Belgian Regulator Imposes Euro 50,000 Fine for Non-Compliance with Data Protection Officer GDPR Requirements

Date : May 19, 2020

Introduction

Under the EU General Data Protection Regulation ("GDPR"), where certain conditions are met it is mandatory for an organisation to designate a Data Protection Officer ("DPO"). GDPR also sets out a number of conditions for the DPO's appointment concerning their role and tasks. These include the requirement that whilst a DPO can fulfil other tasks and duties the data controller or data processor appointing the DPO must ensure that these tasks and duties do not result in a conflict of interest. The Belgian Data Protection Authority (the "Belgian DPA") recently imposed a fine of €50,000 ($54,203) on an organisation for non-compliance with the GDPR conflict of interest requirement.

What's the case about?

Following a data breach notification (erroneously sent emails it seems) made by an unnamed organisation to the Belgian DPA, an investigation was undertaken of the data protection practices of the notifying organisation including the position of the organisation's DPO.

What was the outcome?

In a detailed and in-depth assessment, in what seems to have become a heavily disputed matter between the Belgian DPA and the organisation concerned, the Belgian DPA decided that although the DPO had been sufficiently involved in the data protection processes referred to in this matter (and so there was no infringement of this particular GDPR DPO requirement), by appointing as DPO the person who was the director of the separate compliance, risk management and audit departments, the organisation was non-compliant with the requirement to ensure that its DPO had no conflicts of interest. According to the Belgian DPA, there was no possibility of independent supervision by the DPO of each of these three departments, and the accumulation of these functions could lead to insufficient guarantees of secrecy and confidentiality towards employees (which are also GDPR DPO requirements).

Consequently, for infringing GDPR the Belgian DPA:

- Ordered the organisation to take measures to resolve the DPO issue by no later than July 31, 2020 (three months from the date of the decision); and,
- Imposed a fine of €50,000, in order to "vigorously enforce" GDPR.

The Belgian DPA took into consideration the following factors when it imposed the fine:

- The infringement was the result of "serious negligence" on the part of the organisation;
- The concept of a DPO was not a new one having been around for many years in many EU countries and organisations;
- EU guidance on DPOs (issued in 2016 and revised in 2017) was clear about the extent to which a DPO could also perform other functions within an organisation, taking into account the organisational structure specific to each organisation and assessed on a case-by-case basis;
- The organisation should have carefully prepared for the introduction of GDPR. Processing data was a core activity of the organisation which it did on a very large scale including sensitive/special category data – appointing a non-independent and non-conflict of interest free DPO had a potential impact on (according to the Belgian DPA) millions of individuals; and,
- The duration of the infringement, which was from May 2018, (GDPR's official start) to February 2020.

The Belgian DPA also stated that depending on the activities, size and structure of an organisation, it may be good

practice for data controllers and data processors to:

- Identify positions that may be incompatible with the DPO position;
- Draw up internal rules for this purpose in order to avoid conflicts of interest;
- Include a more general explanation of conflicts of interest;
- Declare that their DPO has no conflict of interest in their DPO function as a way of raising awareness of others about this requirement; and,
- Include safeguards in the organisation's internal rules and ensure that the vacancy for the position of DPO or the service contract is sufficiently detailed to avoid conflicts of interest – here the Belgian DPA noted that it had to be taken into account that conflicts of interest can take various forms depending on whether the DPO has been recruited internally or externally.

It is not known yet if the organisation will appeal this matter (i.e. before a court).

What are the takeaways?

First and foremost, don't have a DPO who is also the department head in your organisation where there is a conflict with that department's work or interests. The Belgium decision seems to suggest that any department head could be conflicted.

Second, do a compliance check concerning your existing DPO's appointment – the issues to be addressed should be wide-ranging and 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;
- Review 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; and,
- Check local law requirements concerning DPOs – Germany is an example of a jurisdiction that has some specific requirements with regard to DPOs.

Doing a review of the DPO's appointment may also be an 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 working from home? Remember that under GDPR a DPO's advice must be sought when a DPIA is being carried out.

Finally, obvious though this may seem, when recruiting a DPO make sure that they have the expertise and experience to undertake the DPO role (knowledge of GDPR is a must and IT expertise is important); whether recruiting a DPO to work internally or as an external contractor do proper and thorough due diligence.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For information about our Breach Navigator tool please see here: https://www.corderycompliance.com/solutions/breach-navigator/

We have written some data protection and Covid-19 FAQs which can be found here: https://www.corderycompliance.com/coronavirus-covid19-and-dp/

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

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary

The Belgian Data Protection Authority's judgement can be found here (currently only available in Dutch): https://www.gegevensbeschermingsautoriteit.be/beslissingen-ten-gronde-0

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