Changes to GDPR Article 9

To: Ministry of Justice and Digital Affairs

Date: 29.12.2025

From: Veriff OÜ, Aleksander Tsuiman aleksander.tsuiman@veriff.net

The proposed amendment

Article 9 is amended as follows:

(a) in paragraph 2, the following points are added:

'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.

(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'

(b) the following paragraph is added:

'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data

> *from being used to produce outputs, from being disclosed or otherwise made available to third parties.'*

Comments, observations, suggestions

Addition of Article 9 section 2 (k) and Article 9 section 5

- Not clear what is the intended purpose of the addition, specifically:
    - How does the change correlate with article 10 section 5 of Regulation (EU) 2024/1689 (AI Act) allowing the processing of special categories of data for the purposes of bias mitigation. It is unclear whether article 10 section 5 of the AI Act would then be considered applicable only for high risk AI systems and article 9 section 2 (k) would then be then applicable to all non high risk systems OR all systems, including high risk systems.
    - The proposed wording, i.e. "*processing in the context of /–/* ***operation*** *of an AI system /–/ or an AI model*" makes it appear like operating an AI system is a processing activity on its own, however, an AI system or a model is a means of technology and should not receive different treatment from any other technological means to process data. If read together with article 9 section 5, this wording can even create a confusing obligation to remove data from processing.
    - Furthermore, the wording is extremely specific focusing on technology as it stands today and that is against the principle of technology neutrality that is a core regulatory principle in the EU stating laws should focus on outcomes/functions, not specific tech, to avoid stifling innovation, future-proof rules, and let markets choose best solutions.
- The proposed wording does not take into account the realities around operating biometric technology. The legislator should understand that as there are AI models and AI systems

processing biometrics then those models and systems need to be properly trained. Training and operating such models presumes the existence of such data as part of the processing operations. This means that such data is used to produce outputs as otherwise those systems would not be able to operate. Hence, the current wording of Article 9 section 5 is far off from how a well performing and "behaving" AI-based biometric system would work.

- Additionally, requiring the controller to remove such data unless doing so involves disproportionate effort imposes an extremely high standard. This could significantly impede the development and functioning of many AI models and systems.
- The phrase "protect data from being used to produce output" is ambiguous because it does not define what "produce output" entails. Since disclosure and making data available are addressed separately, "produce" can only be interpreted as preventing training data from contributing to outcomes. However, this would be technically infeasible, as training data is inherently part of generating results.
- **Suggestions**:
    - Remove the notion of "operation" from article 9 section 2 (k)
    - Reword article 9 section 5 to only state "*For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the unnecessary processing of special categories of personal data.*".
    - Alternatively reword Article 9 section 5 should as follows: "For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the OPERATION OF THE AI system or AI model,

the controller shall remove such data AT THE EARLIEST POSSIBILITY. If removal of those data requires disproportionate effort OR IT CONTRADICTS THE PURPOSE OF THE AI SYSTEM OR AI MODEL, the controller shall ~~in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties~~ *IMPLEMENT APPROPRIATE ORGANISATIONAL AND TECHNICAL MEASURES.*

Addition of Article 9 section 2 (l) and section (34) of the preamble

- Not clear what is the intended purpose of the addition, specifically:
  - What is the provision meant to **enable**?
  - What is the provision meant to **protect** (considering the exception from the general prohibition set forth under article 9) against?
- Our approach is that alleviation should **enable** 2 elements:

  i) create a framework for the usage of biometrics as a safe and an ever-widespread security feature that businesses can apply and enable in the course of their regular business activities while adhering to the already robust standard privacy framework; and

  ii) fraud prevention at scale while ensuring that a good and seamless UX. Therefore, easing the requirements for user verification alone does not recognize that many fraud prevention processes depend on the one-to-many ("authentication"), e.g. enabling account login and password resetting using biometrics.
- In terms of **protecting** the data subjects against potential risks arising from the processing of special categories of personal data the legislator seems to place emphasis on the "sole control" of the data subject. "Sole Control" would refer to very few technological solutions that are rather not used today – the technology mostly used would retain the data under the control of the service provider for verification or authentication. To explain further why

the “sole control” of the data subject does not fulfil the aim of protecting data subjects’ rights is that technical control over the process, considering the complexity of the underlying technology, is not what is protecting the data subject against the actual risks. The data subject does receive more protection when: i) the underlying technology is secure (e.g. encryption is applied as already suggested in the proposal); and ii) the data subject is aware of the processing and can choose whether to be subject to it or not. Therefore, emphasis should be put on not the “sole control” as a technical means but rather the fact that the purpose of confirming the identity of the data subject using special categories of data (both verification and authentication) are made on the request of, or due to services requested by, the data subject. The current wording of the preamble seems to be addressing a very narrow technological solution that is only one, or a very limited set of, privacy preserving technologies available.

- **Suggestions:**
    - Expand the biometrics use-cases to authentication in addition to verification. Ideally, the expansion would also include fraud prevention and detection;
    - The concept of “sole control” should be revised so that control rests with the service provider rather than exclusively with the data subject. This approach would ensure technical security of the data while linking processing activities to operations that are directly or indirectly related to services requested by the data subject. The primary objectives should remain data security and transparency for the data subject.

We remain available for further discussions.

Aleksander Tsuiman