Description of the Data Protection Officer (DPO) role at LUNEX

ABOUT THIS DOCUMENT

PURPOSE

This document describes the role of the Data Protection Officer (DPO) at LUNEX.

SCOPE

This document describes the role of the Data Protection Officer (DPO)

ROLES & RESPONSIBILITIES

DPO: owner of this document and creator/ advisor of data protection policies and processes

Employees: responsibilities are to read and this document and gain an understanding of the role and responsibilities of the Data protection Officer.

Lunex Board: Review and approval of this document

DEFINITIONS

Controller: LUNEX CEO

Processor: LUNEX Staff

Data Subject(s): Lunex Students (primarily)

Personal Data: any information relating to an identified or identifiable natural person ('data subject'), in particular a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

RELATED LEGISLATION & DOCUMENTS

GDPR Regulations Document

APPENDIX/ APPENDICES

n/a

REVISIONS

Version	Date
1st Draft	12.05.2020

APPROVAL

Date	Name	Signature

Description of the Data Protection Officer (DPO) role at LUNEX:

1. The GDPR Regulations state that the designation of a DPO is an obligation if its core activities consist of at least one of the situations below:

    - if the processing is carried out by a public authority or body (irrespective of what data is being processed)
    - if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
    - if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

Therefore, as LUNEX undertakes processing operations on a large scale, it is obliged to appoint a Data Protection Officer.

Definitions:

- '**Core activities'** - considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity
- '**Large scale'** - The GDPR does not define what constitutes large-scale processing but recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
    - the number of data subjects concerned - either as a specific number or as a proportion of the relevant population
    - the volume of data and/or the range of different data items being processed
    - the duration, or permanence, of the data processing activity
    - the geographical extent of the processing activity

2. The DPO should be accessible:

To ensure that the DPO is accessible, the GDPR recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union. However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union, a DPO may be able to carry out his or her activities more effectively if located outside the EU.

When the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and 'person in charge' of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all applicable requirements of the GDPR. 23

3. Professional qualities of the DPO:

The DPO 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 his or her tasks.

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. 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.

Relevant skills and expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- understanding of the processing operations carried out
- understanding of information technologies and data security
- knowledge of the business sector and the organisation
- ability to promote a data protection culture within the organisation

4. What resources should be provided to the DPO by the controller or the processor?

The DPO must have the resources necessary to be able to carry out his or her tasks.

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- active support of the DPO's function by senior management
- sufficient time for DPOs to fulfil their tasks
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- official communication of the designation of the DPO to all staff
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- continuous training

5. What are the safeguards to enable the DPO to perform her/his tasks in an independent manner? What does 'conflict of interests' mean?

Several safeguards exist in order to enable the DPO to act in an independent manner:

- no instructions by the controllers or the processors regarding the exercise of the DPO's tasks
- no dismissal or penalty by the controller for the performance of the DPO's tasks
- no conflict of interest with possible other tasks and duties

The other tasks and duties of a DPO must not result in a conflict of interests. This means, first, that the DPO cannot hold a position within the organisation that leads him or her to

determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

6. The main task of the DPO is to monitor compliance

As part of these duties to monitor compliance, DPOs may, in particular:

- collect information to identify processing activities
- analyse and check the compliance of processing activities
- inform, advise and issue recommendations to the controller or the processor
- DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Data protection compliance is the responsibility of the controller or the processor.

7. The role of the DPO with respect to data protection impact assessments and records of processing activities?

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements

8. Maintaining Records

As far as the records of processing activities are concerned, it is the controller or the processor, not the DPO, who is required to maintain records of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.