

Reference: 2025-048

Thank you for your emails in which you requested the following information under the Freedom of Information Act 2000 (FOIA):

I am requesting a list and summary of any breaches in GDPR regulation of personal data, protection and usage; data losses; or other data security incidents caused by Generative AI chatbots reported to your department from 01/01/22 and the date this request is processed. When referring to confidential or sensitive government information I am referring to any documentation or information placed into an AI Chatbot that was not intended or not cleared for publication. I also note that when referring to Generative AI Chatbots I am referring to any software application that uses machine learning and natural language processing to interact with users through text or speech.

Please could I received the following:

1. The number of times confidential or sensitive government information placed into an AI Chatbot has caused a data breach or cyber security incident between 01/01/22 and the day this request is processed. If possible, please include the nature of each incident, the number of individuals affected (if applicable), and any outcomes or remedial actions taken.
2. The number of times personal or private information placed into an AI Chatbot has caused a breach in GDPR regulation between 01/01/22 and the day this request is processed. If possible, please include the nature of each incident, the number of individuals affected (if applicable), and any outcomes or remedial actions taken.
3. Which AI Chatbot tool the departments allows civil servants and ministers to use, or if applicable any bespoke AI Chabot the department uses.

Response

The SFO does not hold this information.

There have been no breaches of any GDPR regulations from 1 January 2022 to the date of this request.