



Data Protection Officer Position Description

1.0 Purpose

To provide our members a template that can be modified and used to hire and select an employee for your company to serve as a Data Protection Officer (DPO), as required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements. The primary role of the DPO to ensure that the organization's processes to collect, use and store sensitive data of its staff, customers, providers or any other individuals (also referred to as data subjects) follows the applicable data protection rules.

DPOs may be an organizational staff member, and related organizations may utilize the same individual to oversee data protection collectively, as long as the DPO is easily accessible to anyone at those related organizations. It is required that the contact information about the DPO be published publicly and provided to all regulatory oversight agencies. DPOs must not have a conflict of interest, meaning that the DPO must not have any current duties or responsibilities that are in conflict with their monitoring responsibilities.

An organization is required by GDPR to have a DPO if the size of the data collection and handling is of a "large scale". While there are not exact guidelines around the scale of data handling, most small businesses will not be required to hire a DPO, unless their **core focus** is on data collection or storage. Other factors GDPR regulators use to assess "large scale" are the data subjects, the data items, the length of data retention and the geographic range of processing.

2.0 Duties

PROGRAM DEVELOPMENT AND OVERSIGHT

- Educating the company and employees on important compliance requirements.
- Training staff involved in data processing.
- Conducting audits to ensure compliance and address potential issues proactively.
- Serving as the point of contact between the company and GDPR Supervisory Authorities.
- Monitoring performance and providing advice on the impact of data protection efforts and reporting any compliance failure to company leadership.
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purposes of all processing activities, which must be made public on request.
- Interfacing with data subjects to inform them about how their data is being used, their right to have their personal data erased, and what measures the company has put in place to protect their personal information.
- Ensure that data controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them.

Still have questions, need help?

Contact us at our "Ask-an-Expert" service, web@thencss.org or visit us at the link below.



Data Protection Officer Position Description

- Give advice and recommendations to the company about the interpretation or application of the data protection rules.

DPO Candidate Skills Required:

- Experience in data protection and legal compliance.
- Solid knowledge of GDPR and national data protection laws.
- Knowledge of data processing operations in the company's sector is preferable.
- Familiarity with computer security systems.
- Ability to handle confidential information.
- Ethical, with the ability to remain impartial and report all noncompliance.
- Organizational skills with attention to detail.
- Demonstrated leadership skills achieving stated objectives involving a diverse set of stakeholders and managing varied projects.
- Demonstrated negotiation skills to interface successfully.
- Demonstrated client relationship skills to continuously coordinate with other company personnel while maintaining independence.
- Demonstrated communication skills to speak with a wide-ranging audience, from the board of directors to data subjects, from managers to IT staff and lawyers.
- Demonstrated self-starter with ability to gain required knowledge in dynamic environments.
- Demonstrated record of engaging with emerging laws and technologies.
- Experience in legal and technical training and in awareness raising.
- Experience in dealing successfully with different business cultures and industries.
- Professionally licensed as a lawyer, an information security or privacy professional.

Still have questions, need help?

Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.