AI Safe Compliance Report

1-31 December 2024
126 Active Users, France

Table of Contents

Report Summary

This report focuses on how Maya Data Privacy's "AI Safe" Product enables customers to connect with external LLMs like ChatGPT while ensuring compliance with the EU GDPR and AI Act.

The product offers two levels of compliance, a unique feature provided only by Maya Data Privacy's AI Safe Chatbot with its Unique Privacy Layer, helping customers meet key requirements such as the Right to Forget, Right to Access and Data Portability, Data Anonymisation, and Data Breach Detection, Reporting, and Prevention

Report Duration	1st Dec 2024 to 31st Dec 2024
Project Name	Northern City Hospital
Prepared by	Maya Data Privacy
Active Users	126

Compliance Parameters

Compliance Parameters are settings and configurations applied during the anonymisation process to balance data usability and privacy. These parameters determine how much information is retained while ensuring compliance with privacy requirements.

Data Anonymisation

Data anonymisation involves removing or altering personal information to prevent identification while retaining data for analysis.

The report summarizes the number of personal names, phone numbers, and email addresses sent to the LLM server, noting how many were transmitted without anonymisation and were on popular lists with relevant personal information. Referring to Art. 4 GDPR.

	# of **Personal Names** sent to LLM Server
Sent after Anonymisation	187,524
Present on *Popular* Lists	10
Sent without Anonymisation	0

	# of **Phone Numbers** sent to LLM Server
Sent after Anonymisation	15,021
Sent without Anonymisation	0

	# of **Emails** sent to LLM Server
Sent after Anonymisation	18,743
Sent without Anonymisation	0

Right to Forget

The right to forget enables individuals to request the deletion of their personal data when it is no longer necessary or lawful to retain it.

The report summarizes the number of Right to Forget requests received from employees and patients, tracking data deletion activities. Referring to Art. 17 GDPR.

	# of **Requests**
Employee	5
Patient	5
Total	**10**

Data Storage and Retention

Data storage and retention define how long personal data is kept and the conditions under which it is securely stored in compliance with privacy laws.

The report details the storage and retention periods for data, ensuring adherence to organizational and regulatory requirements. Referring to Art. 13 & 14 GDPR.

	# of **Data Storage and Retention**
Data Storage Location	European Union
Data Storage Duration	30 days

Right to Access and Data Portability

The right to access and data portability allows individuals to obtain and transfer their personal data in a structured, machine-readable format.

The report summarizes requests for data access and portability from employees and patients. Referring to Art. 15 & 20 GDPR.

	# of Requests for Downloads
Employee	5
Patient	3
Total	**8**

Data Breach

A data breach is an incident where unauthorized individuals gain access to confidential or sensitive personal data, potentially exposing it to misuse or harm.

The report highlights the number of data report notifications issued and the number of data breaches prevented, emphasizing the system's effectiveness in maintaining data security. Referring to Art. 33 & 34 GDPR.

	Count
Data Breach Notifications	1
Data Breaches Prevented	1
Total	**2**

Sensitive Data

Sensitive attributes are identified by the client and activated in the system by system administrator. Once identified there is no choice for the user to send such information via the APIs processed by the application.

The report highlights, such attributes, which were detected and prevented from being sent to the LLM. Once detected, the attributes were replaced with suitable placeholders, allowing the user to have a meaningful reply from the LLM, while preventing any sensitive data to be sent.

	Patient ID
Sent After Anonymisation	3105
Sent Without Anonymisation	0

	# of **Application Configuration files**
Sent After Anonymisation	2
Sent Without Anonymisation	0

	# of **Third Party service Credentials / Cloud Credentials**
Sent After Anonymisation	25
Sent Without Anonymisation	0

	# of **API Keys and Client secrets**
Sent After Anonymisation	11
Sent Without Anonymisation	0

	# of **Code with Identified keywords**
Sent After Anonymisation	5
Sent Without Anonymisation	0