GPT@EC AT THE EDPS

DATA PROTECTION NOTICE

This data protection notice provides information regarding processing of personal data related to the use by the European Data Protection Supervisor's (EDPS) staff of GPT@EC, which is a general-purpose generative AI service managed by the European Commission (EC) that is available to the EDPS staff.

Personal data is processed in accordance with Regulation (EU) 2018/1725 (hereinafter 'the Regulation').

We provide you with the information that follows based on Articles 15 and 16 of the Regulation.

Who is the controller?
The controller is the European Data Protection Supervisor (EDPS).

Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
Telephone: +32 2 283 19 00
Email: edps@edps.europa.eu

Delegated controller: Secretary-General
EDPS-Secretary-General@edps.europa.eu

Contact form for enquiries on processing of personal data to be preferably used: https://www.edps.europa.eu/about-edps/contact_en.

For more information on the EDPS please consult our website: https://edps.europa.eu.

The EDPS is controller for the personal data it processes in the exercise of its tasks when using GPT@EC. More specifically, the EDPS acts as controller for the purpose of enabling the corporate use of the Large Language Models (LLMs) by the authenticated users of the EDPS by means of their input (text prompts and tools to contextualise the prompts such as the retrieval augmented generation (RAG) functionality) and the use of the generated responses by the LLMs (output).

The EDPS is also controller regarding instructions given to its staff on the use of GPT@EC as defined in the EDPS Guidelines for use of AI tools by EDPS staff ('EDPS AI Guidelines').

EDPS staff can use GPT@EC in all EDPS activities, including supervisory, enforcement, investigative, audit, advisory, policy, and administrative tasks, subject to the rules included in the EDPS AI Guidelines and the safeguards applied in relation to specific processing activities (included in specific records and data protection notices available in the EDPS register).

Particular processing activities, under the remit of EDPS units and services, are covered by specific records, available in the EDPS register.

The EDPS has acquired access to the EC's GPT@EC tool on the basis of a Service Level Agreement.

The **EC DG for Digital Services (DIGIT)** independently determines the purposes and essential means of data processing, acting as a separate data controller for the activities outlined in the EC record on GPT@EC (25348).

The EC DIGIT is also a separate controller regarding EU-Login. For more information, see EC record 03187 and the EU-login privacy statement.

Contact: DIGIT-DATA-PROTECTION-COORDINATOR@ec.europa.eu

Who is/are the processors?
The **EC DIGIT** is a processor for enabling the EDPS staff to use GPT@EC.

Microsoft Azure OpenAI (Azure) – cloud provider Azure is used to call the OpenAI LLM services hosted in its infrastructure.

Mistral AI – providing Mistral AI LLM products hosted in its infrastructure.

Amazon Web Services (AWS) – cloud provider.

What personal data do we process and who has access to this personal data?

Personal data processed:
- personal data related to EDPS staff, which includes:
1. Personal data related with the **user access of the system**: this includes EU Login personal data used for authentication (the relevant EC record is EC record 03187, and the personal data processed are normally the username and e-mail address) and the IAMS - EU Access- personal data used for authorisation (the relevant EC record is EC record 08606 and the personal data processed are normally the username, the email address and the organisational data of the user such as source organisation, department and employee type).

2. Personal data for:
a. **functional cybersecurity and security monitoring**: this processing aligns with record of processing on IT security operations and services: see EC record 02886 and, for instance, the personal data processed can be IP addresses, MAC addresses and IT asset inventory information of corporate devices).

b. **audit purposes**: the personal data collected for this purpose is as follows: for every interaction of an end-user with the tool the tool collects: the end-user's organisational information (i.e. EDPS, employee type), the end-user's user id and email address, the IP address that the end-user used to connect, the AI model used, and all the 'chat' details (such as the user's input prompt and the model's response, as well as the analysis result from the AI Safety Scanner AISS); all these 'chat' details are encrypted and not accessible in the clear to anyone, not even to system administrators.

The AISS is an on-premises GPT@EC component that has been designed to detect abusive or inappropriate content and is used for all user interactions in the tool. It monitors both incoming and outgoing data to and from any of the models, using algorithms to identify suspicious activities, offensive language, or harmful behaviour. All data related to user interactions with the tool (user input, model response, AISS scan details), are processed on-the-fly for this purpose.

The AISS is also used for models running in the cloud on GPT@EC. This is because the cloud provider's abuse-monitoring feature that could scan user content has been disabled. As a result, neither inputs nor outputs are stored in the cloud, and the cloud service providers are contractually restricted from accessing or viewing prompts or generated responses.

c. **user consumption, billing and reporting purposes**: this keeps track of the service consumption; The personal data collected includes the organisational information the user belongs to, the number of tokens sent by the user as input and the number of tokens received by the user as output. In addition, for reporting purposes also the controller processes the time log of when the user accepts of Terms of Use and the users' utilisation of the corporate prompt templates.

3. **Personal data** related with the **user interactions with the system**. This includes the personal data that follows:

a. Personal data **related with the datasets used as part of the input**: This may include personal data included in the documents/datasets that the user attaches to its prompts with the purpose to contextualise its prompts by means of the RAG functionality of the tool. The data in the attachments may include, amongst others, name, surname, email.

b. Personal data **related with the output**: This might include personal data in the

generated response of the LLM based on the user input and/or, if applicable and hypothetically, on the datasets used to pre-train the LLM by the LLM's provider. The data in the attachments may include, amongst others, name, surname, email.

c. **The AI safety-monitoring functionality**, the AI Safety Scanner (AISS), scans the interaction of the user with the system (both the input and output traffic within GPT@EC) to recognise and neutralise harmful content within the user interactions.

4. **Handling the prompt library** to manage and access **favourite prompts** and to use the corporate prompt templates. This refers to the corporate templates only, no to the users' prompts. The personal data handle here are the marking of a certain corporate prompt template as favourite by the user.

5. **Handling of user's feedback**: this includes the personal data shared by the user with the GPT@EC support team with the purpose to handle the feedback. The category of personal data is this described in the ITSM (IT Service Management) EC record 18469, this data includes, for instance: name and surname as well as the feedback shared by the user and the personal data collected is the data shared by the user by email.

Access to personal data:
Access to personal data is provided to the EC staff responsible for carrying out this processing operation and to authorised staff according to the 'need to know' principle. Such staff abide by statutory, and when required, additional confidentiality agreements. In the context of investigations of security incidents, the data could be transferred and further processed following as described in the EC record 02886 on DIGIT IT security operations and services.

GPT@EC LLMs are hosted on-premises (i.e. EC servers) or on Azure or AWS cloud.
The information will be sent to the respective 'processor' entity (e.g. Azure cloud, DIGIT data center) depending on the user's LLM choice. This information is only processed in memory by the respective LLM application with no data storage in the processor entity. Hence, the information is not accessible to these entities for their independent use.
Logs are stored on GPT@EC back end, that runs on a DIGIT data center cluster.

In case of official investigations, the EC may provide technical support to, and as requested by the EDPS competent authorities. Such processing activities are not the subject of this personal data protection record. For more information on the specific EDPS processing activities in scope, you can refer to the EDPS register.

Other possible recipients:
- Bodies charged with a monitoring or inspection task under EU law, where required for official investigations or for audit purposes (e.g. European Ombudsman, the EDPS, as data protection supervisory authority)

- The Court of Justice of the European Union, where applicable
- Where applicable, citizens in the context of requests for access to documents, in accordance with the Regulation (EC) 1049/2001

Where did we get your personal data?
In order to provide access to GPT@EC, the EDPS transmitted identification data of its staff (e.g. name, email address, organisation) to the EC.

Personal data of EDPS staff members is also processed by the EC while GPT@EC is used, as defined by the EC (see categories of personal data processed).

In case personal data is included in prompts this is collected from the user who included the prompt in GPT@EC.

Why do we process your personal data and under what legal basis?

Purpose of the processing
GPT@EC is strictly for professional use. It supports EDPS staff in daily tasks including drafting briefings, summarising documents or surveys, improving the grammar, style, or tone of written texts, assisting with the development of computer code, or producing images and videos.

GPT@EC can be used by EDPS staff to support work-related tasks in all EDPS activities, including supervisory, enforcement, investigative, audit, advisory, policy, and administrative tasks, subject to the rules included in the EDPS AI Guidelines.

When used appropriately, AI systems have the potential to enhance efficiency, support more sophisticated analytical work, and improve the overall quality of outputs.

All EDPS units and services can process personal data within GPT@EC in order to perform their tasks in view of the EDPS' mandate and tasks. In case GPT@EC is used by staff to perform their work-related tasks, processing of personal data will be in relation to the processing activities included in the EDPS register.

Processing of personal data can occur as a result of the prompts included in GPT@EC by EDPS staff. Before including personal data in prompts, EDPS staff must adhere to the provisions of the Regulation, and observe, in particular, lawfulness of processing, data minimisation, and the accuracy of input data.

GPT@EC can support EDPS staff with specific tasks, but do not replace, human judgment or decision-making. EDPS staff must always review GPT@EC generated content intended for work-related tasks prior to utilisation.

Personal data processed included in prompts by EDPS staff is not used to train or improve AI models.

The EDPS can also request some information from the EC in order to investigate security incidents as well as to conduct administrative enquiries and disciplinary proceedings (see specific processing activity in the EDPS register).

The EC processes personal data for the following purposes (according to the EC record):
- authenticating and authorising secure users access to the system through registration and EU Login
- ensuring logging and monitoring of use for cybersecurity purposes
- ensuring logging and monitoring for billing purposes to keep track of the service consumption by individual users and groups of users, to allow cross-charging
- setting up an AI safety monitoring component (AI Guardrails solution for AI safety) to detect and mitigate abusive or inappropriate use of the GPT@EC. This component monitors both ingress and egress flows to the LLMs
- handling the prompt library to manage and access favourite prompts and to use the corporate prompt templates
- handling of end-users feedback on any topic, for instance personal opinion of the user on the tool or reporting a bug

Neither the input nor the output will be used for fine-tuning or re-training LLMs.

Legal basis
As a rule, lawfulness is based on Art. 5(1)(a) of the Regulation: '*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body.*' Article 5(1)(a) is interpreted in the light of Recital 22 of the Regulation, since it is necessary for the performance of tasks carried out in the public interest by the EDPS.

Lawfulness would also depend on the specific processing activity for which personal data is processed within GPT@EC, as set out in the relevant records and DPNs covering those particular processing activities.

How long do we keep your personal data?
EDPS staff using GPT@EC can decide to delete chat history (input and generated output) at all times. Conversely, GPT@EC enables users to save the chat history, so that they can check them again at a later stage or continue the conversation. Chats with the sensitivity level 'Sensitive non-classified' are never saved in the chat history.

The **EC**, as controller, applies the following retention periods:
1. **user authentication and authorisation data** by means of EU Login and EU access: 6 months from the moment the logs are captured.

2. personal data contained in the **log files** required for functional, cybersecurity, security monitoring to respond to security incidents and for audit purposes: 1 year from the moment the logs are captured. In the context of investigations of security incidents, log files could be further processed following EC record 02886 on DIGIT IT security operations and services, where a different retention period applies.
3. personal data for **billing and reporting purposes** to keep track of service consumption: 2 years.
4. **user interactions** (user input and model output), including data processed in order to perform the abuse monitoring through the AI Safety Scanner (AISS scan details) are processed on-the-fly and do not persist by the system in any way for this purpose. Nevertheless, the user may decide to keep their interaction with the tool in their 'chat' history, in which case they decide themselves until when they want to keep their input and the corresponding model response. In the case of user inactivity (defined as the user not having logged into the system for over 6 months), there is an automatic deactivation of the user and subsequent deletion of their chat history.
5. Personal data handled as part of the **prompt library**, specifically the marking of a certain corporate prompt templates as favourites by the user, is kept either until the user decides themselves to unfavourite the prompt, or in the case of user inactivity (defined as the user not having logged into the system for over 6 months), there is an automatic deactivation of the user and subsequent deletion of their chat history.
6. Personal data processed when handling **user feedback** at the ITMS are kept for 24 months.

What are your rights regarding your personal data?
You have the right to request access to your personal data and to relevant information concerning how we use it. You have the right to request rectification of your personal data. You have the right to ask for the erasure of your personal data or to restrict its processing. Where applicable, you have the right to object to the processing of your personal data, on grounds relating to your particular situation, at any time.

Please note that, in certain cases, as provided in Article 25 of the Regulation, restrictions of data subjects' rights may apply.

We will consider your request, take a decision and communicate it to you. The time limit for treating your request is one (1) month. This period may be extended by two (2) further months where necessary, taking into account the complexity and the number of the requests. In those cases, the EDPS will inform you of the extension within one (1) month of receipt of your request and will provide reasons for the delay.

You can send your request to the EDPS electronically or by post (see section on contact details below).

Is personal data subject to automated decision-making?
The EDPS prohibits using GPT@EC to make decisions that would subject individuals to outcomes based solely on automated processing, including profiling, where those decisions produce legal effects for them or similarly significantly affect them.

You have the right to lodge a complaint
If you have any remarks or complaints regarding the way EDPS processes your personal data, we invite you to contact the delegated controller or the EDPS DPO (see section on contact details on the first page and below).

You have, in any case, the right to lodge a complaint with the EDPS as a supervisory authority: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

Contact details for enquiries regarding your personal data
We encourage you to contact us using the EDPS contact form, selecting 'My personal data' as the relevant subject: https://edps.europa.eu/about-edps/contact_en.

If you wish to contact the EDPS DPO personally, you can send an e-mail to DPO@edps.europa.eu or a letter to the EDPS postal address marked for the attention of the EDPS DPO.

EDPS postal address: European Data Protection Supervisor, Rue Wiertz 60, B-1047 Brussels, Belgium

You can also find contact information on the EDPS website: https://edps.europa.eu/about-edps/contact_en.