REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Juliane Stall
Healiomed
juliane@healionmed.com

Yours: 17.07.2025

Ours: 29.07.2025 nr 2.2-9/25/2340-2

Answer to request

Estonian Data Protection Inspectorate (DPI) has received request where is written:
We are reaching out as the developers of a new telemedicine platform established in Estonia. As we expand our operations within the European Union, we are committed to ensuring full compliance with the General Data Protection Regulation (GDPR) and related Estonian data protection laws. Our platform does not store electronic health records or medical charts. We only collect limited personal data directly from patients, such as: Full name, Email address, Date of birth, Physical address, Brief description of symptoms (provided voluntarily by the user).
Given the nature of our service, we would appreciate your guidance on the key compliance measures we should implement. Specifically, we are looking for recommendations or official documentation regarding: The necessity of appointing a Data Protection Officer (DPO); Requirements for a Data Protection Impact Assessment (DPIA); Recommended safeguards for storing and processing basic patient data; Any Estonian-specific obligations that may apply to telemedicine platforms.

In light of the matters presented, DPI can provide general explanations regarding the processing of personal data.

Data protection requirements in Estonia are primarily set out in the General Data Protection Regulation (GDPR) and the Personal Data Protection Act.

We explain that Article 5(1)(a) of the GDPR states personal data must be processed lawfully, fairly, and in a transparent manner with respect to the data subject. Furthermore, data may only be processed (including collected, transferred, storaged etc.) for specified and legitimate purposes (Article 5(1)(b)), and only data that is necessary for those purposes may be collected (Article 5(1)(c)).

The list of legal basis for processing personal data is found in Article 6 of the GDPR. It is **the data controller's responsibility to explain and demonstrate the legal basis and purpose of data processing** (Article 5(2) GDPR). Special categories of personal data, which include an individual's health data, may be processed only if there is a legal basis under Article 9(2) of the GDPR. If there is no legal basis for processing personal data, such processing is unlawful.

Based on your referral to processing basic patient data (as if this is not health data), we find it necessary to clarify the concept of health data (special categories of personal data). According to Article 4, point 15 of the GDPR, health data refers to personal data related to the physical and

mental health of a natural person, including data concerning the provision of health care services to that person, which reveal information about their health status. Pursuant to Article 9(1) of the GDPR, health data is classified as a special category of personal data, and the legal bases for its processing are set out in the second paragraph of the same provision. In case C-21/23, the European Court of Justice has explained that the notion of health data should be interpreted broadly. In particular, if data allows conclusions to be drawn about the health status of an identified or identifiable individual, such data should be considered health data[1].

In any case, every data processor must think through their data processing procedures and inform data subjects before data processing begins.

It is essential to prepare privacy terms before collecting data, or refer to existing ones, explaining what data is processed, for what purpose, and on which legal basis. These terms help people understand what is done with their data. Therefore, privacy terms must be written in simple and understandable language, freely accessible and easy to find (e.g. on company´s website).

The data controller must follow the principles in Article 5(1) of the GDPR, be responsible for compliance, and able to demonstrate this (Article 5(2)). One principle includes ensuring adequate security, protecting data from unauthorized or unlawful processing and from accidental loss, destruction, or damage, using appropriate technical or organizational measures ("integrity and confidentiality", Article 5(1)(f)). So it is crucial that everyday security measures must be carefully observed—such as preventing data leaks due to weak systems or unauthorized transfers.

It's crucial for data controllers to understand that data subjects have a right to know how their personal data is processed and to whom it is shared (external parties like the Tax and Customs Board or Health Insurance Fund), as well as who processes it internally or via partners (e.g. accountants). That's why policies should be written down and introduced to data subjects before their personal data is processed. Data subjects may seek clarification from the controller and, if needed, contact the Data Protection Inspectorate.

We strongly recommend reviewing the Data Protection Inspectorate's general guide to data processing, which highlights key points every data controller should know.

You have the opportunity to read additional relevant information on Estonian DPI website www.aki.ee (however, it is mostly in Estonian):

- where to start when processing personal data and which are the main principles of personal data processing: Andmetöötluse põhimõtted | Andmekaitse Inspektsioon;
- appointing DPO: Andmekaitsespetsialisti määramisest;
- DPO tasks, knowledge, and skills: Andmekaitsespetsialisti ülesanded, teadmised ja oskused;
- about DPO-s on general guide: Isikuandmete töötleja üldjuhendi 3. peatükk;
- info about DPO-s in English: https://www.aki.ee/en/inspectorate-news-information-dpo-s/information-dpo-s.
- data protection impact assessment (DPIA) information leaflet (find here) is a helpful guide that explains when and how to conduct an impact assessment for the processing of personal data. It's prepared by the Estonian DPI and it helps to reach compliance with GDPR

[1] European Court of Justice 4.10.2024 decision nr C-21/23, p 78-81.

requirements.

- information about DPIA on EDPI general guide: 5. peatükk. Andmekaitsealane mõjuhinnang | Andmekaitse Inspektsioon.
- the information leaflet on data protection terms and consent (find here) provides an overview of what data protection terms are and what they must include. The leaflet also explains what constitutes consent (is it really given voluntarily), in which cases consent can be used as a legal basis, and in what format consent must be given.
- the information leaflet on compliance with the GDPR (find here) helps to understand better what personal data is, why its protection matters, and what the main responsibilities of a data processor are.
- Here you will find Estonian-language summaries of the guidelines and guidance materials of the European Data Protection Board Euroopa Andmekaitsenõukogu suunised | Andmekaitse Inspektsioon. English versions are available on EDPB website.

In conclusion, every company is processing different kind of data sets. Estonian DPI expects in every case systematical, well-thought-out and proven lawful data professing. To ensure that the processing of personal data is lawful, we recommend consulting legal advisors (such as a lawyer or attorney). They can provide the company based advice and solutions.

I hope our answer and references help.

Respectfully

Liina Kroonberg
lawyer
authorized by Director General