BCLP. Client Intelligent

Insights

EUROPEAN DATA PROTECTION BOARD'S OPINION ON AI MODELS

Dec 23, 2024

SUMMARY

On 17 December 2024, the European Data Protection Board (**EDPB**) adopted its opinion on certain data protection aspects related to the processing of personal data in the context of AI models (**Opinion**).

The Opinion comes as a response to the Irish supervisory authority's (**Irish SA**) request. The Irish SA's request made to the EDPB was prompted due to the current lack of harmonisation amongst supervisory authorities when it comes to assessing AI models and addresses key components of an AI model such as training, updating, developing and the operation of AI models where personal data is part of the dataset.

The Irish SA posed four specific questions as part of the request which covers:

1. Anonymity in AI models where personal data has been used to train the model;
2. The appropriateness of relying on legitimate interest as a lawful basis and how this can be demonstrated; and
3. The continued use of an AI where unlawfully processed data sets have been used to create, update or develop an AI model.

We cover each of these themes in turn below.

ANONYMITY IN AI MODELS

The bar for a data set to be considered 'truly anonymous' remains high and the EDPB refers us to its detailed guidance on this topic. However, the Opinion does outline the elements which will need to be met in order to agree with a controller that the relevant AI model may be considered anonymous.

First, any AI model that provides personal data (as output) regarding individuals whose personal data is used to train the AI model (as input) cannot be considered anonymous.

Therefore, to consider an AI model as being anonymous, the supervisory authority will need to be provided with evidence that:

1. any output produced when querying the model does not relate to the data subjects whose personal data was used to train the model; and

2. personal data relating to the training data cannot be extracted out of the model.

When assessing the likelihood of identification, or reidentification, the supervisory authority will need to take into account "*all the means reasonably to be used*" by the controller, or by a third party, to extract personal data from the training data set. This assessment must be done using factors such as the characteristics of the AI model's design with the assessment differing between a public and a private AI model.

DOCUMENTATION

The EDPB makes clear that documentation is a key component when assessing whether or not personal data is processed in an AI model and also as part of compliance with GDPR more generally, noting that organisations should have documented the relevant technical and organisational measures when deploying AI systems even when the objective of the processing is anonymisation.

Documentation covers data protection impact assessments (**DPIA**) (including documented rationales when a DPIA is considered to not be necessary), technical and organisational measures taken at each part of the model's lifecycle, threat model and risk assessments.

In this context, whilst documentation can assist with the anonymity assessment relating to an AI model, it is also intertwined with accountability obligations under the GDPR and if after reviewing an organisation's documentation, the supervisory authority is not able to conclude that effective measures were taken to anonymised the AI model, the supervisory authority may also consider this to be a failure to meet accountability obligations.

LEGITIMATE INTEREST

The EDPB reiterates that there is no legal basis hierarchy but it offers a useful guidance for AI model developers wishing to rely on legitimate interest. Legitimate interest is likely to be used in in the context of publicly available data likely to be obtained through web scraping.

If relying on legitimate interest, the supervisory authority will need to be comfortable that controllers have assessed and documented whether the:

- **controller or a third party pursues a legitimate interest**: the EDPB considers that developing the service of a conversational agent to assist users or developing an AI system to detect fraudulent content or behavior are examples which may constitute a legitimate interest of the controller.
- **processing is necessary to pursue the legitimate interest** meaning that the data processing must be necessary to allow the pursuit of the purpose and that no less intrusive way exists; and
- **legitimate interest is not overridden by the interests or fundamental rights and freedoms of the data subjects (balancing test)**: the development and deployment of AI models may raise serious risks to rights of individuals such as the right to private and family life, reputational risk, identity theft or fraud, security risk The Opinion also includes a number of criteria to help supervisory authorities determine whether individuals can reasonably expect certain uses of their personal data. This criteria includes:

  1. whether or not the personal data was publicly available;
  2. the nature of the relationship between the individual and the data controller;
  3. the nature of the service;
  4. the context in which the personal data was collected;
  5. the source from which the data was collected;
  6. the potential subsequent uses of the AI model;
  7. information provided by the controller to the data subjects and
  8. whether individuals have actual knowledge that their personal data is online.

Specific measures may prove useful to mitigate the risk in the context of web scraping including **technical measures** such as excluding data content from publications or excluding collection from websites whose terms and conditions clearly object to web scraping (for example, by respecting robots.txt or ai.txt files to express exclusion from automated crawling). The EDPB also mentions specific measures to protect data subject rights such as **facilitating the exercise of individuals' rights and transparency** by creating an opt-out list, managed by the controller and which allows data subjects to object to the collection of their data on certain websites.

UNLAWFULLY PROCESSED DATA SETS

The EDPB recalls that each controller (either being a developer or a deployer) must ensure the lawfulness of data processing. As such, it is for the controller deploying the AI model to conduct an

assessment to ascertain that the AI model was not developed by unlawfully processed personal data.

This could be a difficult task for AI deployers who might not have the same level of information as the developer.

The EDPB makes clear that controllers deploying AI models may not be able to comply with their GDPR obligations if the model itself was not developed lawfully even where the provider is a third-party supplier.

CONCLUSION

Whilst the Opinion seeks to provide a framework for supervisory authorities to asses specific cases where some of the questions/considerations raised in the Irish SA's would arise, a recurring theme throughout the Opinion is that many of these questions/considerations should be assessed on a case by case basis and as such the battle between harmonisation and discretion continues.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21

Olivia Wint

London

olivia.wint@bclplaw.com
+44 (0) 20 3400 4621
