COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
The Role of the Data Protection Officer in Europe

By Robert Bond[1]

The EU General Data Protection Regulation[2] (GDPR) came into force on May 25, 2018, and has, at long last, given the role of the data protection officer (DPO) a pan-European legislative construct.

This article will look at examples of the roles and responsibilities of the DPO in Europe.

Previous Position

Prior to the GDPR, many multinationals already had a chief privacy officer or chief data privacy officer, and whilst there were a number of EU member states, such as Germany, that specifically referenced the role of the DPO, there was no harmonized approach.

Before the GDPR, some European jurisdictions had mandates or legislation for the appointment of the DPO, for example Germany, France, Hungary, Slovenia, Russia, and Poland. Where a DPO was appointed, they were empowered to ensure that the data controller was compliant with all aspects of applicable data protection laws and regulations, and in some jurisdictions, the contact details of the DPO may have been required to be registered with the relevant data protection authority (DPA).

In a number of jurisdictions, the formal appointment of a DPO negated the requirement for notification or registration of the data controller with the relevant DPA. It was the duty of the DPO to maintain a compliance register and to oversee the management of processing personal data that would have otherwise been covered by a notification or registration process.

DPO Responsibilities

Currently in the EU, one of the first responsibilities of the DPO is to manage notifications or registrations with the relevant data protection authority regarding data processing fees (in the UK) and the details of the DPO in all EU member states. In addition, specific notifications fall within the responsibility of the DPO where those notifications relate to notifications of data breaches for cyber incidents. Another general responsibility of the DPO is to monitor the activities of all data controllers within the DPO's corporate group, including human resources, sales and marketing, IT, procurement, and outsourcing.

The DPO needs to have in place a policy and procedure that ensures liaison with relevant departments regarding any changes to processing activities, such as human resources in relation to staff, leavers, job interviews and recruitment, background checks, new members of staff, and the use of agents or subcontractors.

The DPO is or should be a C-suite person who has direct reporting to the management in respect of data protection and related compliance issues. The DPO must have the autonomy and related budget and decision-making powers to manage non-compliance and related events, including reporting of such incidents to the relevant DPA.