Luxembourg Regulator Imposes Fines For Data Protection Officer GDPR Non-Compliance

Date : November 5, 2021

Introduction

Under both UK and EU GDPR, where certain criteria are met organizations are required to appoint a Data Protection Officer ("DPO"). Many organizations choose to appoint a DPO on a voluntary basis, to which the same high standards as a mandatory DPO must apply. A DPO can be appointed internally (i.e. a staff member) or outsourced (an organization or an individual).

Broadly-speaking, a DPO's tasks are to:

- Inform and advise an organization and its employees of their obligations under GDPR and other domestic data protection law;
- Monitor compliance with GDPR and other domestic data protection law and with the organization's data protection policies;
- Provide advice where requested as regards Data Protection Impact Assessments (DPIAs);
- Co-operate and consult with data protection regulators and act as a contact point with them about data protection issues; and,
- Receive and handle communications from data subjects, both within and outside the organization.

It will also be important for a DPO to handle Subject Access Requests, investigate and manage data security breaches, keep records of data processing activities, horizon scan on data protection developments and trends, and foster a good and robust data protection culture within an organization.

Compliance failure with regard to GDPR DPO requirements can result in financial sanctions being imposed on an organization as can be seen in a number of recent decisions of the Luxembourg data protection regulator (Commission nationale pour la protection des données/Nationale Kommission für Den Datenschutz). This article briefly looks at these cases and sets out some takeaways.

What are the cases about?

In two August 2021 decisions and two October 2021 decisions, following targeted audits (including site visits) of a number of organizations by the Luxembourg regulator which examined eleven DPO requirements (also relying on EU guidance about DPOs), the regulator found on the facts that four (unnamed) companies had acted inadequately and amongst them each infringed several of the following GDPR obligations:

- The requirement that a DPO must be designated on the basis of professional qualities, notably their expert knowledge of data protection law and practices, and their ability to fulfil their GDPR prescribed tasks (Article 37(5) GDPR);
- The requirement for an organization to publish the contact details of a DPO and communicate them to the regulator (Article 37(7) GDPR);
- The requirement for an organization to ensure that a DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data (Article 38(1) GDPR);
- The requirement for an organization to support the DPO in carrying out their GDPR prescribed tasks by providing resources necessary to fulfil those tasks and access to personal data and processing operations, and to maintain a DPO's expert knowledge (Article 38(2) GDPR);
- The requirement for a DPO to not receive any instructions regarding the exercise of their tasks (they cannot be dismissed or penalised by the organization for performing their tasks, and, the DPO reports directly report to the highest management level in the organization) (Article 38(3) GDPR);
- The requirement that whilst a DPO may fulfil other tasks and duties these must not result in a conflict of interests (Article 38(6) GDPR);

- The requirement for a DPO to inform and advise the organization and those employees who process personal data of their GDPR and domestic data protection law obligations (Article 39(1)(a) GDPR); and,
- The requirement for a DPO to monitor compliance with GDPR and domestic data protection law obligations, and the organization's data protection policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits (Article 39(1)(b) GDPR).

For infringing these requirements the companies were respectively fined: €10,700; €6,600; €13,200; and, €18,000;

In addition, three of the companies were officially ordered to take measures to rectify a number of these infringements (within 4 months for two of the companies and within 6 months for one of the companies).

What are the takeaways?

The takeaways are that businesses should consider doing a compliance check on their existing DPO's appointment or for the appointment of a DPO, whichever is applicable – the issues to be addressed could include the following:

- Either check and update where need be an existing list or job description and role profile, or create a new document, that sets out the DPO's duties, tasks and responsibilities;
- Ensure that the DPO has the necessary resources to be able to carry out their tasks, including access to personal data and processing operations and resources to allow the DPO to maintain their expert knowledge;
- Review/determine the relationship between the DPO and senior management;
- Determine whether there are there any possible current or future conflicts of interest – if this seems to be the case, consider re-assigning some of the DPO's roles and responsibilities. Those who are likely to determine the purposes and means of processing personal data and therefore will be in a position of conflict include: the CEO; the COO; the CFO; the Chief Medical Officer; the head of marketing; the head of HR; and, the head of IT;
- Check local law requirements concerning DPOs – we understand that under German law the thresholds for the appointment of a DPO are lower than those specified under EU GDPR and so more organizations will be caught by these requirements than under EU GDPR requirements;
- Ensure that the DPO's contact details are published internally and externally;
- When recruiting a DPO make sure that they have the expertise and experience to undertake the DPO role (knowledge of GDPR and domestic data protection rules is a must and IT and sector expertise are important) – whether recruiting a DPO to work internally or as an external contractor do proper and thorough due diligence;
- If an external DPO is appointed make sure that they are properly involved and in a timely manner in the organization's data protection decision-making processes, and ensure that there is a direct reporting line to the organization's highest management level – someone internal will also need to be appointed as the contact person for the external DPO; and,
- Take the opportunity to update and/or revise any data protection risks that require the DPO's involvement. For example, in light of the Covid-19 pandemic has a Data Protection Impact Assessment ("DPIA") been done about employees returning to the office? Remember that under GDPR a DPO's advice must be sought when a DPIA is being carried out.

Resources

Cordery's GDPR Navigator subscription service is an expansive set of resources and a community of peers helping companies deal with GDPR and related issues. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

We've written previously about DPO compliance failure as regards conflicts of interest here https://www.corderycompliance.com/belgian-dpa-dpo-fine/. We have also done a podcast about DPOs here https://www.corderycompliance.com/countdown-to-gdpr-episode-2-the-role-of-a-data-protection-officer/.

The Luxembourg regulator's rulings can be found here (in French) https://cnpd.public.lu/en/decisions-sanctions.html.

We report about data protection issues here https://www.corderycompliance.com/category/data-protection-privacy/.

We report about compliance issues here https://www.corderycompliance.com/news/.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com