REQUEST FOR AN OPINION OF THE EUROPEAN DATA PROTECTION BOARD PURSUANT TO ART. 64(2) GDPR

The IE SA hereby requests that the EDPB examine the within matters of general application (and which produce effects in more than one Member State) and issue an opinion on the said matters pursuant to Article 64(2) GDPR (the "**Request**"). The IE SA notes that the EDPB has not already issued an opinion on the matters detailed in this Request.

Context of this Request

The training and use of AI Models, including so-called "large language models", gives rise to a number of wide-ranging data protection concerns. The issues arising impact data subjects across the EU/EEA. The IE SA has received a number of complaints both from data subjects in Ireland and from data subjects throughout the EEA, by way of referrals from other SAs, which raise questions concerning the extent to which the processing of personal data associated with the development of AI Models complies with the GDPR. Alongside these complaints, an increasing number of data controllers are incorporating the use of AI Models within their business operations. This gives rise to the need for supervisory authorities to engage generally in the regulation of the processing of personal data associated with the development of AI Models. The IE SA understands that certain of the key matters arising, in this context, have already been considered by individual supervisory authorities and that divergences exist, in terms of the views held by individual supervisory authorities on certain key issues.

Thus far, the EDPB has not reached a common position or shared consensus on matters central to the processing of personal data that occurs through the creation, operation and maintenance of AI models. These matters include the question of what legal basis might be relied upon to lawfully ground processing for the training of such AI Models using personal data, be it third-party or first-party data. Similarly, the EDPB has not formed a harmonised position on whether such AI Models, either operating alone or as part of an AI System, can be said to be processing personal data once the AI Model has been trained using personal data.

While there are Guidelines adjacent to the subject-matter planned for drafting within the EDPB, the EDPB will greatly benefit from reaching a common position on the matters raised by this Request, such matters being central to the planned work of the EDPB in the short and medium term. The identification of a harmonised position on these matters will also facilitate the efficient handling of the complaints that have been lodged and the conclusion of outcomes and decisions on a harmonised basis. The establishment of harmonised positions will also support the general regulation of processing taking place across the EU/EEA in this field by all supervisory authorities. In these circumstances, the IE SA respectfully submits that it is important that the EDPB adopt a common position on as many of the novel and potentially contentious issues arising in this area as soon as is reasonably possible.

Existing research publications highlight some potential vulnerabilities that can exist in AI Models which could result in personal data being processed,[1] as well as the personal data processing that may go on when models are deployed for use with other data, either through Application Programming

[1] Such as Membership Inference Attacks (OWASP), and Model Inversion Attacks (OWASP & Veale et al, 2018).

Interfaces ("APIs") or "prompt" interfaces. There is also a question about when and if personal data continues to be involved after deployment of models, in AI Systems or otherwise:

- is the reduced format of the training data still personal data in all or perhaps only some circumstances, if at all?;
- does source data erasure mitigate any such processing that arises?; do AI Systems influence this analysis?;
- what must be demonstrated by a data controller where personal data processing is claimed not to occur?

[redacted]

Where data is scraped from the publicly available internet, it can also be considered to be personal data. That is to say, just because personal data is made public does not mean that it is no longer personal data. Careful consideration of this situation is required in order to demonstrate compliance under data protection legislation, including in relation to further processing and legal basis.

While the GDPR is technology-neutral, AI-related processing, while novel in some ways, is certainly covered by the GDPR whenever personal data is processed. As such, it is vitally important to the work of the EDPB and all supervisory authorities that a common understanding and position is reached about how and when the processing of personal data involved in AI Models begins and ends, and what risks are associated with it.

Given that these issues are both systemic, abstract and novel, and impact a large number of data subjects throughout the EU/EEA, the IE SA is of the view that a harmonised EDPB position on the matters arising would best be reached by way of an Opinion of the EDPB pursuant to Article 64(2) GDPR.

The issues identified by the IE SA (as detailed further, below) impact on all data controllers that train, or intend to train, AI Models using personal data, and are therefore self-evidently of general application. Furthermore, given the large number of data controllers involved and the large number of data subjects impacted, any such opinion would produce effects in more than one Member State, as a matter of certainty. As a result, the IE SA submits that the issues raised meet the standard required by Article 64(2) GDPR.

Please note that the within Request relates to the application of the GDPR/LED only – it does not concern the possible application of, or interplay with, any extraneous legal frameworks such as those represented by the AI Act, DMA, DGA, DSA, etc. In these circumstances, the IE SA requests that the EDPB consider the questions set out below by reference to the application of the GDPR/LED only.

Definitions for the purpose of this Request

To ensure a common understanding of the issues falling for discussion, the IE SA has framed the questions that follow by reference to the term "AI Model" which has been ascribed the meaning set out immediately below. Please note that, in having formulated this definition, the IE SA is not requesting the EDPB to agree or confirm that this definition shall have general application beyond this Request. In other words, the IE SA has ascribed a particular definition for the term "AI Model" for the limited purpose of this Request and, more particularly, for the purpose of avoiding confusion or misunderstanding as to what might be meant by this key term that is central to the questions that the EDPB is requested to examine.

"AI Model" – Definition

When this Request refers to an "**AI Model**", it refers to the common understanding of an 'AI Model'[2], to encompass the product resulting from the training mechanisms that are applied to a set of training data, in the context of Artificial Intelligence, Machine Learning, Deep Learning or other related processing contexts.

The term applies to AI Models which are intended to undergo further training, fine-tuning and/or development, as well as AI Models which are not.

Questions for examination, discussion and agreement in the form of an Article 64(2) Opinion

Against the background of the above, the following specific questions arise for determination, as a result of the training and use of such AI Models:

In the 'life-cycle'[3] of the creating, updating, developing and operation of an AI Model where personal data forms part of the data upon which the model is trained, fine-tuned or otherwise updated, or operated:

Q1: Is the final AI Model, which has been trained using personal data, in all cases, considered not to meet the definition of personal data (as set out in Article 4(1) GDPR)[4]?

If the answer to Q1 is "yes":

i. At what stage of the processing operations leading to an AI Model is personal data no longer processed?
    a. How can it be demonstrated that the AI Model does not process personal data?

ii. Are there any factors which would cause the operation of the final AI Model to no longer be considered anonymous?[5]
    a. If so, how can the measures taken to mitigate, prevent or safeguard against these factors (so as to ensure the AI Model does not process personal data) be demonstrated?

If the answer to Q1 is "no":

[2] This is not expressly defined in legislation, such as in the AI Act
[3] Namely. all activities performed to achieve the creation, updating and/or developing of an AI Model.
[4] And Article 3(1) of the Law Enforcement Directive and Article 3(1) of Regulation 2018/1725.
[5] Such as integration into an 'AI System' as defined in the AI Act, which may provide the 'means' to re-identify data subjects whose personal data was used to train the Model.

i. What are the circumstances in which that might arise?
    a. If so, how can the steps that have been taken to ensure that the AI Model is not processing personal data be demonstrated?

Q2: Where a data controller is relying on legitimate interests as a legal basis for personal data processing to create, update and/or develop an AI Model, how should that controller demonstrate the appropriateness of legitimate interests as a legal basis, both in relation to the processing of third-party and first-party data?

i. What considerations should that controller take into account to ensure that the interests of the data subjects, whose personal data are being processed, are appropriately balanced against the interests of that controller in the context of:
    a. Third-party data
    b. First-party data

Q3: Post-training, where a data controller is relying on legitimate interests as a legal basis for personal data processing taking place within an AI Model, or an AI System of which an AI Model forms part, how should a controller demonstrate the appropriateness of legitimate interests as a legal basis?

Q4: If an AI Model has been found to have been created, updated or developed using unlawfully processed personal data, what is the impact of this, if any, on the lawfulness of the continued or subsequent processing or operation of the AI model, either on its own or as part of an AI System, where:

i. The AI Model, either alone or as part of an AI System, is processing personal data?
ii. Neither the AI Model, nor the AI Model as part of an AI System, is processing personal data?