Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

18 January 2024 V1.2[1]

Fact sheet on the use of generative AI tools in the Federal Administration

Reference: 822.1-1/8/5/1

What are generative AI tools?

Tools available on the internet with generative artificial intelligence (AI)[2] - for example ChatGPT from OpenAI, Copilot from Microsoft, Bard from Google, Grok from X and many more - simplify a range of tasks that are also part of the work content of many employees in the administration. They enable users, for example, to ask the AI tools for an opinion on an existing text[3] or to request them to create a new text on a specific topic.

These tools are not "intelligent"; For example, in the case of text generation, they only calculate the statistical probability of the word sequence - in other words, they are *next token prediction systems* - but nevertheless often deliver astonishing results. They are fed large amounts of data, whose sources are often not disclosed. The probabilities calculated on this basis may therefore be outdated, misleading, discriminatory or simply incorrect. Input from users (known as *prompts*) may also be used to further train the AI system, i.e. they can be incorporated into other conversations. Data are usually stored outside Switzerland.

Responsible experimentation? Yes!

Generative AI tools can help you with your daily work in the administration. Try it out, learn something new! With a little creativity, you can contribute to an innovative administration. However, do be cautious and follow the rules in force.

➔ Possible areas of use: Summarise lengthy publicly available texts, get tips for the structure of your next presentation, get inspired by programming code suggestions for your work or take a quick and light-hearted dive into a new topic by entering into a dialogue with the tool – find out where it can help you most.

➔ You can enrol for professional purposes using your work email address. Choose a strong password that you use only for this service.

Test the answers from the generative AI tool by giving different prompts and develop an effective prompting technique.

Infringe existing regulations? No!

➔ Be careful when entering information:

Never enter personal data or sensitive information into these tools!

- Do not enter information classified as internal, confidential or secret[4];

[1] This fact sheet is regularly reviewed to take account of new developments and a better understanding of the application cases of generative AI tools in the Federal Administration.

[2] For general terminology see https://cnai.swiss/en/products/terminology/ and https://www.bfs.admin.ch/bfs/en/home/statistics/prices.assetdetail.29325686.html (Chapter 3.3) - "Generative AI" is a broad term that refers to AI systems that are trained on large amounts of data from the real and virtual world in order to generate data themselves (e.g. texts, imagery, sound recordings, videos, simulations, and codes). They are often multimodal, e.g. with input and/or output in on or several modalities (e.g. text, image or video).

[3] In addition, there are AI tools that can generate images, sound recordings, videos, simulations or codes.

[4] See Art. 13 ISG (SR 128) and Art. 18 ff. ISV (SR 128.1)

- do not enter texts that although not classified still contain sensitive information, for example because they are protected by data secrecy (official secrecy, special (professional) secrets, contractually protected information)[5];
  Caution is advised when entering images, private photos, sound recordings, videos, simulations and code;
- Do not enter personal data[6] of any kind. In the case of anonymised or pseudonymised entries, ensure conclusions cannot be drawn about the person concerned on the basis of additional information (for example, the name has been changed, but the person in question can be identified relatively easily based on the date of birth, gender and place of residence).

If you are unsure whether the information and data you wish to use qualify as confidential, do not enter them and refrain from using generative AI tools. Information that has already been published publicly (on the internet), such as Open Government Data (OGD) may be used.[7]

➔ Take care when (re-)using the results:

Generative AI tools deliver results of varying quality. Always check the results of the tools with a critical eye for accuracy and completeness and compare them with other sources. **Responsibility for the results used remains with you and cannot be delegated to the generative AI tools.**

You must be able to justify at all times any decisions made on the basis of results from generative AI tools. In particular, affected persons have the right to be informed about a decision based solely on automated processing and which has legal consequences for them or a significantly negative impact on them (automated individual decision-making).[8]

Where appropriate, clearly indicate that you have used AI tools. Pay attention to the instructions for use of the selected generative AI, as these sometimes contain information on the further use of contents (copyright).

➔ Beware of security:

Due to security requirements, certain ICT applications (and in particular email login services) are blocked within the Federal Administration and their display depends on the internet browser. **Comply with IT and cyber security regulations at all times.**

[5] For official secrecy, see Art. 320 SCC (SR 311.0); Professional secrets are, for example, medical confidentiality or tax secrecy; contractual non-disclosure agreements must also be respected.

[6] Any information relating to an identified or identifiable natural person (Art. 5 let. a FADP [SR 235.1]); see also the FDPIC news in brief.

[7] See Art. 10 EMOTA (BBl 2023 787)

[8] Art. 21 FADP (SR 235.1). See the FOJ's FAQ on the total revision of the FADP (Sections 6.2.1 and 6.2.2) for the term "automated individual decision making" and the further claims of the person affected by an automated individual decision.

Examples for the use of generative AI tools

Generative AI tool allowed 👍	Generative AI tool prohibited 🚫
Summarise published texts (e.g. reports).	Summarise documents of the joint reporting procedure (→ not public; Documents possibly classified.
As an introduction to a new topic (similar to Google / Wikipedia)	Translate CVs (→ Personal data)
Support in formulating slide sets	Enter specific enquiry from Mr Hans Muster unchanged (→ personal data)
Inspiration for code generation	Use the results *verbatim* (→ without checking)
Create images for presentations	Enter existing software code for debugging (→ copyright infringement)

To answer your questions:

- on AI in the Federal Administration: AI working group and competence hubs in the Competence Network for AI (CNAI)
- on information security and data protection: the IT security officials and data protection advisors of your administrative unit
- For user support: IT service you trust or RoBIT (AI ChatBot of the FOITT)
- For specific services in the field of data science and AI: DSCC

Further information:

Guidelines on AI for the Federal Administration

The seven guidelines on AI for the federal administration continue to apply: Put people first, ensure regulatory conditions for the development and application of AI, demand transparency, traceability and explainability, clearly define accountability, guarantee safety, actively shape AI governance, involving all relevant national and international stakeholders in the process.

Federal Administration's code of practice for human-centric and trustworthy data science (and AI)

The Code of practice provides the federal government's administrative units with guidance and practical explanations to raise awareness of the core principles of human-centric and trustworthy data science (and AI) and enables them to implement these principles in everyday work. The core principles are: Data and information protection, information security, data security, data governance, non-discrimination, explainability, traceability, transparency, reproducibility, neutrality, objectivity and ethical handling of data and results.

This fact sheet was drafted in the "AI in the Federal Administration" working group in the CNAI with the cooperation of representatives from all departments and the FCh.