Swedish Data Protection Regulator Imposes Fine for Failure to Report Data Breach

Date : June 22, 2020

Introduction

The Swedish Data Protection Authority ("the Datainspektionen") recently imposed a fine of 200,000 Swedish kronor (approximately €18,700 or $21,320) on the Swedish National Government Service Centre ("the NGSC") for failing to notify both the Datainspektionen and others about a personal data breach in sufficient time. This brief article highlights the issues in the case.

What's the case about?

The background is as follows:

- The NGSC coordinates the administration of government agencies by offering administrative support services to other government agencies. In its role handling personal data the NGSC appears to have been a data controller (for its employee data it seems) and a data processor (for the data of individuals connected with the government agencies it seems);
- A number of data breaches were notified by the NGSC to the Datainspektionen concerning an error in the IT system for payroll administration. This error allowed for unauthorised access to employee personal data of the agencies using the system and of NGSC personnel – it seems that there had been some illegal access;
- Personal data affected included name, gender, address, social security details, employment data and financial data. All told it seems that the data of some 281,800 individuals was involved;
- It appears that the police were informed of the breach, at least in connection with an individual gaining unauthorised access to personal data; and,
- The Datainspektionen undertook an investigation and determined that after the NGSC had become aware of the data breach it was almost three months before the Datainspektionen was notified of the breach and almost five months before others (agencies and individuals connected with them it seems) were notified about it.

What did the regulator decide?

The Datainspektionen decided that:

- The NGSC had not investigated what had happened adequately or with sufficient urgency nor had it handled the matter in a coordinated way;
- The NGSC failed to report the personal data breach to the Datainspektionen in due time;
- The NGSC took too long to inform others (mainly the agencies it seems) concerned about the error;
- Documenting the breach (the facts relating to it, the effects of the breach and remedial action taken), as required under Article 33(5) of GDPR, was found to be incomplete with regard to the personal data of NGSC personnel and although the NGSC was formally reprimanded for this it was not sanctioned with a monetary penalty; and,
- There were irregularities as regards data processing agreement issues (with an external service provider it seems) under GDPR processing agreement requirements under Article 28(3)&(4), but no sanctioning action was taken against this.

Accordingly the Datainspektionen:

- Imposed a fine of 150,000 Swedish kronor on the NGSC for breaching Article 33(2) of GDPR (the obligation of a data processor to notify a data controller without undue delay after becoming aware of a data breach);
- Imposed a fine of 50,000 Swedish kronor on the NGSC for breaching Article 33(1) of GDPR (the obligation

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

of a data controller to notify the relevant data protection regulator [in this case the Datainspektionen] without undue delay and where feasible not later than 72 hours after becoming aware of a personal data breach); and,
- Ordered the NGSC to introduce internal processes to document personal data breaches and to check that those processes are followed.

What are the takeaways?

First, this case demonstrates that regulators are prepared to sanction, with monetary penalties, failure to notify personal data breaches in time, both to the regulator and to others.

Second, data processors have breach reporting obligations too, i.e. not just data controllers – regulators can take action directly against data processors – in this case the bigger fine was for a processor failing to notify a controller.

Third, although it hardly needs emphasising, IT security is very important – this continues to be a key weak spot for organisations.

Fourth, document breaches – this can be done fairly simply.

Finally, whilst payroll is an area which businesses often outsource, they can't outsource the risk.

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 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 Swedish Data Protection Agency's press release about the case can be found here:
https://www.datainspektionen.se/nyheter/the-swedish-data-protection-authority-issues-fine-against-the-national-government-service-centre/

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

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.