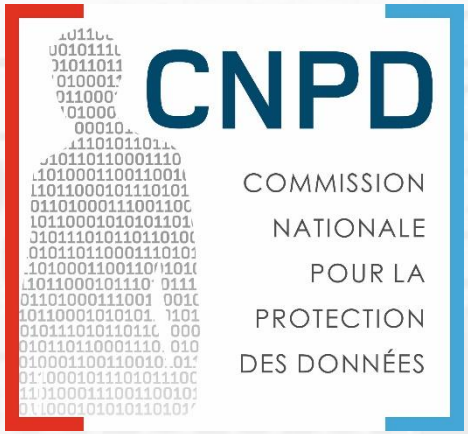
Information sessions

The General Data Protection Regulation

The role of the future Data Protection Officer (DPO)



19th October 2017

Esch-sur-Alzette (Belval)

Thierry Lallemang

Commissioner

I. The guidelines of Art. 29 WP on the DPO

1. Designation of a DPO

1.1 Mandatory designation of a DPO

1.2 Voluntary designation of a DPO in all other situations

1.3 Shared DPO

1.4 The profile of a DPO: expertise and skills

1.5 Internal or external DPO

2. Position of the DPO

3. Tasks of the DPO

II. The transition between the "*chargé de la protection des données*" under the Act of the 2 August 2002 and the data protection officer (DPO) under the GDPR

1. In relation to the designation

2. In relation to the position

3. In relation to the tasks

I. Guidelines of Art. 29 WP

- The Article 29 WP (working party composed of all EU data protection authorities) adopted on 5 April 2017 guidelines on Data Protection Officers (WP243).

- The guidelines are focused on 3 issues:

  - **The designation of a DPO (art. 37 GDPR)**

  - **The position of a DPO (art. 38 GDPR)**

  - **The tasks of a DPO (art. 39 GDPR)**

I. Guidelines of Art. 29 WP
1. Designation of a DPO (art. 37)

1.1 Mandatory designation of a DPO

Designation of a DPO **is mandatory** in **3 cases** (art. 37(1)) where**:**

a) the processing is carried out by a **public authority or body**, except for courts acting in their judicial capacity;

b) the **core activities** of the C or the P 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**;

c) the **core activities** of the C or P consist of processing on a **large scale** of **special categories of data** pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10;

The provisions of article 37 apply both to the controller (C) as well as to the processor (P).

- **a) public authority or body**

- Notion of public authority or body → no definition in the GDPR
  → necessary to refer to national law.

- Some public service missions may be carried out by organizations which do not have a public status. It is recommended that such organizations also designate a DPO.

1. Designation of a DPO

b) the **core activities** of the C or the P 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**

- Notion of **« core activities »**: The requirement to designate a DPO is analysed having regard to the « key » data processing activities, operated by the C or the P to achieve the objectives of its **primary activity**

→ **inextricable part** of the C's / P's activity

- *Example: The core activities of a bank require the processing of financial data of clients. The bank must also process HR data but it is an **ancillary activity**.*

1. Designation of a DPO

- Notion of **« large scale »** is also not defined in the GDPR. It remains to the C/P to carry out this analysis based on criteria such as:
  - The number of data subjects concerned (specific number or as a proportion of the relevant population)
  - The volume of data
  - The duration, or permanence, of the data processing activity
  - The geographical extent

- *Examples:*
  - *Processing of patient data by a hospital (contrary to processing of patient data by an individual physician);*
  - *Processing of data by an insurance company or a bank;*
  - *Processing of data (content, traffic, location) by telecom or internet service providers;*

1. Designation of a DPO

- Notion of **regular and systematic monitoring** is not defined, but it clearly includes all forms of surveillance, tracking and profiling on the Internet and is not limited to the online environment.
- A data processing is systematic when it is methodically organised, pre-arranged or carried out as part of a strategy.
- It is regular when there is a particular recurrence/periodicity/constancy in the implementation of the data processing.
- *Example: A bank which must systematically and regularly follow the evolution of the accounts and the transactions of its clients especially for complying with its obligations to prevent fraud, money-laundering or terrorist financing.*

1. Designation of a DPO

c) the **core activities** of the C or P consist of processing on a **large scale** of **special categories of data** pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10;

As a reminder, **special categories of data** refer to :

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- Data concerning health or a natural person's sex life or sexual orientation;
- Genetic data;
- Biometric data;
- Data relating to criminal convictions and offences;

Example: A hospital processes health and genetic data

1. Designation of a DPO

- Except in cases where it is obvious that the designation of a DPO is not required, it is recommended that the C/P documents the analysis undertaken to determine whether a DPO should or should not be designated.

- The compulsory designation of a DPO for a C does not automatically trigger the requirement for a P to also designate a DPO and vice versa. The criteria need to be analysed individually on a case by case basis for each C or P.

Example: A small local family business, active in the distribution of household appliances uses the services of a P whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively limited activities. However, the activities of the P, having many customers like this small enterprise, taken together, are carrying out large-scale processing and must therefore designate a DPO. At the same time, the family business itself is not under an obligation to designate a DPO.

1. Designation of a DPO

1.2 Voluntary designation of a DPO in all other situations

- It is always possible to designate a DPO on a voluntary basis. In that case all legal requirements (art. 37-39) will apply to his or her designation, position and tasks as if the designation had been mandatory.There is **no difference in status** between a DPO designated on a **voluntary or mandatory basis.**

1.3 Shared DPO

- A **group of undertakings** or several public authorites or bodies can designate a single DPO provided that he or she is **easily accessible from each establishment or body**. (art. 37(2))

  The notion of **accessibility** refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority but also internally within the organisation, considering that one of the tasks of the DPO is to inform and advise the C and the P as well as the employees.

- In order to ensure that the DPO, whether internal or external, is effectively and easily accessible, it is important that the **contact details of a DPO** (postal address, dedicated phone number and email address *(dpo@nameofcompany.lu)*) are available which means that the C/P must make them publicly available and communicate them to the supervisory authority. The supervisory authority, but not necessarily the public, must be informed of the name of the DPO.

1. Designation of a DPO

1.4 The profile of a DPO: expertise and skills

- 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 tasks (art. 37(5)).
- The **level of expertise** is not defined, but it must be commensurate with the sensivity, complexity and amount of data processed by the C/P.
- The necessary skills and expertise should, in particular, include:
  - *In-depth understanding of national and european data protection laws and practices*
  - *Knowledge of the data processing operations carried out by the C/P*
  - *Knowledge in the field of information system and data security*
  - *Knowledge of the business sector and of the organisation of the C/P*
  - *Ability to foster a data protection culture within the organisation*
- ***The DPO will no longer be approved by the CNPD***

1. Designation of a DPO

1.5 Internal or external DPO

- The function of the DPO can be exercised by an **employee** (**internal DPO**) or on the basis of a service contract concluded with an **external** individual or an organisation outside of the C's/P's organisation (art. 37(6)). All the requirements set out in articles 37 to 39 also apply to the external DPO.

- When the function of the DPO is exercised by an external contractor, a **group of persons** working for the contractor, who must comply with all the conditions and requirements of the GDPR (e.g. no conflict of interest), can fulfil the tasks of the DPO as a team. All the members of this team benefit from the protections relating to the DPO set out in the GDPR.

- For reasons of legal certainty, it is recommended that the service contract clearly specifies the allocation of tasks within the external DPO team and assigns a single individual as a « lead » contact and « in charge » for each client.

I. Guidelines of Art. 29 WP

2. The position of the DPO (art. 38)

- The C/P must ensure that the **DPO is involved, from the earliest stage possible** in all issues relating to data protection (art. 38(1)). Thus, the opinion of the DPO should be integrated at the earliest stage of the design of data processing operations (privacy by design and by default) in particular when carrying out a DPIA. Therefore, the C/P should, for instance, ensure that:
  - The DPO is regularly invited to participate in meetings of senior and middle management
  - The DPO has the opportunity to be present when decisions related to data protection are taken
  - The opinion of the DPO is always taken into consideration; it is good practice to document the reasons not to follow the opinion of the DPO, should there be a disagreement between the management and the DPO
  - The DPO should be promptly consulted in case of a data breach
- **Good practice:** Development of internal guidelines that set out when the DPO must be consulted

2. The position of the DPO

- Article 38(2) requires that the C/P assists the DPO by providing the **necessary resources** to accomplish his/her tasks.

- Therefore, in accordance with the scope, the type of data processing operations and the size of the C/P, the C/P should, in particular, provide the DPO with the following resources:

  - Active support of the DPO's function by senior management
  - Sufficient time for the DPO to fulfil his tasks
  - Adequate support in terms of financial resources, infrastructure and staff where appropriate
  - Official communication of the designation of the DPO to all staff members
  - Access to data of all services and departments within the organisation
  - Continuous training

2. The position of the DPO

- Article 38(3) provides some safeguards so that the DPO can freely and efficiently carry out his function. In that respect, he must be able to act in an **independent manner** without receiving any instruction from the C/P, and he should **not be dismissed or penalised (directly or indirectly)** for performing his task. The DPO shall directly report to the highest management level. He or she shall be submitted to professional secrecy or an obligation of confidentiality.

  Examples: Dismissal following a disagreement between the company's managers and the DPO as regard to the requirement to draft a DPIA; lack or delay in the DPO's career advancement.

- As a corollary to his independence, the other potential tasks of the DPO must not give rise to **conflicts of interests** with his function as a DPO (art. 38(6)). In particular, he must not be in a position to determine the purposes and means of data processing activities. This has to be considered on a case by case basis.

  Examples: Positions which can be considered as being incompatible with the postion of DPO: all management positions such as chief executive, chief operating, head of IT, chief financial, head of HR, chief medical officer, head of marketing etc… The activity of both Processor and external DPO at the same time for one Controller is also incompatible.

3. The tasks of the DPO (art. 39)

- The main tasks of the DPO are:
  - To inform and advise the C/P as well as all staff members on issues related to data protection
  - To monitor compliance with the provisions of the GDPR by the C/P
  - To provide advice to the C/P in relation to a data protection impact assessment (DPIA) and to monitor its performance
  - To take into account the risks associated with data processing operations when providing advice and analyses
  - To cooperate with and act as a contact point for the supervisory authority
  - → role of facilitator of the DPO in relation to CNPD
- It is up to the C/P, and not the DPO, to hold a record of processing activities; however, the DPO should be associated to the mapping of the proceesing activities.
- In any case, the **C/P always remains responsible** for the compliance with the regulation. This responsability **can not be transferred** to the DPO.

II. The transition between the "**chargé** de la protection des données" and the data protection **officer** (DPO)

- The Act of the 2 August 2002 **already allows** the C to designate a « **chargé de la protection des données (art. 40) »** on a voluntary basis.

- The DPO under the GDPR will be the natural successor of the actual « chargé de la protection des données »

- What are the similarities and differences between the current regime and the future one in relation to:

  - **The designation**

  - **The position**

  - **The tasks ?**

II. The transition to DPO

1. In relation to the designation

- **What is changing as of 25 May 2018?**
  - Contrary to the current regime for the « chargé », the designation of a DPO will be **compulsory** in the aforementioned 3 hypotheses.
  - The CNPD will **no longer approve the DPO**. Nevertheless, as previously stated, it is useful to document the decision to designate whether or not a DPO.
  - The **function** of DPO will be **more accessible** and will not be limited to persons having a university diploma in the field of law, economy, management, biological science, information technology or member of a regulated profession (lawyer, auditor, accountant and physician).
  - The designation of a DPO also apply to **processors**.
- **Similarities between the two regimes**
  - As with the « chargé de la protection des données », the DPO will also need to have professional integrity while performing his tasks and will be subject to professional secrecy.
  - As it is currently possible under national law, the GDPR also allows the use of **internal or external DPO**.

II. The transition to DPO

2. In relation to the position

- With the DPO, the key role of this function is reinforced. The **position/function** of DPO will be **« upgraded »** within an organisation; he/she must directly report to the senior management of the C/P.

- The current legal framework in Luxembourg is mainly focused on the time available to the « chargé de la protection des données » in order to accomplish his tasks. The GDPR expands this requirement which will encompass all the technical and human resources made available to the DPO for achieving his tasks.

- Even if the minimum requirement of annual training is not needed anymore (art. 1(2) of the « règlement grand-ducal of 27 november 2004 »), the DPO must regularly update his abilities and knowledge.

- Like the « chargé », the DPO is independent and there should be no conflict of interest with other tasks assigned to him/her.

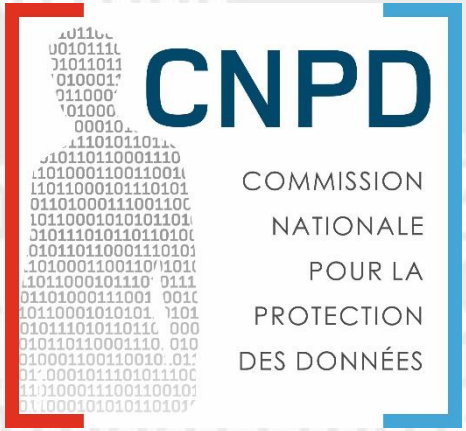
3. In relation to the tasks

- The tasks of the DPO are more demanding than those of the « chargé ».
- Ensuring the implementation of a coherent data protection policy within the C/P, applied and followed by all those involved in the data processing activities, requires someone gifted with a broad range of professional and personal skills.
- The currently active « chargés de la protection des données » have a head start as regard to this transition since they intimately know the structure and organisation of the C as well as already understand the risks related to the data processing activities.
- The Regulation does not require the DPO to provide a copy of the record of processing operations unlike the « règlement grand-ducal of 27 november 2004 » (art. 4) for the « chargé de la protection des données ». Nevertheless, as stated earlier, it is recommended that the DPO should be closely associated with the keeping of this record, as it is an important element for the C/P to demonstrate compliance with the GDPR.

Thank you for your attention !

Questions?

Commission nationale pour la protection des données



1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu