Client Alert: Belgian DPA Takes Action Over Leaver's Email Account

Date : October 16, 2020

Introduction

The Belgian Data Protection Authority (DPA) recently fined a small unnamed Belgian medical business €15,000 for breaching GDPR for failing to deactivate their email messaging system for a former employee. This meant that customer personal data could be accessed for an extended period. This brief article highlights a number of important issues raised in the case about what to do about former employee email accounts.

This note uses some GDPR terms which are explained at www.bit.ly/gdprwords. You can find some general background to GDPR here www.bit.ly/gdprfaq.

What's the case about?

The background is as follows:

1. The family-run medical company dismissed its CEO in November 2016. Later other members of the family seem to have also left. However, as at March 2019 seven professional e-mail addresses of various family members were still active, including for the former CEO who requested the company to stop using those e-mail addresses and close the email boxes;
2. Because the former CEO didn't get a reply he brought the matter to the Belgian DPA, following which, in a procedure that is particular to Belgium, there was an attempt at mediation to resolve the issue. But mediation failed and a complaint was brought and an official investigation was undertaken by the Belgian DPA's Inspection Service;
3. The investigation found that three e-mail addresses were still active, with no message being sent out to those who might email those email addresses to say that the individuals in question no longer used them. The company then closed these three email boxes and claimed that, when the individuals in question had left, their email boxes had been deactivated albeit with a company internal redirection function. The company said it did this because the individuals in question had occupied senior positions and the company hadn't wanted to lose important emails such as those concerning clients;
4. The Inspection Service recommended that the company block email messaging of former employees as soon as possible and set up an automatic message informing those contacting the email addresses about the departure of the employees. This is to be done for a reasonable period of time, which in its view was one month, after which the email account should be terminated. Further, it said that former employee email addresses must not be used under any circumstances at all. Finally, it stated that maintaining an email account without informing those contacting the email address that the individuals in question no longer used these e-mail addresses allowed for the potential collection and use of personal data of those sending emails to those email addresses without the senders knowing about this.

What did the regulator decide?

The Belgian DPA's Litigation Chamber then made an official decision in the case where it:

1. Imposed a fine of €15,000 on the company; and,
2. Ordered the company to introduce a policy that deals with email messaging closure and departing staff members, to also be sent to the Belgian DPA within three months.

The Belgian DPA stated that, based on the GDPR principles of purpose limitation, data minimisation and storage limitation, a data controller must block the email account of a departing employee, at the latest on the day of actual departure.

In addition, the employer data controller must also set up an automatic message for a reasonable period of time (one month) alerting those sending emails to that email address that the individual in question no longer works for

the employer, and provide an alternative contact name and details of who to contact in the organisation instead. The period of time could be longer according to the seniority of function of the individual in the organisation, but ideally no longer than three months. The reasons for extending the time should be set out and done in agreement with the individual in question - or at least the individual should be informed. During this period another solution to the issue would also have to be found. This was a better solution than simply redirecting emails internally, which could expose both recipient and sender's personal data. Once the time period came to an end the individual's email account would have to be terminated.

With regard to these factors above the company had breached the GDPR purpose limitation, data minimisation and storage limitation principles – closing the email addresses two and half to three years after departure was clearly unacceptable for the Belgian DPA.

The Belgian DPA also found that the company had no lawful grounds for processing the personal data in the way it had done – the Belgian DPA did seem to indicate that "legitimate interests" could provide the basis for lawful grounds for an organisation to continue its business in such circumstances, but for a short period only.

The Belgian DPA also found that the company had not complied with what constituted a Right to be Forgotten (or erasure) request by the former CEO when he requested the company stop using the e-mail addresses and close the email boxes in question, and so the company had also breached this GDPR obligation.

Practical tips

Businesses should consider either reviewing their existing policy on departing and former employee email accounts or creating a new policy. Issues to be addressed include the following:

1. Having a clear process for a departing employee – these could include a process to collect and/or delete their private emails prior to the employee's departure from the organisation;
2. Having a clear process where the organisation needs to recover content from the departing employee's email-box to ensure the good functioning of the organisation after the employee's departure – this action should usually take place prior to the employee's departure and in their presence;
3. Setting up automated email responses with clear information about the departure of the individual and who to contact within the organisation instead, to only go out for a brief and limited period of time unless this can be justified for a longer period;
4. Ensuring that the appropriate lawful grounds for the (brief) continued use of the departing employee's email has been determined, which may be "legitimate interests" in which case a "legitimate interests" assessment will need to be done;
5. Setting up a timed process to delete the content of the former employee's emailbox and completely shut down their email account;
6. Considering whether generic accounts rather than employee-specific accounts might be more appropriate for some functions; and,
7. Ensuring the organisation knows how to deal with data rights requests such as Right To Be Forgotten requests concerning former employees' email accounts.

Anecdotal evidence suggests that issues like this are especially acute at the moment with some organisations struggling to keep up-to-date with greater staff turnover. It needs to be an area of focus especially at this time with greater phishing and ransomware risks (see here https://bit.ly/cvransom). We are also seeing more departing employees seek to take advantage of any weaknesses in the company's processes and procedures – for example to take away customer details when they move on. For those organisations who outsource some functions they may also need to make sure that data processors working for them also have appropriate policies and procedures in place to close down accounts when their employees leave.

Organisations should ensure that in their practices, documentation and training they are getting the message across about this issue – a quick audit might also reveal if any immediate action needs to be taken.

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

includes template processes and procedures to deal with data rights requests and short films and other guidance. You can find out more about GDPR Navigator at www.bit.ly/gdprnav.

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 regulator's decision can be found here (in French): https://autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-64-2020.pdf

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

Image courtesy of H&M