TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

DATA PROTECTION OFFICER (DPO)

A Guide to Foster Data Security Culture in Organizations

@tataadvanced | contactcs@tataadvancedsystems.com | www.tataadvancedsystems.com

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Need for DPOs is gaining momentum with the rising spike of data breaches globally. As per the Internation Association of Privacy Professionals (IAPP), around half-million organizations registered data protection officers across Europe in 2019. Businesses are experiencing the necessity to secure their corporate data, revamp security approaches, and align themselves with different data protection laws governing the collection, utilization and disclosure of personal data.

Data Protection Officer (DPO) is an expert responsible for ensuring compliance with data protection laws, like GDPR and PDPA, and nurturing the tradition of data protection within an organization. The DPO works together with other functional units engrossed in the processing of personal data as it helps in attaining detailed visibility into the regulatory and data segment of an organization.

Explore more about the responsibilities, challenges and other important aspects of a DPO.

What functions does a DPO perform?

A DPO executes a myriad of tasks to ensure that the organization fulfils all the requirements of protecting business-critical data.

Have a look at some primary functions of a DPO that will help you understand the importance of its role.

- Designing and implementing policies and processes for managing personal data to ensure compliance with data protection laws.
- Guiding organizations and their employees on data protection obligations.
- Reviewing organizations' internal data security strategies, which may include (but not limited to) allocation of responsibilities, internet audits, training of individuals engaged in the processing of personal information, etc.
- Handling issues (raised by data subjects, public authorities or relevant supervisory authorities) related to data protection, data breach, Data Subject Access Requests (DSARs), etc.
- Regular evaluation of data processing activities to monitor compliance with data protection laws.
- Reporting to concerned authorities in case of security risks that might occur concerning sensitive personal information.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Who needs to appoint DPO?

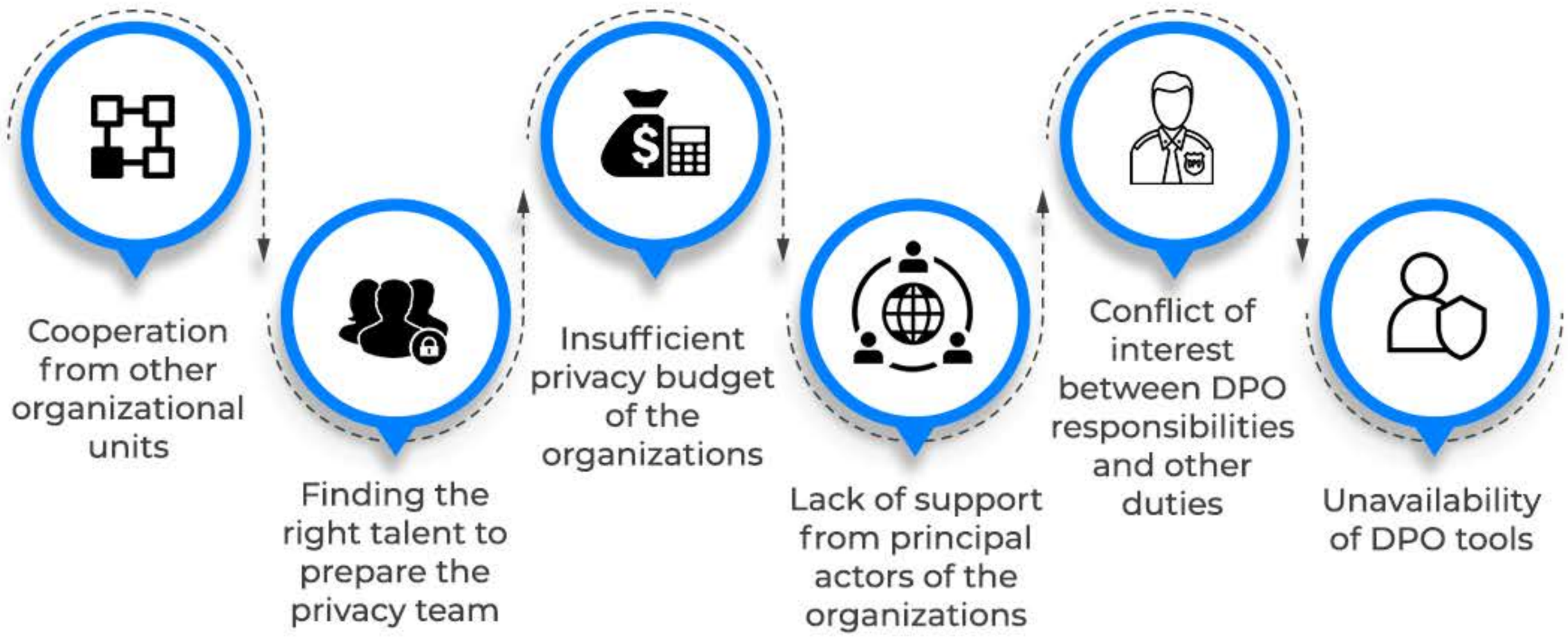
An organization is required to hire a DPO if:

- It is a public institution or body (except for courts).
- Its core activities require large scale, regular and systematic monitoring of data subjects (such as employees and customers).
- Its core activities include processing of sensitive, personal information that may include (but not limited to) health information, criminal records, etc.

Besides above-mentioned factors, an organization can voluntarily hire a DPO as a matter of good practice. Also, the DPO doesn't need to be hired internally. Organizations can also outsource the role of a DPO to address the compliance demands of the data protection laws.

What challenges does a DPO face?

While addressing the requirements for an organization to achieve compliance with data protection laws and create a safe environment for data processing, a DPO has to go through several challenges including (but not limited to):



TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Why choose us?

- Vast array of working experience with different sectors
- Result-oriented and customer-centric approach to data protection
- Pool of professionals having extensive experience in data security and privacy

To start your data protection journey, connect with us at
contactcs@tataadvancedsystems.com