Data protection

Artificial intelligence is changing the way we work, communicate and search for information. Generative AI tools, such as chatbots or text and image creation systems, bring tremendous opportunities – but only if we treat them with caution.

Generative AI models can be trained, among other things, on the data fed into them by their users. Therefore, they are not usually designed to ensure the confidentiality of these data or protect information that is shared with chatbots and other tools.
Keep in mind that most commonly available chatbots use the data you input into AI tools to further train AI models. This data also leaves your device and is processed on the operator's servers.

Therefore, do not input sensitive data, personal data or internal data of the Uni-versity into commonly available chatbots.

You may only input these protected and internal data into Microsoft Copilot un-der a university licence or, in specific cases, into locally operated models.

Protected, internal and public data

Why do we need to think about data protection?

From the point of view of legal and ethical responsibility, it must be borne in mind that some data are subject to special protection; according to legislation (e.g. GDPR), personal and sensitive data in particular should not be inputted into generative AI tools.

Chatbots usually function as cloud services, which means that the information entered in them leaves the user’s device and is processed on the operator’s servers. The inputting of any personal data (e.g. name, address, voice recording or IP address) into these systems without the express consent of the persons concerned is contrary to the GDPR.

This covers not only the direct inputting of data into the chatbot, but any form of provision of data to AI tools. If we give an AI tool access to sensitive data, this is, from a risk point of view, essentially the same as inputting the data directly into chat.

The granting of broad authorisation to AI tools (access to disks, e-mails and re-positories) is very risky and not recommended.

In addition, most publicly available chatbots and generative AI tools use embed-ded data as standard for further model training. This poses a significant risk not only from the point of view of personal data protection, but also when working with information that is protected by copyright, trade secrets or contractual confidentiality.

For example, if we insert a piece of text from non-public research, student work, or licensed material into a tool, the system may “remember” this information and fragments of it may later appear in outputs provided to other users. In addition, the AI tool provider itself gains access to the data, which can continue to be used without your knowledge.

This may not only violate the confidentiality of the input data, but also uninten-tionally leak protected content. Therefore, it is necessary to carefully consider what we put into AI systems and, whenever possible, work with anonymised or publicly available sources.

Even if the AI tool operator does not use the data for training or other own purposes, there is still a risk of data loss or misuse due to a security incident (e.g. hacker attack, configuration errors, backup leakage). The infrastructure for the functioning of AI tools is usually very extensive and involves a large number of subcontractors, which significantly increases the risk of such a leakage.

Therefore, when sharing data with AI tools, we must always assume that a leak-age of those data may occur. It is important to carefully consider whether such a risk is acceptable.

What is protected data?
Personal information
Any information that facilitates the direct or indirect identification of a specific natural person is considered personal data under the General Data Protection Regulation (GDPR) and Act no. 110/2019 Coll., on the processing of personal data.

During their studies, students may often work with personal data in connection with questionnaire surveys, interviews, recordings or when working with medi-cal documentation. In addition to typical examples of personal data, such as human identification data (e.g. personal numbers/other identification numbers for foreigners, name and surname, date of birth, address), these may also include data that may not be so obvious at first glance, e.g. voice recordings, X-rays or IP addresses.

Materials containing personal data can be anonymised or reformulated before being inputted into the generative AI tool. In practice this means, for example, deleting names, any identifying numbers, addresses, etc.

The so-called special categories of personal data, which include information on racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership, genetic and biometric data, and data on health or sex-ual life or sexual orientation, are subject to a special level of protection.

Therefore, the basic rule is that users are not permitted to enter personal data into chatbots and other AI tools unless they have explicit consent from the per-sons to whom the personal data relates. Such use carries with it a risk not only of interference with the subjects’ private lives, but also of possible misuse of personal data by the provider of the tool. At the same time, it also constitutes processing of personal data, which must be compliant with the GDPR.

Some external generative AI tools – especially paid versions – offer users the option of turning off the use of inputted data for further training of the model. Although we recommend always activating this function if it is available, it should be noted that even in this case, the data leaves the user's computer and is processed on the servers of the service provider.

For this reason, we do not recommend inputting sensitive information or per-sonal data, even into chatbots where such training is deactivated, unless data protection is covered by contract.

Copyrighted data

Data that are the unique result of the creative activity of a natural person (i.e. a person, not a legal entity or a generative AI tool) are protected by copyright as copyrighted works under Act no. 121/2000 Coll. (the Copyright Act). The range of copyrighted works that can be created is a broad one, and may include, for example, literary, photographic, artistic or cartographic works. Software and its source code are also protected by copyright.

It should be borne in mind that the very inputting of a copyrighted work into a generative AI tool constitutes use of a work. It is necessary to have a licence (au-thorisation from the author or copyright holder) for such use of the work, or be able to invoke an exemption to copyright law, e.g. free use of the work for per-sonal use. In addition, it is also necessary to pay attention to the conditions of use of the AI tool, including whether the generative AI tool is trained on user prompts.

In the case of generative AI outputs, users must bear in mind that outputs may contain parts of third-party copyright works, the publication of which through academic outputs could constitute the use of a work for which it is necessary to obtain a licence from the author. This also applies to situations where genera-tive AI tools are used to modify a work, such as an image, as this creates what is known as a derived work.

In the event that the work is then used without a licence and at the same time none of the exemptions to copyright law (e.g. a citation licence) applies, this constitutes a breach of the rights of the author of the original work. The author subsequently will then have the right to a legal claim for remediation and the provision of adequate compensation for damage caused.

Other sensitive data

If, when creating academic outputs at the University, a student has a relationship with an entity (e.g. an employment relationship with a commercial business or a state institution) and the data of this entity is being utilised, it must also be borne in mind that those data may be highly valuable to that entity.

Typically, these could be data covered by the confidentiality obligation laid out in their contract (employment contract, agreement on work performed outside the employment relationship, cooperation agreement, etc.), data constituting a trade secret or data that is defined as classified information under Act no. 412/2005 Coll., on the protection of classified information and security capability.

Inputting such data into generative AI tools could result in their disclosure, which could have serious consequences for the entity. When using such data, it is therefore advisable, in all cases, to consult the entity first before processing data through generative AI tools.

Microsoft Copilot

Microsoft Copilot is an AI tool that is available to all CU students and employees in the form of a web chatbot.

Users who are logged in to Microsoft Copilot have several advantages. Copilot is a more powerful model that offers the possibility of longer conversations.
However, its fundamental advantage lies in its increased degree of data protec-tion. When you log in with a student or employee account, Copilot pro-vides commercial data protection – meaning that your data is better protected and protected by contract.

Like any tool, MS Copilot cannot be considered 100% secure. The options for controlling what actually happens to data throughout the infrastructure are very limited, and even this infrastructure can be hacked and data stolen. However, unlike commonly and freely available chatbots, with MS Copilot, data pro-tection measures are in place and data is contractually protected.

Enhanced data protection only applies to the Copilot version used under the University's account. It is not to be confused with the public version of Copilot, which is available free of charge. Users must always log in to MS Copilot Chat with their university account.

Log in here.

How to log in and more information here.

Local models

Local generative AI models are models that run directly on the user's device – for example, on their personal computer or on the institution's secure server – and do not communicate with external cloud services. As a result, no data is sent or stored outside the user's environment, which significantly reduces the risk of the leakage or misuse of information.

For this reason, sensitive or internal data (e.g. research results, student work or personal data) can also be entered into these models, subject to appropriate security measures, which is usually undesirable or unacceptable for publicly available online tools.

Assessing whether the environment in which the local model is operated is truly secure requires expertise. It is recommended to use only local models and environments that are officially verified and approved.

Five principles for working with AI tools

Do not input personal, sensitive, internal, or otherwise protected data into regular chatbots.

This avoids the risk that your data will be used to train other models or that it will be leaked or misused.

Use Generative AI tools that are recommended by the University or your faculty.

These tools have contractual data protection measures in place.

Anonymise your data where possible.

The most secure way of working with any chatbot is to anonymise the data you enter into it. In practice this means, for example, deleting names, personal numbers and addresses.

Share with AI tools only the minimum necessary data for any given task.

There is a difference between entrusting a tool with one specific file or granting it access to entire drives.

Do not trust AI tools with highly sensitive data that you cannot afford to have leaked or misused at any cost.

No AI tool is completely without risk..

Now that you know the basic principles of data protection, you can start prompting and experimenting with artificial intelligence.

Charles University supports the use of generative artificial intelligence tools by students, provided that the use of AI is transparent and in accordance with the law of the Czech Republic and the regulations of Charles University or its units.

Check out the tools available at the University, read the initial prompting advice, or contact us if you have any further questions.

AI tools at CUNI

Recommendations from Charles University's management for the safe use of AI tools

Get in touch with us