REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Mehdi Raufi
MedExFuture OÜ
management@medexfuture.com

Yours: 09.02.2026

Ours: 25.02.2026 nr 2.2-9/26/519-2

Answer to request

Estonian Data Protection Inspectorate (EDPI) has received your request regarding the responsibilities as a data controller. EDPI is a supervisory authority and shall provide explanations to requests, free of charge, concerning the legislation as stated in Response to Memoranda and Requests for Explanations and Submission of Collective Proposals Act § 3.[1] EDPI does not provide legal aid. Legal aid is when a legal assessment is given regarding specific circumstances. We recommend contacting a legal adviser for assistance with the legality of processing personal data and creating the necessary documentation. Nevertheless, we will provide general explanations regarding the questions raised.

Legal basis

Firstly, you require information on appropriate lawful bases and consent approach for processing health data. The legal basis and specific purpose requirement arise from Article 5 of the General Data Protection Regulation (GDPR), which sets out the principles of data processing. GDPR Article 5 (1) (a) stipulates that there must be a legal basis. The legal bases for processing personal data are set out in Article 6(1) of the GDPR.

According to Article 5(2) of the GDPR, the controller is responsible for compliance and required to determine the legal basis for processing who must ensure the lawfulness of the processing of personal data. Therefore, EDPI cannot determine the appropriate legal basis for your processing activities. The controller is responsible for determining the legal basis for processing personal data according to Article 5(2) of the GDPR.

Furthermore, it is important to note that health data falls under special categories data (GDPR Article 9 (1)). This means that in addition to having a legal basis under Article 6 (1) of the GDPR, the processing must also meet one of the exceptions set out in Article 9(2) of the GDPR. Consent can be a legal basis to process health data but for it to be a valid legal basis, it must meet the following four conditions: it must be freely given, specific, informed, and unambiguous. Among other things, consent can be withdrawn at any time. We recommend you read the European Data Protection Board guidelines on consent[2].

The processing must also comply with the other principles set out in Article 5 of the GDPR. For example, Article 5(1)(b) of the GDPR states that the controller must ensure transparency by providing a clear and accurate privacy policy, in addition to determining the legal basis, purpose, and other relevant elements of the processing. The information provided to data subjects in the privacy policy must accurately reflect the controller's actual data-processing activities. Therefore, it is equally important to identify and map the personal data that will be collected and processed. Personal data must be collected only to the extent necessary to achieve a specific purpose. Collecting personal data "just-in-case" is unlawful under Article 5(1)(c) of the GDPR.

[1] Response to Memoranda and Requests for Explanations and Submission of Collective Proposals Act. Link: https://www.riigiteataja.ee/en/eli/529122024003/consolide
[2] EDPB Guidelines 05/2020 on consent under Regulation 2016/679. Link: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

DPIA

Secondly, you ask if there are any guidelines available for conducting DPIA. GDPR Article 35 states that a DPIA must be carried out by all controllers whose processing operations, considering their nature, scope, context, and purposes, are likely to result in a high risk to individual particularly when using new technologies. Unfortunately, we do not have a specific guidance document in English, but we do have a chapter in our general guidance for data controllers, written in Estonian, which explains the nature of a DPIA[3].

Data subjects' rights

Your third question concerns data subjects' rights and principles relating to processing personal data. Data subjects' rights are set out in Chapter III of the GDPR. It is important to remember that the controller must comply with GDPR Article 5 when carrying out processing. The processing of personal data must always be linked to a specific purpose. Before obtaining or collecting personal data, you must identify the purpose for which it is required and the objective to be achieved. As we stated beforehand in this answer, you can only collect the minimum amount of data necessary for that purpose. It is important to establish which data is actually required.

Cross-border and obligations of processors

Fourth question is regarding cross-border data transfers and the obligations of processors and sub-processors. Without knowing the exact circumstances, it is difficult to provide specific guidance. When transferring personal data within the European Union, the data controller must ensure that there is a valid legal basis for the processing and transfer of personal data, as required under Article 6 or Article 9 of the GDPR. When personal data is transferred outside the European Union, it must be ensured that the level of protection afforded to the data remains essentially equivalent to the level guaranteed within the EU.

It is important to keep in mind that the data controller must select a processor who meets and follows GDPR requirements. A data processing contract should be in place between the controller and the processor (GDPR Article 28 (4)). This agreement should clearly outline the roles and obligations of both parties regarding the processing of personal data. We recommend that you review the European Data Protection Board guidelines on the concepts of controller and processor in the GDPR[4].

AI system specific guidance

Your fifth question concerns guidance on specific considerations for AI systems that interact with users about health topics. As stated before, DPIA must be carried out by all controllers whose processing operations, considering their nature, scope, context, and purposes, are likely to result in a high risk to data subjects particularly when using new technologies. Processing special categories of data (health data) which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms (Recital 51 GDPR).

The European Union's Artificial Intelligence Act[5] establishes additional requirements for high-risk AI systems, including obligations related to transparency, human oversight, and documentation. For a system to be considered an AI system under the Act, it must, among other characteristics, be capable of making inferences. This means that if a trained model (e.g., machine learning) is used and it generates inferences based on input data, it qualifies as artificial intelligence within the meaning of the Act. If a system is purely rule-based and relies on simple algorithms (such as an if-then rule) without any learning capability or inferential processing, it is considered a standard

[3] Isikuandmete töötleja üldjuhend, 5. ptk. Link: https://www.aki.ee/5-peatukk-andmekaitsealane-mojuhinnang
[4] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Link: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

software system rather than artificial intelligence.

In addition, articles 10–17 of the AI Act set out detailed documentation and compliance obligations for high-risk AI systems, including requirements related to data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, and the establishment of a quality management system. With regard to legal regulation concerning artificial intelligence, no specific national legislation is currently in force. Although the AI Act foresees the adoption of a national implementing act, such legislation has not yet been enacted in Estonia. We therefore recommend requesting information on forthcoming legislation from the Ministry of Justice and Digital Affairs.

Conclusion

In conclusion, it is necessary for you to determine the legal basis for such processing, comply with the data protection principles, including the obligations arising from Article 5 of the GDPR, conduct a DPIA if needed. We recommend contacting a legal adviser for assistance to comply with GDPR.

Hope this answer helps you.

Respectfully

Grete-Liis Kalev
lawyer
authorized by Director General