Funded by European Union's Rights, Equality and Citizenship Programme (REC)

DPO – CISO – Privacy Team

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

(www.bydesign-project.eu)

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The DPO – role and responsibilities

- The controller and the processor shall designate a data protection officer (DPO) when:
  - the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
  - the core activities of the controller or the processor 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
  - the core activities of the controller or the processor consist of processing on a large scale of special categories of data (art. 9-10 of the GDPR).
- A group of undertakings may appoint a single data protection officer
  - provided that a data protection officer is easily accessible from each establishment.
- For public authority or body: A single DPO may be designated for several authorities or bodies
  - taking account of their organisational structure and size.
- The DPO shall be designated on the basis of professional qualities
  - Expert knowledge of data protection law and practices and the ability to fulfil the tasks (see next).
- The DPO may be a staff member or fulfil the tasks on the basis of a service contract.
- The controller or the processor shall publish the contact details of the DPO and communicate them to the supervisory authority.

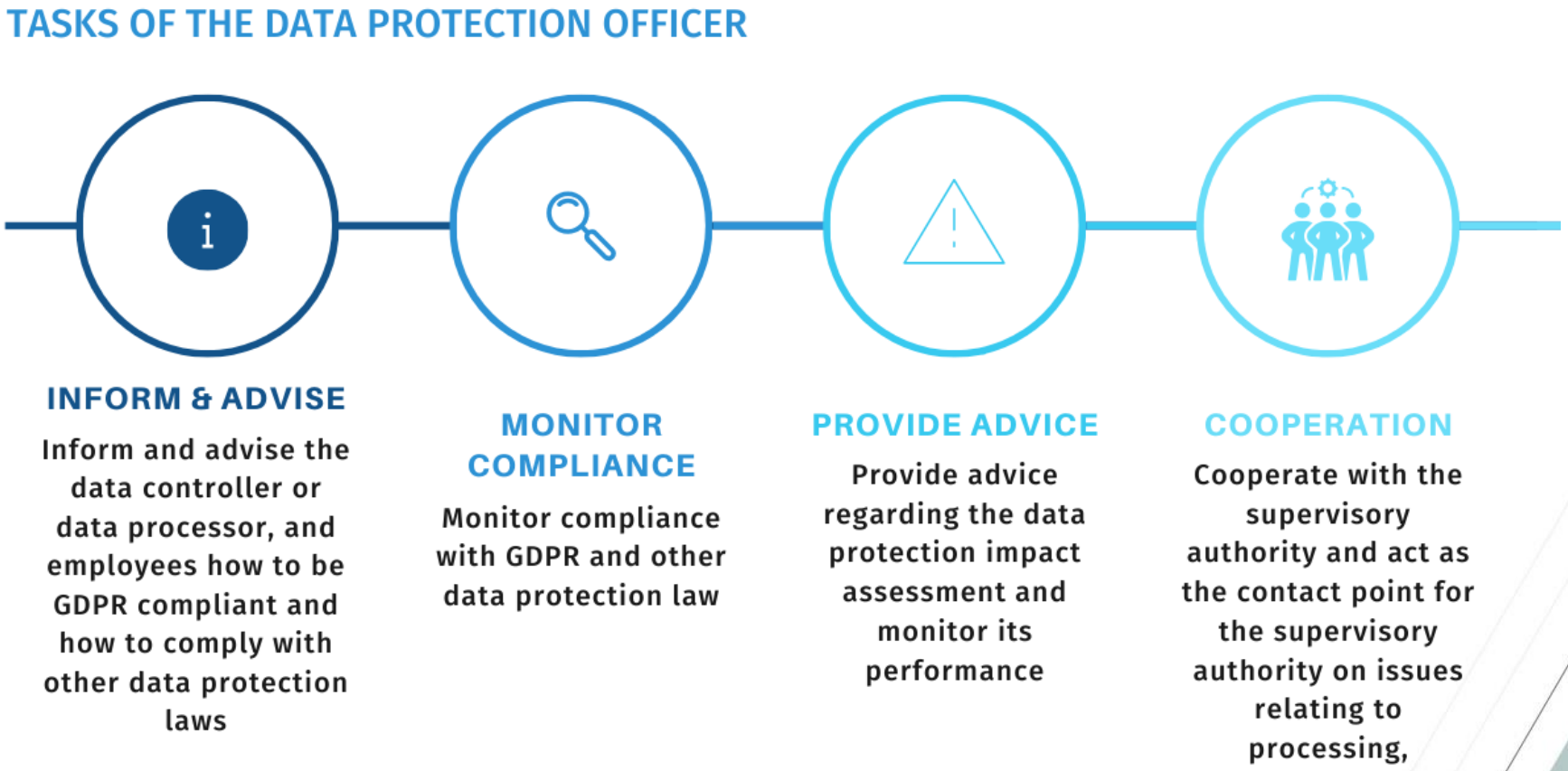
Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The DPO – role and responsibilities

- The controller and the processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- The controller and processor shall support the DPO in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
- The controller and processor shall ensure that **the DPO does not receive any instructions regarding the exercise of those tasks**. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The DPO shall directly report to the highest management level of the controller or the processor.
- Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under GDP.
- The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
- The DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties **do not result in a conflict of interests**.

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The DPO – role and responsibilities



Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The DPO – role and responsibilities

- The DPO shall have at least the following tasks:
  - 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;
  - 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;
  - to **provide advice** where requested as regards the data protection impact assessment and monitor its performance;
  - to **cooperate** with the supervisory authority;
  - to act as the **contact point** for the supervisory authority on issues relating to processing, including the prior consultation for a data protection impact assessment, and to consult, where appropriate, with regard to any other matter.

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The DPO – role and responsibilities

You should position the DPO in line with the following criteria:

- DPO reports directly to your highest level of management and is given the required independence to perform their tasks
- DPO is involved in all issues relating to the protection of personal data
- DPO is sufficiently well resourced to perform tasks
- DPO is not penalized for performing their duties
- Any other tasks or duties do not result in a conflict of interest with their role as a DPO

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Chief Information Security (CISO) responsibilities[1]

· *Act as* the organization's *representative* with respect to inquiries from customers, partners, and the general public regarding the organization's security strategy.

· *Act as* the organization's *representative* when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees.

· *Balance security needs* with the organization's strategic business plan, identify risk factors, and determine solutions to both.

· *Develop security polices* and procedures that provide adequate business application protection without interfering with core business requirements.

· *Plan and test responses to security breaches*, including the possibility for discussion of the event with customers, partners, or the general public.

· *Oversee* the selection *testing, deployment, and maintenance* of security hardware and software products as well as outsourced arrangements

· *Oversee* a staff of *employees* responsible for organization's security, ranging from network technicians managing firewall devices to security guards

(1. Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer, Matthew Cho, SANS GSEC Certification, Practical Assignment Option 1.4 – Research on Topics in Information Security, 2021 SANS Institute)

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

DPO and CISO relationship and possible conflict of interest

- Initial position of the Belgian DPA (BDPA): very strict delineation (20 April 2020)
  - BDPA's Litigation Chamber: "the role of head of a department is […] incompatible with the role of DPO" because the DPO cannot carry out any independent supervision of such a department, even though the departments in question (e.g., Risk) had an advisory function
- DPA changes course: new insights following a decision of April 26, 2021
  - the DPO at the financial institution could combine the role of DPO with a role as CISO
    - the CISO "presents to the Management of the company the risks and their importance and […] it befalls Management to decide whether the measures put in place are sufficient to mitigate the risks";
      "in case of disagreement between [the CISO] and Management regarding the measures taken and notwithstanding the comments submitted to [Management], it is not [the CISO]'s decision to make";
      "security measures fall within the scope of the IT department, not that of the CISO"
- DPO and CISO roles may be compatible if purely advisory

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Privacy team

- team should be familiar with the operations and privacy needs of
  - Chief privacy officer
  - Privacy manager
  - Privacy analyst
  - Business line privacy leaders
  - First responders- incident response and security computer incident response team
  - Data Protection Officers
- no particular qualifications or certifications specified in the GDPR, but organizations should consider the *necessary skills and expertise* to include:
  - expertise in national and European data protection laws and practices, including an **in-depth understanding of the GDPR**
  - the apprehension of the **processing operations** carried out;
  - understanding of **information technologies** and data security;
  - insight into the **business sector** and the organization; ability to **promote a data protection culture** within the organization.