can, depending on the duration of the data collection, lead to high-risk profiling if the collected data alone or in combination with other data and data sources are used to generate precise profiles of the user's movements that allow inferences to be made about key aspects of the user's personality. Practice shows that this result can also be achieved by combining imprecise location data.

Controllers (website operators or any embedded third parties) must assume high-risk profiling if a large number of different data records are included in the profiling and if they cannot rule out the possibility that the result could have serious consequences for data subjects' personality and fundamental rights (see section 3.11.3).

When using non-essential cookies in the context of highly intrusive processing, controllers cannot claim an overriding private interest or rely on providing an option to reject data processing. Instead, they must obtain express consent from data subjects before carrying out the processing (see section 3.12). This applies even in cases where intrusive processing is commonly expected[38].

3.10.2 Unexpected use of cookies

Use of non-essential cookies is to be considered unexpected or unusual if it serves purposes that are in obvious contrast to the purposes of the main personal data processing. One example could be using cookies to link and commercialise visitors' address and telephone data on websites that provide charitable or social services or on certain online gaming websites. If, based on the specific circumstances, it can be assumed that usage of this kind is contrary to the expectations of a significantly high proportion of website visitors, the controllers must make notification of the cookie usage and opt-out feature particularly prominent on the website.

The contrast between purpose and expectation has a more serious impact on data subjects when cookies serving commercial purposes are used on websites with sensitive content of a political[39], trade union or religious nature. Due to the involvement of sensitive personal data, operators of such websites must obtain express consent from data subjects before using cookies in an unexpected way (see section 3.10.1).

3.10.3 Special notification and prominent disclosure obligations

In accordance with the principle of good faith, controllers must notify data subjects in a prominent place on the website of the high level of intrusion or unusual nature of personal data processing or the related use of non-essential cookies. This notice must be positioned separately and must be particularly clear. For example, in the case of qualified processing with a high level of intrusion, it is advisable for an automatic notice (pop-up window) about the particularly intrusive or unusual use of cookies to appear when visitors access the website for the first time, or for the cookie usage to be indicated clearly through a prominent font size or typeface (for technical implementation, see section 3.13).

In the case of qualified cookie usage, controllers are also obliged to follow these requirements when obtaining express consent (opt-in), which is generally mandatory, or when providing the option to reject cookie usage (opt-out), which is sufficient in some cases:

[38] In applications used by transport companies to bill passengers for paid transport services, it is currently common practice to record location data as described above to issue tickets. However, consent obtained for this purpose does not include selling sensitive data to third parties; separate consent would be required for that.

[39] See also the guide of 15 December 2022 by the data protection authorities of the Confederation and the Cantons on the application of data protection laws to the digital processing of personal data in connection with elections and voting in Switzerland: https://www.edoeb.admin.ch/en/guide-to-elections-and-voting

3.10.4 Mechanism for statutory right to reject cookies and opt-out

It may be acceptable to make data processing optional if the unexpected cookie usage does not involve a high level of intrusion (see section 3.10.2, first paragraph). When granting the right to reject qualified cookie usage, controllers must ensure that the opt-out feature is highlighted with a degree of visibility that corresponds to the unusual nature of the cookie usage. This is in addition to data protection-friendly default settings, prominent website placement and a clearly displayed option to refuse cookie usage (see section 3.9). The required degree of visibility is reached when very prominent notices make it impossible for data subjects visiting the website for the first time to ignore the fact that cookies will be used in a qualified way and that they can refuse with just a few clicks.

3.10.5 Mechanism for consent for cookies and opt-in

To justify highly intrusive processing and the associated use of cookies, controllers must obtain express consent from data subjects, as specified in Article 6 paragraph 7 FADP. Letter c of the same paragraph requires federal bodies to obtain express consent even if the cookie usage does not result in profiling that exceeds the high-risk threshold.

To obtain opt-in consent in a legally acceptable way, controllers must require data subjects to actively click on a button or select a box when visiting the website for the first time and before using the web service. Once consent has been given, the website must display a prominent notice to data subjects on each visit, informing them that they can withdraw their consent for the use of these cookies at any time. The page must then direct visitors wishing to withdraw their consent to the relevant button using simple navigation (for the technical implementation of these requirements, see section 3.13).

3.11 **Use of cookies for personalised advertising**

3.11.1 Prevalence of advertising cookies in a commercial processing context

It is common practice and widely known that a large number of private companies in the e-commerce sector use cookies to deliver personalised advertising. As such, this type of use cannot be considered unexpected or unusual in a commercial context. Depending on the circumstances of the specific service, comparable expectations may also exist for free online services such as those that enable users to connect with each other (see section 3.10.2). However, the situation is different if the controller provides third parties with access to personal information in return for payment by means of third-party cookies or similar technologies. If these third parties are embedded in a large number of websites, they are enabled to carry out high-risk profiling (see section 3.11.3).

In the interests of harmonisation and transparency, the advertising industry has standardised the use of consent management platforms (CMPs) to inform users about the collection of their personal data through cookies and the purposes of this processing[40]. While this is a step in the right direction, practice shows that user profiles created from personal data and tracking mechanisms can be sold to various parties. This data can be used for purposes other than targeted advertising, making it difficult to assess the risks associated with this type of practice.[41]

Even if a significantly high proportion of website visitors expect advertising tracking and the controller fulfils their duty to provide information by offering a statutory opt-out option that is sufficiently data protection-friendly (see section 3.9), the controller’s private interest in the use of cookies for online

[40] CMPs enable the management of internet users' consent and offer customisable cookie banners that are designed to clearly explain what data is collected for what purposes (marketing, statistics, etc.) and give users the option to accept or reject these processing operations in detail. This standard is supported in particular by IAB Europe's TCF (Transparency and Consent Framework), which aims to standardise consent management in the digital advertising ecosystem. Thanks to this standardisation through CMPs, online advertising aims to better inform users and guarantee them more compliant and transparent data processing.

[41] Studies have shown, for example, that companies create very detailed profiles in which individuals are even categorised according to sensitive personal characteristics (addictions, mental disorders, political opinions, etc.) and that these profiles are exchanged and sold among numerous players in the data market. This intensive profiling, which is often linked to advertising practices such as real-time bidding (RTB), can lead to an increased risk of manipulation, invasion of privacy and uncontrolled use of data that is beyond the control of the individuals concerned. This raises serious concerns about transparency, data security and the user's actual control over their digital identity.

advertising purposes may not always be overriding. In this respect, it is necessary to distinguish between advertising tracking through 'normal' profiling and advertising tracking through qualified profiling or between medium and high risk (for profiling, see section 1.2, and for a diagram illustrating the risk classifications, see Appendix A).

3.11.2 Advertising tracking through 'normal' profiling

Advertisers use cookies to track website visitors' behaviour and interests. The aim is to present offers in a personalised way or to send personalised advertisements for their own products based on this data. Accordingly, the data collected and the resulting analyses lead to profiling as defined in Article 5 letter f FADP, because specific aspects of the user's personality and consumer behaviour can be inferred.

When using advertising cookies within the limits of 'normal' profiling, private controllers must ensure, as a minimum requirement, that website users can immediately recognise on their first and subsequent visits how to exercise their right to reject cookies (opt-out) with just a few clicks if they search for the relevant 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 as defined in Article 5 letter f FADP. However, it should be noted that federal bodies can act under both public and private law. When advertising cookies are used, the latter is generally likely to be the case, meaning that the FADP provisions on data processing by private individuals apply.

3.11.3 Advertising tracking through high-risk profiling

As explained in section 3.11.1, website operators or third parties embedded in the website use cookies to track visitors' behaviour and interests. The aim is to use this data to enable third parties to place personalised advertising or buy placement of personalised advertisements by auction. In order to create the most comprehensive picture possible of users' consumer behaviour, this kind of tracking is usually carried out via cookies across several websites. This may therefore exceed the threshold of 'normal' profiling, resulting in high-risk profiling as defined in Article 5 letter g FADP.[42] If this threshold is exceeded, controllers must fulfil the notification and prominent disclosure requirements for processing operations that involve a high level of intrusion, as well as meeting the requirements for obtaining consent (see sections 3.10.3 and 3.10.5).

If controllers cannot rule out the possibility that the threshold of 'normal' profiling has been exceeded, due to having not carried out the necessary analyses, they must assume there is a potentially high risk (see section 3.10.1). In its final report of 11 April 2024 on an investigation completed under the old FADP of 19 June 1992, the FDPIC assumed qualified processing as defined by the old legal concept of 'personality profile' under Article 3 letter d old FADP, which in 2020 formed the basis for the new legal concept of 'high-risk profiling' under Article 5 letter g FADP. The investigation was directed against a company that had used cookies to process its customers' usage data on its own platform and linked this with data from other companies in the same consortium in order to analyse user behaviour across all services. When classifying the processing as a 'personality profile', the FDPIC took the following circumstances into account: firstly, the economic stakeholders participating in the tracking were operating in different sectors. Secondly, the personal data in question was collected over a long period of time. Thirdly, publicly available data and data from third-party providers were also used to improve the database[43].

[42] BEAT RUDIN, in: BAERISWYL/PÄRLI/BLONSKI (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Auflage, Art. 5 N 52.

[43] See the FDPIC final report of 11 April 2024 re Ricardo AG and TX Group: https://www.newsd.admin.ch/newsd/message/attachments/90124.pdf

3.12 Legal requirements for obtaining consent and granting the right to withdraw and reject consent

Neither the FADP nor Article 45*c* TCA require that consent be obtained in order for data processing via non-essential cookies to be lawful. The data subject's consent is only one of several grounds for justifying data processing that violates personality rights. These grounds are listed in Article 31 paragraph 1 FADP.

Even in scenarios 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 reasons of practicability, consent is therefore usually obtained by private controllers only when it becomes apparent that the resulting disadvantages for the data subject override the controllers' private interest in the use of non-essential cookies in cases where a mere right to reject them is granted.

3.12.1 Mutatis mutandis application of the provisions on the right to reject cookies

In accordance with Article 6 paragraph 6 FADP, there are two key requirements for valid consent to the use of non-essential cookies or similar technologies: the first is that data subjects must be provided with appropriate information about the data processing in question, and the second is that data subjects must give their consent voluntarily.

The following four rights are related to these requirements: consent to personal data processing, rejection of personal data processing, and withdrawal of consent or rejection. In accordance with the good faith principle, the requirements explained in the following sections on obtaining legally valid consent and granting valid withdrawal of this consent must therefore apply mutatis mutandis to the data subject's right to give and reject consent for cookies (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 to provide appropriate information is intended to ensure that data subjects give their consent in full knowledge of the facts, i.e. that they do not have to make a decision until they have gained an idea of the potential negative consequences of their consent. Ultimately, it is necessary (but also sufficient) that the data subject is clear about what they are consenting to, i.e. what the implications of their decision are.[44] The requirement to provide appropriate information is therefore closely linked to the principle of recognisability and the information obligations under Article 19 FADP (see section 3.3). If the controller wishes to justify data processing that violates personality rights by obtaining the data subject's consent, the requirements for transparency must be set high. This is because, by demanding consent, the controller is transferring part of the responsibility for any violation of personality rights to the data subject. The data subject must therefore be able to understand which data processing will be carried out based on their consent and what the purpose is. Only then can they assess the consequences or risks of data processing in relation to their personality rights and make a legally valid declaration of consent. In application of the proportionality principle, the more sensitive the personal data in question, the clearer the information must be.[45]

The Federal Administrative Court states that, depending on the situation, the information provided must not only specify the circumstances of the data processing, but also the most significant potential risks or consequences for the data subject.[46] This is because the nature of appropriate information depends on the person or group of people who need to be informed.[47] If the target audience of the data processing comprises minors who are capable of judgement and are exercising their right to informational self-determination independently,[48] the processor is expected to use simple and unambiguous language and to specifically point out the potential risks and consequences of the data processing.

---

[44] See Federal Administrative Court decision 2009/44, consid. 4.2.

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

[46] See Federal Administrative Court decision 2009/44, consid. 4.2.

[47] TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, Zurich 2017, N 263.

[48] In the case of children, parents exercise this right on behalf of the children within the scope of their parental custody.

As explained above under section 3.3.2, information about the planned use of cookies must always be provided before the data subject gives their consent.[49]

3.12.3 Specific consent

Consent to the use of non-essential cookies must clearly reflect the data subject's willingness to agree to the data processing after having been informed of it. This expression of willingness must also relate to clear, specific and legitimate data processing.[50] General clause-like declarations of consent or blanket consent are therefore not permitted (e.g. the frequently used phrase "for marketing purposes").[51] If the declaration of consent relates to several different data processing operations and purposes and if different purposes are combined, users must be clearly informed that they have the option of consenting to or rejecting the relevant data processing operations individually. If the website operator obtains consent for processing by embedded third parties, the declaration of consent must also be clear in this regard (see section 3.11.1).

3.12.4 Voluntary consent

Consent must be given voluntarily, as specified in Article 6 paragraph 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.[52] As such, misleading representations and phrasing (known as dark patterns or nudging) may make the consent invalid.[53]

It can be inferred from Federal Supreme Court case law that consent is to be deemed non-voluntary in particular if refusal to give it would result in disadvantages unrelated or disproportionate to the purpose of the data processing.[54] Consent is therefore deemed voluntary if the data subject has a genuine or free choice or can refuse or withdraw consent without suffering disproportionate disadvantages.

In the context of websites, the question of whether consent is voluntary arises in particular if access to the website or a characteristic main service is denied until the data subject has given consent to one or more data processing operations, such as installation of third-party cookies, that are not necessary for the main service. This is particularly common with so-called 'free services', which are partly financed by personalised online advertising. Whether valid consent can be given under these circumstances depends on whether it can be considered reasonable for the data subject to forgo using the main service in each specific case. If it is not reasonable to expect the data subject to forgo using the service, the controller must provide an equivalent alternative so that consent can be considered voluntary. It is less likely to be considered reasonable if the data subject depends on the service and the result would be a lack of alternatives or poor alternatives[55]. It is easier to forgo taking part in a one-off competition than to forgo ordering a product from a dominant online retailer or using an online job site or social network. It should be noted that social networks and online portals are likely to become even more important to participation in social life as digitalisation progresses[56].

With cookie paywalls, data subjects are given the choice of either consenting to all processing by cookies and similar technologies or paying a fixed price (known as pure subscription models) in order to view the website's content. This means that the data subject does not have to forego using the service if they do not give their consent, but they do have to pay an amount of money. Under these circumstances, the voluntary nature of consent to data processing depends on whether the financial contribution is (1) proportionate and (2) does not undermine the data subject's fundamental right to data protection. With

[49] MONIKA PFAFFINGER in: BAERISWYL/PÄRLI/BLONSKI (eds), Stämpflis Handkommentar zum DSG, 2nd ed., Art. 31 DSG N. 33; TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, Zurich 2017, N 252.

[50] Art. 5 para. 4 Council of Europe Convention 108+; Dispatch on the Federal Act on the Total Revision of the Federal Act on Data Protection and the Amendment of Other Data Protection Enactments of 15 September 2017, BBl 2017 6941, p. 7,027.

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

[52] TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, Zurich 2017, N 276 ff.

[53] 'Dark Patterns. Documenting the Unknown'. Federal Council report in response to postulate 22.3190, Michaud Gigon Sophie, 16 March 2022, p. 30 ff. Available at: https://www.newsd.admin.ch/newsd/message/attachments/88176.pdf (de, fr)

[54] Federal Supreme Court decision 138 II 331, consid. 7.4.1.

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

[56] See European Data Protection Board (EDPB), Opinion 08/2024 of 17 April 2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.

regard to compliance with the criterion of proportionality, website operators must ensure that the price they charge is proportionate to the loss of income they incur by not disclosing data to third parties.

3.12.5 Form and mechanism of consent

The FADP does not tie consent to any legal form[57]. However, the mechanism through which it is obtained may be relevant to its validity, e.g. if the controller obtains consent for several data processing operations with different purposes. If different cookie types and functionalities are combined, users must be given the option of individually selecting or deselecting data processing with different purposes. A dialogue box that only allows users to accept everything or to completely forgo viewing the content of the website cannot be regarded as a clear declaration of consent. This is particularly the case when processing operations that can be carried out without the data subject's consent are combined with processing operations that require consent. 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 Article 6 paragraph 7 FADP requires an express declaration or opt-in, controllers must always request active behaviour from data subjects, through which they must demonstrate their express consent. This is not the case when granting rights to reject and withdraw consent, which are options that data subjects can – but do not have to – exercise by actively clicking on buttons or checking boxes (for technical implementation, see section 3.13).

3.12.7 Withdrawal of consent

It must be possible to withdraw consent to the use of non-essential cookies informally and without justification at any time. Website owners must offer website visitors simple options for exercising their right to withdraw consent. If website owners make it more difficult for data subjects to withdraw consent, e.g. by introducing administrative obstacles that require considerably more effort to reject than give consent, this violates the principle of voluntary consent. If controllers require data subjects to deselect a large number of data processing operations in order to withdraw consent, this constitutes an unlawful dark pattern. Furthermore, if the mechanism for withdrawing consent is so complicated that the average user could not be expected to take the time to make a conscious decision, the consent must be deemed invalid.

Similarly, data processing cannot be considered lawful if the controller does not respect the good faith principle when implementing data subjects' statutory right to reject cookies or withdraw their rejection.

3.12.8 Consequences of legal defects when granting the right to consent to and reject cookies

Legal defects for which the controller is solely responsible and that result in data subjects consenting to cookie usage based on a lack of information or willingness or that prevent data subjects from rejecting cookie usage must not have any legal effect to the detriment of the declarants or data subjects affected by the processing.

3.13 Technical implementation

The general and more detailed information obligations for the use of non-essential cookies and the requirements for obtaining consent and granting data subjects the right to withdraw and reject consent have been presented above. The following information is intended to assist website operators in the technical implementation of these data protection requirements, which is largely left unspecified by the Swiss legislator:

3.13.1 Implementation of timing of processing

In order to meet the legal requirements for obtaining consent for cookie usage, websites must be configured in such a way that the data processing in question does not take place until data subjects have had the opportunity to acknowledge it. For example, if cookies are used so that third parties can collect data from visitors and this data processing is based on the data subjects' consent, then the data processing must not be activated by default when the website is accessed. In order to enable prior

[57] In accordance with Article 6 paragraph 7 FADP, however, express consent must be given for processing of sensitive personal data, high-risk profiling by a private individual, or profiling by a federal body.

information, it is recommended for website operators to implement a two-click solution that ensures the JavaScript is not activated until the visitor has been informed and given consent. This applies in particular to the integration of social plug-ins, tracking pixels and other third-party services.

3.13.2 Consent banner

It is common practice to use cookie banners or CMPs in order to implement website visitors' rights to information and self-determination (see section 3.10.3), obtain consent (opt-in) and store permitted cookies or block non-essential cookies following rejection (opt-out).

These banners inform users of the options for activating or deactivating individual aspects and functionalities of a website, enabling them to make informed and self-determined decisions about cookie usage. Users then communicate their decisions to the website operator and any third parties by various means, such as selecting boxes, deselecting boxes that have already been selected, or clicking on the relevant buttons.

When implementing cookie banners to obtain express consent as defined by Article 6 paragraph 7 FADP, controllers must always use buttons or boxes that need to be actively clicked on or selected, enabling users to demonstrate their express consent in a visual manner (see section 3.12.6). If website operators decide to preset specific default processing operations and procedures for which the law does not require express consent[58], they must not make it more complicated to deselect an already checked box than to select that same box.

If website operators decide that the consent banner should display both the data processing operations for which they are obtaining consent and those for which this is not the case, it must be easy for data subjects to recognise which fields are mandatory and which are optional. With regard to the appearance of the consent banner, controllers must also ensure that the use of fonts, images and colours does not lead to confusion, errors or omissions when data subjects exercise their rights of alteration (see section 3.12.4).

[58] In accordance with Art. 6 para. 7 FADP, however, express consent must be given for: a. processing of sensitive personal data; b. high-risk profiling by a private individual; or c. profiling by a federal body.

Appendix A

Risk factors of using cookies		Risk values 1-3
Personal data	No	0
	Yes	1
Technical necessity	Yes	1
	No	2
Expected by users	Yes	1
	No	2.5
Profiling	No	1
	Yes	2
High-risk profiling	Yes	3
Sensitive personal data	No	1
	Yes	3

Rights of configuration of the interested parties	
For risk values 0 – 1 (necessary cookies)	Acceptance or waiver of the entire offer
For risk values 1 - 2.5 (Functional cookies and use of cookies with 'standard' profiling)	Mandatory opt-out
For risk values > 2.5 (qualified use of cookies)	Compulsory opt-in