Attention! Please note that the translation of this document into the English language is for information only. Officially you have to address the supervisory authority, i.e. State Data Protection Inspectorate, in the Lithuanian language.

Data Protection Officer

The **Data Protection Officer (DPO)** is a new position provided for in the General Data Protection Regulation (GDPR) which is applicable in Lithuania and other European Union Member States since 25 May 2018.

What organisations must appoint a Data Protection Officer? The GDPR provides for that a DAP must be appointed by all public authorities and bodies and other organisations that – as a core activity – monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale. A PDO may be an employee of the organisation or a person from the outside.

You must give a notification of the appointed Data Protection Officer to the State Data Protection Inspectorate (SDPI).

ATTENTION! The notification must be signed by the manager or his/her authorised person and contain the following information:

- Name, registration number, contact details of the company, institution or organisation, i.e. the data controller or the data processor;
- Information if the DPO was appointed by the data controller or the data processor;
- Name and surname of the DPO;
- Position of the DPO *(in case of appointment of an employee of the data controller) or the name of the legal person (if the DPO is an employee of another legal person);*
- Address of the DPO;
- Telephone number of the DPO;
- E-mail address of the DPO;
- Other means of communication of the DPO.

How a notification of the appointed data protection officer may be provided to the State Data Protection Inspectorate

1. Using the electronic item delivery system **eDelivery** (delivery in the eDelivery system has legal and evidentially effect which is equivalent to delivery of registered mail);
2. Sending of documents signed by an **electronic signature** by e-mail ada@ada.lt;
3. Service of a document by **registered mail or delivery in person** in the premises of the SDPI;
4. Using the old **e-service (VDAI EPS)** provision system (electronic service system of the State Data Protection Inspectorate).

(Electronically provided documents must be drawn up so that the SDPI could recognise the format and content of the electronic document, identify the electronic signature and the person who has provided the documents).

In order to provide documents through the electronic service system (EPS), the documents of the established form indicated in the section “Form(s) of the Application” by the requested purpose of processing must be filled in and attach it as an annex to the order by clicking on the link “Order the service online”. A confirmation of receipt of the documents and forwarding of the documents for examination under the competence will be sent to you to the indicated e-mail address.

Key aspects of the position of the Data Protection Officer

Under the GDPR, it is mandatory for certain organisations, i.e. controllers and processors to designate a DPO. This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

A DPO may be an employee or another person from the outside who would be responsible for compliance with the personal data protection requirements.

Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis

In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

DPOs are not personally responsible in case of non-compliance with the GDPR by the organisation. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions. Data protection compliance is a responsibility of the controller or the processor.

DPOs must be enabled to effectively perform the DPO's tasks, DPOs must be given sufficient autonomy and resources to carry out their tasks effectively.

The DPO is recognised as a key player in the new governance system, Articles 37–39 of the GDPR lay down conditions for his or her appointment, position and tasks. For more details, please see 13 December 2016 Guidelines on Data Protection Officers No WP 243 of the Working Party under Article 29 of Directive 95/46/EC (hereinafter referred to as the "Guidelines").

Qualification of the Data Protection Officer

Article 37(5) of the GDPR) provides for that "the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39". Recital 97 of the Preamble to the GDPR sets forth that "the necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor."

The afore-mentioned Guidelines contain information which should be taken into account when appointing the DPO:

1. Level of expertise. The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.

2. Professional qualities. Although Article 37(5) of the GDPR does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. Furthermore, the DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.

3. Ability to fulfil its tasks. Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches.

Functions of the Data Protection Officer
Article 39(1) of the GDPR provides for that the DPO shall have at least the following tasks:

1. to **inform** and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
2. to **monitor** compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
3. to **provide advice** where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
4. to **cooperate** with the supervisory authority, i.e. the State Data Protection Inspectorate;
5. to act as the **contact point** for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.