REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

DNAlyse
contact@dnalyse.com

Yours: 29.05.2025 nr

Ours: 13.06.2025 nr 2.2-9/25/1291-4

Answer to request

Estonian Data Protection Inspectorate (EDPI) has received your additional 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.[1] The Inspectorate does not provide legal aid. Legal aid is when a legal assessment is given regarding specific circumstances.

Firstly, as we stated in our last letter to your request, it is imperative that you establish clear roles, responsibilities and define the specific personal data that is being processed. As a data controller or a processor, it is your responsibility to comply with GDPR and decide whether a DPO is necessary according to Article 37 GDPR. Once the roles are clearly defined, you will gain a comprehensive overview of the data you will be processing and ensure a full understanding of your responsibilities for GDPR compliance.

If your core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale or processing on a large scale of special categories of data pursuant to Article 9, you are required to assign a DPO pursuant to the Article 37 (1) GDPR. GDPR does not define what is large scale, but you must factor in the number of data subjects concerned, the volume of data and/or the range, the duration, or permanence, of the data processing activity and the geographical extent of the processing activity.[2]

Below is a guideline issued by EDPI regarding the definition of large-scale processing:
- special categories of personal data or criminal data concerning 5,000 or more individuals;
- high-risk data concerning 10,000 or more individuals;
- other personal data concerning 50,000 or more individuals.[3]

Secondly, compliance with data protection regulations is the responsibility of the controller or the processor. DPO is not personally responsible for non-compliance with data protection requirements.[4] Additionally, member of the management board cannot hold a position as a DPO, if as a management member they determine the purposes and the means of the processing of personal data. The data protection officer may fulfil other tasks and duties, but controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests (Article 37 (6) GDPR).

[1] Response to Memoranda and Requests for Explanations and Submission of Collective Proposals Act § 3.
[2] Working Party 29 Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017, page 21.
[3] Isikuandmete töötleja üldjuhend. - 3. peatükk. Andmekaitsespetsialist (AKS) | Andmekaitse Inspektsioon
[4] Working Party 29 Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017, page 24-25.

To summarize, clearly define the personal data you collect, the legal basis for its collection, the scope of the data processing, and your specific role in handling that data. We recommend you read more about the concepts of controller and processor in the EDPB guidelines[5] and WP29 guidelines on DPOs.[6]

Respectfully

Grete-Liis Kalev
lawyer
authorized by Director General

[5] European Data Protection Board „Guidelines 07/2020 on the concepts of controller and processor in the GDPR“, Version 2.0, Adopted on 07 July 2021.
[6] Working Party 29 Guidelines on Data Protection Officers (‘DPOs’), Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017.