Diarienummer:
IMY-2024-5156

Datum:
2024-12-18

Disclosure of Public Records Using AI

English summary: the Swedish Authority for Privacy Protection, IMY, finishes its third regulatory sandbox project

- **The Swedish Data Protection Authority (Integritetsskyddsmyndigheten, IMY) has conducted its third project within its regulatory sandbox during the spring and summer of 2024.** With regulatory sandbox, IMY refers to in-depth guidance on how the data protection framework should be interpreted and applied. Characteristic of the working method is that IMY, together with the project participants, identifies the legal issues on which the guidance should focus. Guidance is then given orally on several occasions over a few months in the form of workshops or other dialogue-based forms. The work results in a public report where reasoning and assessments are summarised to enable learning for a broader audience.

- **The project "Disclosure of Public Records Using AI"** marks IMY's third regulatory sandbox project. The participants in this project have been the Municipality of Lidingö and Atea Sverige AB (Atea). The aim was to explore some of the legal grey areas that arise when using an AI-based digital tool to streamline parts of the confidentiality assessment process before disclosing public records.

- **The project encompasses two main concepts**: a comprehensive system (the "full-service solution") and a more limited system (the "masking service"). The full-service solution aimed to automate large parts of the public records disclosure process. However, during the project, both technical and legal challenges were identified, leading participants to focus on and proceed with the narrower masking service. The solution is based on AI-powered language models and is intended to assist officials in making confidentiality assessments. It is important to note that the redaction service is purely an aid for officials, meaning that it is ultimately the official who decides what information should be subject to confidentiality and what should not.

- **The use of the masking service is expected to yield significant efficiency gains** for the municipality by automating the initial identification and redaction of personal data in public records. The participants reported that the current manual process for confidentiality redaction is time-consuming and labour-intensive for the case handlers, especially when large volumes of documents are requested. By allowing the masking service to perform preliminary redactions, identifying both direct and indirect personal data, case handlers can save time and resources otherwise spent on manual work. This enables a

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

faster and more efficient handling of disclosure requests and enhances the municipality's ability to meet the promptness requirements of the Freedom of the Press Act.

- **The guidance provided during the project focused on three legal questions.** Beyond these, other legal issues must also be considered before deploying an AI service, which were not analysed within the scope of this project.

- **Question 1: Is there a legal basis for using an AI service in public record disclosure under the General Data Protection Regulation (GDPR)?** IMY analysed whether legal grounds exist under the GDPR and complementary Swedish legislation for processing personal data, including sensitive personal data, in connection with using the AI service for handling public record requests. IMY initially assessed that there might be a legal basis for using both the holistic service and the redaction service in tasks of public interest. The same basis could also support the processing of sensitive personal data in both services. Regarding the requirements for necessity and proportionality, IMY considers that there is strong justification for processing both regular and sensitive personal data in the redaction service. However, predominant reasons weighed against the necessity and proportionality of processing personal data in the full-service solution, particularly concerning sensitive personal data.

- **Question 2: How is responsibility for personal data distributed, who is the controller and processor?** According to IMY, it is highly likely that the responsibility for personal data processing is limited to the individual municipality, while the AI provider (Atea in this project) acts as a data processor. Furthermore, several factors suggest that each municipal committee is separately responsible for the personal data processing occurring when the masking service is used. Thus, the individual committee ultimately bears responsibility for ensuring that the public records requested are properly redacted for confidentiality.

- **Question 3: What security measures are appropriate when using the AI service?** Suggested security measures include specific governance and increased risk awareness within the organization regarding the use of AI, as well as strong authentication, encryption, logging, and regular monitoring to prevent unauthorized access and incorrect data processing. There must also be clear and transparent control over the data the AI model can access, ensuring all handling complies with the GDPR. IMY particularly emphasizes the importance of maintaining a "human-in-the-loop" approach, requiring responsible case handlers to independently verify the accuracy of redactions before disclosing records. IMY also recommends conducting a data protection impact assessment (DPIA) before the AI service is implemented.