

Installing a chatbot: data protection issues

Question

A service wishes to clarify legal questions about a chatbot project, in particular with regard to data protection and compliance with Swiss law.

Answer

The new data protection legislation imposes a number of specific requirements on federal bodies. Federal bodies can access a range of documents on the [FOJ website](#) containing general and more specific information that can be useful when preparing the legal basis for data processing (see FAQ "Where can I find information on AI on the FOJ website?") These documents can also be useful for projects involving the use of AI systems and the processing of personal data.

The document 'Révision totale de la loi fédérale sur la protection des données (LPD) - Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux' on the FOJ's website describes specific developments in AI within the Federal Administration (pp. 18)

It may be useful to carry out an impact assessment for the protection of personal data. You can find more information on this subject on the [FOJ website](#).

Installing a chatbot: principle of good faith

Question

A service wishes to clarify legal questions about a chatbot project, in particular about the possibility of adding a disclaimer on the lack of reliability of chatbot answers.

Answer

It is important to consider whether the inclusion of a disclaimer about lack of reliability complies with Article 9 of the Federal Constitution ("Protection against arbitrary conduct and principle of good faith"). According to doctrine and case law, this safeguard generally confers the right not to suffer any disadvantage (or prejudice) as a result of the conduct of a public authority which is contrary to the rules of good faith. The French-language commentary cites the example of inaccurate information concerning rights of appeal: an appeal that is wrongly addressed or arrives late must be declared admissible if the defendant relied on the information and did not notice – and could not reasonably be expected to have noticed – the mistake despite giving it the attention required by the circumstances. If the information provided by the chatbot is grossly inaccurate, there should be no negative consequences for the defendant. However, seemingly plausible information could conceivably lead a citizen to behave in a certain way (e.g. incorrect deadline information). In such a case, the authority should take this into account to ensure that the citizen is not disadvantaged. The warning to users about the lack of reliability of the information provided by the chatbot must always be clearly visible and feature prominently on the website, so that citizens are aware that reliable information can only be obtained through another channel.

Robot as IT user

Question

A service wishes to know whether and under what conditions a "robot" could have access rights to a system and carry out transactions as a user. More specifically, the following questions are raised:

- General legal context: Is there legislation covering the use of robots as IT users in the public administration?
- Legal responsibility and compliance: What compliance and accountability issues should we consider when using robots in this context?
- Data protection: What are the potential implications on data protection and how should we deal with them?
- Practical recommendations: What recommendations or good practice can be followed to ensure that robots are integrated legally and ethically?

Answer

General legal context: We are not aware of any specific legislation covering the use of robots as IT users. However, the relevant legal principles of Swiss law are applicable to such a situation, in accordance with the technology-neutral approach adopted by the Swiss legislator. Any use is subject to the provisions of the Federal Constitution, the Federal Act on Data Protection (FADP), the Administrative Procedure Act (APA), the Swiss Code of Obligations (CO), the Civil Code (CC), the Swiss Criminal Code (SCC), the Government Liability Act ([GLA](#)) and the Federal Act on Product Safety.

Responsibility and compliance: The legal bases cited above are also relevant to responsibility and compliance.

Data protection: If the robot is an AI system and involves processing of personal data, the use of the system should undergo an impact assessment under the FADP if it is likely to pose a high risk to the fundamental rights of the persons concerned. Furthermore, if the use of the AI system leads to an automated individual decision, this must comply with the rights and obligations under Art. 21 and 25 para. 2 let. f FADP. The use must comply with the statutory basis requirements under Art. 34 FADP. Please refer to the various documents available on the FOJ website regarding data protection and AI systems. <https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html>

Practical recommendations:

- Fully automated machine-generated decisions need to be reviewed by a human. Staff using these systems must be trained to understand the overall functioning of the system, enabling them to question the results proposed by the machine.
- If the system is authorised to make decisions, the interaction with an AI system and the decisions taken must be clearly identified as such.
- To foster transparency, the AI project can be announced to the Confederation's AI Competence Network for inclusion in the federal database of AI projects.
- The [Confederation's guidelines](#) on AI should be observed.

Transcription of minutes by a robot

Question

Is there a legal requirement that minutes taken in the context of proceedings before administrative bodies must be written by a human being, or would it be possible from a legal point of view in the future for the entire transcription to be done by an AI system?

Answer

A complete digital recording of a hearing is no substitute for written minutes. To respect the person's right to be heard ([Art. 29, para. 2, Cst.](#)), the written minutes must contain the key elements for the continuation of the proceedings. However, there is no constitutional obligation to add a full copy of the hearing to the file. Minutes limited to the key elements of the hearing are sufficient.

There are certain software solutions that automatically transcribe audio files using an AI system. In principle, the administration can use such transcription software – as a tool, as mentioned above. However, the administration using this software is obliged to check the quality of the transcription. This also applies to a complete and word-for-word transcription. It is necessary to check that the words used have been transcribed correctly and that non-verbal communication has been taken into account. The person checking the transcription must have attended the hearing. The authority is responsible – even if it uses transcription software as an aid – for ensuring that (at least) the key elements for the continuation of the proceedings are recorded. In accordance with procedural law, the authority is responsible for establishing the facts ([Art. 12 APA](#)). If the transcription software is used in this sense, the state's action complies with the law and there is therefore no legal objection.

In conclusion, the writing of minutes cannot be 'entirely' entrusted to an AI system. However, the administration can use a software solution as a tool, provided that someone who attended the hearing checks the quality of the transcription. Other conditions of administrative procedure apply, in particular the right to be heard of the person concerned.

Where can I find relevant information on AI on the FOJ website?

- www.bj.admin.ch > State & Citizen > Data protection > Questions et réponses concernant la protection des données
 - [FAQ Droit de la protection des données](#) : Décision individuelle automatisée, ch. 6.2 / Profilage, ch. 2.3 / Analyse d'impact relative à la protection des données, ch. 6.3
- www.bj.admin.ch > State & Citizen > Data protection > Informations destinées aux organes fédéraux
 - [Révision totale de la loi fédérale sur la protection des données \(LPD\) - Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux](#) : Décisions individuelles automatisées, ch. 2.2.1 let. c (avec des développements spécifiques sur l'IA) / Profilage, ch. 2.2.1 let. b / Analyse d'impact relative à la protection des données, ch. 4.3
 - [Guide de législation en matière de protection des données](#) : Décision individuelle automatisée : ch. 2.3.4 et 3.2.3 / Soutien automatisé à la prise de décision individuelle grâce à des systèmes d'algorithmes, ch. 2.3.5 et 3.2.3 / Profilage, ch. 2.3.3 et 3.2.2
 - [Instrument d'examen préalable des risques](#) (tableau excel)
 - [Guide AIPD](#), pp. 3 and 17