Factsheet

Planning and justifying online access to personal data

Personal data can be disclosed between authorities in various ways. A distinction can be made between four different forms of disclosure: mandatory disclosure (ex officio or on request), spontaneous disclosure, disclosure on request (at the discretion of the requested authority) and online access (on a self-service basis).[1]
Overall, the chosen form of disclosure must comply with the principle of proportionality. In other words, if disclosure on request is enough to enable the recipient to fulfil its statutory duties, a more extensive form of disclosure, such as online access on a self-service basis, is not permitted.[2]

Online access

Increasingly, federal and cantonal legislators are instructing their authorities to grant other authorities in the same or other sectors online access to selected parts of the data collections that they process.

With online access, several authorities are able use the same IT system and the controller allows third parties access to the data as and when they wish; the controller remains passive, as he does not necessarily know that someone has accessed the data.[3] Even logging access does not change this, as the controller is not aware that data are being disclosed at the time of access. Access based on the principle of self-service can take different technical forms, whereby the legal qualification as "online access" cannot depend on whether the disclosure of the shared personal data takes place via direct access to source systems or via "query platforms", which bring together and visualise data from several source systems.

Planning

As online access can seriously compromise the fundamental rights of data subjects, federal authorities must plan for such access and comply with the requirements of the Federal Act on Data Protection (FADP) in good time when doing so:

- Online access must be formally authorised in primary legislation if sensitive personal data or personal data based on profiling are involved. In other cases, the possibility of online access must at least be mentioned in an ordinance so that the principles of legality and transparency are respected.[4]

[1] See chapter 3.2.4.3, page 24 Legislative guidelines on data protection of the FOJ.

[2] See chapter 3.2.4.3, page 24 Legislative guidelines on data protection of the FOJ.

[3] See chapter 3.1.3, page 16 Legislative guidelines on data protection of the FOJ.

[4] See chapter 3.2.4.3, page 24 Legislative guidelines on data protection of the FOJ.

Feldeggweg 1, 3003 Berne
Phone +41 58 463 74 84, Fax +41 58 465 99 96
www.edoeb.admin.ch

- The principle of legality requires legal rules to be sufficiently specific. They must be formulated so precisely that it is possible for a data subject to recognise which authority may process which categories of data for what purpose (who, what, why). In some cases, the rules must specify the form of processing, especially where online access is permitted.[5]

- It must be clear from the legal provisions that, in line with the principle of proportionality, access by an outside authority will be limited to selected categories of data that are required to support the outside authority in achieving its processing purposes, which must be sufficiently defined. The reason why the other authority requires access must therefore be clear. For example, an authority may access a specific category of data in a third-party system online in order to perform a specific statutory duty. If data are processed to fulfil several statutory duties, the relevant provision must make it clear in the case of each duty who may carry out what processing and how this processing should be carried out[6]. Particular caution is required if the information system being accessed is used for a purpose that is very different from the purpose pursued by the data recipient. The same applies if the data controller and data recipient do not belong to the same public authority and this results in data being released that crosses the boundaries of federal or cantonal jurisdiction. When assessing existing and planning new instances of access, all types of data disclosure must therefore be considered and the various options must be weighed up in accordance with the principles of proportionality and privacy by design.[7]

- In addition, it must be proven in quantitative terms that the granting of online access is appropriate and necessary. This is the case if a disproportionate number of administrative assistance requests on similar or identical grounds would be required if online access were not granted. In addition, the group of persons entitled to access must be limited to those members of the other authority's staff who have the expertise and training to carry out the required duties in accordance with the law.

- A data protection impact assessment must be carried out for projects which, in view of the scope and volume of online data sharing and the sensitive nature of the shared data, could potentially compromise the fundamental rights, privacy and legal protection interests of a large number of people.

Justification

Federal authorities must demonstrate to the political authorities responsible for approving their work in sufficient detail that they have complied with the requirements of the FADP mentioned above.
Any claims that the digitalisation of administrations based on the latest technologies means that online links between authorities are now essential and require neither special justification nor restrictions in terms of purpose or scope are not legally tenable. These unjustified claims conflict with both the principle of proportionality and the obligation of public data controllers to identify risks to the privacy and informational self-determination of data subjects associated with new networks and, where appropriate, to compare them with the risks inherent in existing networks. When planning new networks, fed-

[5] See chapter 3.1.1, Legislative guidelines on data protection of the FOJ.

[6] See chapter 3.1.3, page 16 Legislative guidelines on data protection of the FOJ.

[7] See chapter 2.2.2 of the FOJ's overview of the '4.3 Total revision of the Data Protection Act (FADP) - Overview of the most important changes for the development of the legal basis for data processing by federal bodies'

eral authorities must also pay attention to the principle of legality under data protection law and the strict requirements of legal precedent regarding the specificity of legislation.

New technologies must not lead to the indiscriminate networking of all authorities that overrides jurisdictional boundaries and the material and territorial separation of powers within the state.

18/06/2024