Client Alert: Hamburg Data Protection Authority fines H&M €35.2m for GDPR violations

Date : October 1, 2020

Introduction

The Hamburg Data Protection Authority (HmbBfDI) has today fined H&M Germany €35.2m for GDPR violations. The case concerned excessive use of employee data and is the largest fine so far imposed by regulators for the handling of employee data. We are likely to see more pressure on employers to justify the handling of employee data as a result of today's fine.

Background

Hennes & Mauritz AB (commonly known as H&M) is a Swedish multinational clothing-retail company known for its fast-fashion clothing for men, women, teenagers and children. In November 2019 it employed 126,000 people and operated 5,000 stores in 74 countries.

Part of its operations included the H&M Service Center in Nuremberg. These operations were investigated by HmbBfDI in a long-running investigation which concluded today with a fine of €35,258,707.95 for one of H&M's German subsidiaries, H&M Hennes & Mauritz Online Shop A.B. & Co KG.

HmbBfDI found that since at least 2014, parts of the workforce have been subject to extensive recording of details about their private lives. The records were held in network drives. After absences including holidays and sick leave team leaders would hold so-called "Welcome Back Talks" with their employees and they would record details of those conversations including holiday experiences, symptoms of illness and diagnoses. In addition, some supervisors acquired a broad knowledge of their employees' private lives from one-to-one conversations. These conversations were also on occasion recorded on the system and ranged from trivial details about the employee to family issues and religious beliefs. Some of this data was accessible by up to 50 other managers throughout the company.

The data was used to make decisions about employees. The regulator found that "*The combination of collecting details about their private lives and the recording of their activities led to a particularly intensive encroachment on employees' civil rights.*"

The extent of the data collected became known after an IT glitch in 2019 due to a configuration error. HmbBfDI picked up on press reports about the incident and launched its investigation.

What did the regulator do?

On finding out about the incident HmbBfDI ordered that the database be 'frozen' and then ordered that it be given to them for analysis. It is worth remembering that in addition to having the power to levy fines, data protection authorities (DPAs) have the power to do other things under GDPR Art. 58 including the power to order a data controller or data processor to provide any information it requires, to obtain from a controller or processor access to all personal data "and to all information necessary for the performance of its tasks" and the power to access premises and equipment.

H&M turned over 60 gigabytes of data for evaluation. HmbBfDI also looked at additional evidence from witnesses and the company's internal process and procedures.

What did the regulator say?

Prof. Dr. Johannes Caspar, Hamburg's Commissioner for Data Protection and Freedom of Information, said in announcing the fine:

"This case documents a serious disregard for employee data protection at the H&M site in Nuremberg. The amount of the fine imposed is therefore adequate and effective to deter companies from violating the privacy of their employees. Management's efforts to compensate those affected on site and to restore confidence in the company as an employer have to be seen expressly positively. The transparent information provided by those responsible and the guarantee of financial compensation certainly show the intention to give the employees the respect and appreciation they deserve as dependent workers in their daily work for their company."

What did H&M do after the investigation?

The HmbBfDI has taken into account corrective action taken by H&M. This has included new policies and procedures, an apology to those affected and compensation for employees. In addition H&M invested in monthly data protection updates, increased whistleblower protection measures and a new process to deal with data subject requests. HmbBfDI has called this "*an unprecedented acknowledgement of corporate responsibility following a data protection incident*".

H&M has confirmed today that everyone employed at this entity since GDPR came into force in May 2018 will receive financial compensation.

What about the current pandemic?

The investigation here was into data collected before the current pandemic. In our view however it is unlikely that the DPA would have been more sympathetic to the collection of additional data without credible justification even now. We've written about the issues with the collection of data during the pandemic (see www.bit.ly/gdprvirus) and the issues with a return to office working https://bit.ly/cvrtw. More than 40 DPAs have issued specific guidance on the collection of extra data during the pandemic (including health data, data on holiday travel and domestic arrangements) and there's a need for extra caution when processing data like that. We're also seeing a significant rise in data protection requests and complaints, especially from employees who have been furloughed or let go and so the 2020 situation is likely to be even more challenging than the situation H&M faced in 2019.

In addition we have seen some employers using so-called 'productivity tools' to collect data on employees whilst they work from home. We know that these tools are under investigation in at least one case (involving Barclays Bank) and there is a special need for care when processing this type of data.

Practical tips

We have found in our work that some HR professionals and managers do store more data than is necessary. Every organisation needs proper guidance on the employee data that can be stored and proper training on that guidance. This needs proper planning. That plan might include:

1. Education on the 6 principles of good practice in GDPR (outlined at www.bit.ly/gdprfaq). This will include an understanding of the need to be transparent with employees about how their data is held, making sure that the data held is limited to what is necessary and properly securing that data not only from the outside world but from other employees who don't have a need to know. It will be hard for example to justify access to medical records by 50 other employees even if they are managers in the business.
2. Making sure you have a lawful purpose for the processing of all data. As we've said before in the employment context consent is unlikely to be sufficient.
3. Making sure your HR systems are properly configured. From our experience global HR systems can cause GDPR issues with the wide number of fields and open access by default. Those installing or running a global HR system need to give careful thought to the data which needs to be processed (which may vary between locations or job roles), how long it needs to be retained for and who will have access to it. A Data Protection Impact Assessment will almost always be necessary.
4. Think about how you transfer data. We've written recently on the collapse of Privacy Shield in the EU and Switzerland (https://bit.ly/swisspshield). The use of Standard Contractual Clauses has also been limited by the European Court. Dr. Caspar has been heavily involved in data transfer cases and we're likely to see data transfer investigations in Hamburg and across Europe.

5. The number of subject access requests you receive under GDPR is likely to rise, especially in Germany. We have found that Dr. Caspar can get substantial media coverage for his activities and that is likely to translate into employees and former employees asking to see the data you hold on them. Make sure that all of your employees know how to recognize a subject access request, that they know how to handle them within the short time available to respond, and make sure that you have the proper resources in place to locate and redact the data.
6. Employees (and customers) are now much more likely to ask general questions about the way in which you handle data. In addition to data subject requests under GDPR you'll need to be ready for more general questions. Some prepared FAQs may help HR teams and contact centres respond. Works councils are also likely to ask questions too. Take into account the fact that class actions after data incidents are on the rise across Europe (see for example here https://www.corderycompliance.com/doors-open-for-class-action-appeal-as-court-allows-google-claim-to-proceed/) and whilst H&M have confirmed it will compensate those affected that might not be enough to fend off litigation.
7. Keep training refreshed. Some organisations have not trained their employees since GDPR came in. Regulators have said in the past that training must be refreshed to be valid and the cases suggest a minimum of once a year or once every 2 years depending on the job role, access to data etc. Your plan should include regular refreshers too and not just annual events.
8. Make sure you have a plan to deal with security breaches. H&M confirmed today that it reported the software glitch as a data breach to the Hamburg DPA although we do not yet know the details and timing. Organisations will need to be able to detect and assess breaches quickly to comply with their GDPR obligations. There's a short film on the processes we recommend here https://www.corderycompliance.com/dealing-with-a-data-breach/.

You can read today's announcement from the Hamburg DPA here https://bit.ly/3cKtnBi

For other articles that we have written about data protection issues please see here: https://www.corderycompliance.com/category/data-protection-privacy/

For details about Cordery's GDPR Navigator subscription service, which includes short films, straightforward guidance, checklists and regular conference calls to help you comply, please see here: www.bit.ly/gdprnav.

For more information please contact Jonathan Armstrong or André Bywater 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