Browne Jacobson

EDPB guidelines: Processing personal data in the context of AI models

12 February 2025

The European Data Protection Board ('EDPB') released new guidance on certain data protection aspects of personal data in the context of AI models (the 'Guidance') for the statutory authority ('SA').

This comes after the Irish supervisory authority requested the EDPB to issue an opinion pursuant to Article 64(2) of the GDPR, which relate to AI models and the processing of personal data (the 'Request').

Scope of the Request

The Request addressed certain elements of the training, updating, development and operation of AI models where personal data forms part of the dataset. The Irish supervisory authority highlighted that the Request concerned key issues that impact data subjects and controllers in the EEA. Specifically, the Request sought clarity on the following questions:

1. when and how an AI model can be considered as 'anonymous',
2. how controllers can demonstrate the appropriateness of legitimate interest as a legal basis in the development,
3. when using legitimate interest as a legal basis for processing, how should a controller demonstrate legitimate interest as a legal basis, and
4. what the consequences of the unlawful processing of personal data in the development phase of an AI model on the subsequent processing or operation of the AI model are.

Question 1: When and how an AI model can be considered as anonymous?

AI models are usually deigned to make predictions or draw conclusions. Therefore AI models 'trained' (as described by the EDPB) with personal data are often designed to make inferences about individuals, some are designed to provide personal data regarding individuals whose personal data was used to train the AI model. These models will inherently include information relating to an identified or identifiable natural person and will therefore involve the processing of personal data. These types of AI cannot be considered anonymous. In their Guidance the EDPB noted that all AI models trained on personal data cannot be considered anonymous.

For an AI model to be considered anonymous, using reasonable means both (i) The likelihood of direct extraction of personal data regarding individuals whose personal data were used to train the model, as well as (ii) the likelihood of obtaining, intentionally or not, such personal data from queries, should be insignificant. SA's will now require that AI models are likely to require a thorough evaluation of the likelihood of identification to reach a conclusion on their possible anonymous nature. This likelihood should be assessed considering all the means likely to be used by the controller or another person and should also consider unintended (re)use or disclosure of the model. Statutory bodies will be evaluating whether the measures used by the controller to ensure that an AI model is anonymous are appropriate and effective on a case by case basis.

The Guidance provided a non-exhaustive and non-prescriptive list of elements for SA's to consider when assessing a controllers claim of anonymity (such as AI model design, selection of sources, data preparation and minimisation etc). Due to the new guidance SA's will now look closely at the documentation whenever an anonymity claim needs to be evaluated, verifying whether the controller's documentation includes a DPIA (or assessment that determines a DPIA was not necessary – Pre DPIA), any advice or feedback from data protection

officer, information on technical and organisational measures taken while designing the AI model, technical and organisational measures taken at all stages which contributed to the lack of personal data, the documentation demonstrating the AI models resistance to re-identification and documentation provided to the controller deploying the model in particular and the documentation related to the measures taken to reduce the likelihood of identification and regarding the residual risks.

Question 2 and 3: How can controllers validate legitimate interest as a legal basis in AI development and processing?

In order to verify whether the processing of personal data can be based on legitimate Interest SA's must verify that controllers have carefully assessed and documented whether the three following conditions are met (i) the pursuit of a legitimate interest by the controller or by a third party, (ii) the processing is necessary to pursue the legitimate interest (necessity test), and (iii) the legitimate interest is not overridden by the interests or fundamental rights and freedoms of the data subjects (balancing test). This is to be determined by the relevant statutory body on a case by case basis.

The Guidance emphasised the potential risks to fundamental rights during the development and deployment phases of AI models, noting that the impact on data subjects can vary widely. It is important to consider the data subjects' reasonable expectations in the balancing test, influenced by the complexity of AI technologies and the potential obscurity of their uses. Factors such as the public availability of data, the nature of the relationship between data subjects and controllers, and the context of data collection play a critical role in assessing these expectations. The omission of information can contribute to the data subject not expecting a certain processing, the mere fulfilment of the transparency requirements set out in the GDPR is not sufficient, meaning If information relating to development phases of an AI model is included in the controller’s privacy policy this does not necessarily mean that the data subjects can reasonably expect it to happen. The Guidance states that SA's are tasked with evaluating this all on a case-by-case basis.

Question 4: What are the consequences of unlawful data processing during AI development?

In accordance with article 51(1) GDPR SA's “are responsible for monitoring the application of the GDPR” they have the discretion to evaluate the lawfulness of the processing and to decide on appropriate actions, considering each case's unique circumstances exercising their powers granted by the GDPR in line with their national framework.

SA's may impose certain corrective measures considering the circumstances of each scenario, such as ordering controllers to take actions in order to remediate the unlawfulness of the initial processing. These could include issuing a fine, imposing a temporary limitation on the processing, erasing part of the dataset that was processed unlawfully or, where this is not possible, taking into consideration the specific details of each case and the proportionality of the action ordering the erasure of the whole dataset used to develop the AI model and/or the AI model itself. When assessing the proportionality of the envisaged measure, SA's may consider measures that can be applied by the controller to remediate the unlawfulness of the initial processing (e.g. retraining).

Scenarios

The EDPB addressed three (3) scenarios covered under question 4 of the Request, where the differences lie on whether the personal data processed to develop the model is retained in the model, and/ or whether the subsequent processing is preformed by the same or another controller. These scenarios were as follows:

In the first scenario where a controller engages in the unlawful processing of personal data for the development of an AI model and retains this data for further use during the deployment phase, the EDPB highlighted that SA's are empowered to enforce corrective actions regarding the initial violation. This may include the erasure of data processed unlawfully, effectively limiting any future processing activities associated with that data. Noting the necessity of evaluating on an individual basis whether the development and deployment phases represent distinct processing activities. Pointing out that in cases where subsequent processing relies on legitimate interests, the illegitimate nature of the initial data processing should be considered when assessing the validity of these interests.

Scenario 2 explores a case where personal data, initially processed unlawfully during the development of a model, is later processed by a different controller. The EDPB emphasised the importance of clearly defining the roles and responsibilities of various entities under the GDPR. It is for each controller to verify the legality of their data processing activities. SA's are tasked with assessing not just the original

processing activities conducted by the first controller but also the subsequent actions taken by the second controller. Additionally, SA's will examine whether the second controller has adequately investigated the model's adherence to lawful processing standards during its development phase.

In Scenario 3, where a controller initially processes personal data unlawfully but then anonymises this data prior to deployment, the operation of the model falls outside the scope of the EU GDPR, provided the anonymisation process is effectively and verifiably carried out. This ensures that any further processing of the anonymized data remains unaffected by the original unlawful processing. However, it is not enough for controllers to simply claim that data has been anonymised as SA's will now be rigorous in verifying these claims through a detailed evaluation tailored to the specifics of each case.

For further advice on this topic please contact Jeanne Kelly and Raymond Sherry in our Dublin office and for UK law insights into use of AI, contact Richard Nicholas or Francis Katamba.

Contact

Jeanne Kelly

Partner

jeanne.kelly@brownejacobson.com

+353 (85) 846 3955

Raymond Sherry

Associate

raymond.sherry@brownejacobson.com

+35315743916

Related expertise

Services

Data protection and higher education

Data protection and privacy

Data protection for retail

Data protection guidance for schools and trusts