International Law Office

EMPLOYMENT & IMMIGRATION - GERMANY

€35.3 million fine issued under GDPR for employee monitoring and IT security failings

11 November 2020 | Contributed by Mayer Brown

AUTHORS

Miriam Bruce

Francesca Ingham

Vanessa Klesy

Ana Hadnes Bruder

Introduction

During the COVID-19 pandemic, data privacy – and, in particular, employee data privacy – has been at the forefront of employers' minds. In the past six months, employers across the globe have had to give careful thought to a whole host of potential issues, from contact tracing apps to temperature and other health checks in the workplace, as well as processing an increased volume of staff health data. While not COVID-19 related, a recent decision from the Hamburg Commissioner for Data Protection and Freedom of Information is an important reminder of the significant financial and reputational penalties that employers may face if they do not appropriately collect, retain and protect employee personal data in line with the EU General Data Protection Regulation (GDPR).

In this case, the commissioner issued a €35.3 million fine against an international retailer due to its failures in monitoring and processing the personal data of several hundred employees at one of its sites in Nuremberg. The decision demonstrates the risks involved when organisations fail to comply with the GDPR's data minimisation principle by collecting and retaining excessive amounts and types of personal data in light of the purposes for which it has been collected.

Investigation and outcome

From 2014, parts of the retailer's workforce in Nuremburg were subject to extensive recording of details about their private lives which were stored on a network drive. This included information about employees' health obtained from return-to-work meetings (eg, their symptoms and diagnoses). In addition, supervisors recorded and digitally stored information that they acquired about employees' private lives, including details about family issues and religious beliefs. All of the information processed was then made available to up to 50 other managers in the company.

The processing of such data came to light after a local IT error resulted in the data being accessible countrywide for several hours in October 2019. On being alerted of this security breach, the Hamburg Commissioner for Data Protection and Freedom of Information opened an investigation, during which the retailer had to provide the commissioner with a copy of all the data that had been processed.

The commissioner concluded that the business had not taken appropriate steps to protect its staff's personal data. As well as being fined, the other notable outcomes from the investigation included:

- various pronouncements from the commissioner about the organisation, including that it had demonstrated a "serious disregard for employee data protection"; and
- the business taking additional steps to protect its reputation, rebuild trust with the workforce and prevent a reoccurrence, including:
  - confirming that it will give financial compensation to any individual who has been employed at the affected site for at least one month since May 2018 when the GDPR came into force. However, no further information has been issued as to the level of such compensation;
  - making personnel changes at management level at the relevant site;
  - providing additional training for managers on data protection; and
  - implementing enhanced data cleansing processes and improved IT solutions to ensure the GDPR-compliant storage of personal data.

Comment

The commissioner's decision is a stark reminder of the penalties that can be implemented against companies for breach of their obligations under the GDPR. As well as financial implications, there are obvious reputational and employee relations issues which the company must now handle.

While this decision was made in Germany, other European data protection supervisory authorities (including the United Kingdom's Information Commissioner's Office) are likely to take a similar view based on the facts of the case regarding the collection, retention and protection of employee data.

In light of COVID-19 and the additional employee personal data that companies may have to process as a result, it is more important than ever to ensure that companies take appropriate steps to:

- collect and retain only personal data which is necessary for the purposes for which it is used; and
- protect individuals' personal data, especially health-related data.

Companies should ensure that they have appropriate measures in place for processing personal data in line with the GDPR and the latest guidance issued by the relevant regulator in their jurisdiction.

For further information on this topic please contact Miriam Bruce or Francesca Ingham at Mayer Brown's London office by telephone (+44 20 3130 3000) or email (mbruce@mayerbrown.com or fingham@mayerbrown.com). Alternatively, please contact Vanessa Klesy or Ana Hadnes Bruder at Mayer Brown's Frankfurt office by telephone (+49 69 7941 0) or email (vklesy@mayerbrown.com or abruder@mayerbrown.com). The Mayer Brown website can be accessed at www.mayerbrown.com.

Oliver Yaros, partner, assisted in the preparation of this article.
