DATA MATTERS

HITACHI
Inspire the Next

Data Protection Case Law in the EU Confirms that Data Breaches Constitute a Major Legal Liability but Are Not the Only Privacy Risks Organizations Need to Address

EXECUTIVE LEGAL BRIEFING SERIES

New Trends in European Privacy Law 2

Customer Data Breaches, Violating Employees' Rights: Understanding Privacy Incidents for Advanced Governance

By Victor Alexander de Pous
March 2021

Contents

Headlines

- Privacy-related incidents come to light every day. Almost three years after the application of the General Data Protection Regulation (GDPR) on 25 May 2018, the enforcement of the major European privacy law reaches a certain size and pace. Increasingly, the data protection authorities (DPA's) of EU the Member States impose *administrative fines* (monetary penalties). These cases also show a variety of topics, just like incidents that occurred but not have been addressed (yet) by a supervising body.

- Especially personal data breaches are on the rise *in connection to criminal attacks* on organizations with a large consumer base. The data protection authority in the Netherlands, Autoriteit Persoonsgegevens, concludes an increase of 30% of reported criminal data breaches in 2020, after a 25% rise the year before. Hacking, using malware such as ransomware, and advanced phishing technics are the preferred modus operandi of the current threat actors; in conjunction with a more refined approach to explore and map networks over a longer period of time before striking.

Analysis

- Incidents with personal data are not only stunning from numbers, scale and frequency, but also differ in nature. Looking at interventions of national data protection authorities in the EU, we see cases relating to the deployment of an unlawful database with human-resource information, including health data (fine: Euro 35 million), sending-out millions of marketing emails and SMS messages to addressees without prior consent (fine: 50.000 GBP), not managing corporate email addresses of ex-employees (fine: Euro 15.000), and for example, using an unsecure website for selling airline tickets (fine: 20 million GBP).

- Nevertheless the individual and sometimes unique differences, the dominating cause of the series of privacy law-related violations are personal *data breaches*. In the wording of the GDPR: ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.’ And then with criminal intent as the surging category.

- In addition to gaining ground considerably through digital crime, the data breach crime itself changes. Threat actors take their time. They often have been present in a network for some time before they strike and attacks sometimes continue for months, even years.

- One advice reads that since information and network systems are often protected with just one password, organizations should deploy multifactor authentication (MFA) everywhere by default, although this 'simple' security measure is currently only mandatory when processing sensitive personal data. Another general security measure relates to use data encryption and keeping the keys safe and strictly confidential, just as the need for immediate security patching after receiving the software update.

- Understanding the provisions and definitions of the GDPR in general truly comes at hand for executives because, among other matters, the two main categories of personal data — personal data as such and ‘sensitive’ or ‘special’ personal data — have a different regulatory regime.

Data Privacy as a Matter of Serious Risk and Liability

The institution of independent supervising authorities appointed by national governments in Europe has become a trend. These public administrative bodies monitor compliance with laws and regulations by organizations, due to the increased complexity of supervision that requires special expertise. Not surprisingly, this oversight and control process does apply in full to the digital domain, with a centre of gravity in one of the oldest supervisory areas: the *processing of personal data*. Under the GDPR both 'processing' and 'personal data' are defined broadly: practically everything one can do with any information relating to an identified or identifiable natural person (the data subject).

For many companies and public sector entities personal data consists of two main types: (i) personnel or human resource data and (ii) customer data. A third type of personal data that mainly exists in corporations concerns personal data used for (direct) marketing purposes — often a data mix of existing customers and prospects. This privacy framework will be addressed in a legal briefing on ePrivacy and the upcoming EU ePrivacy Directive. Furthermore, the GDPR divides in personal data as such and 'sensitive' or 'special' personal data with different legal frameworks. For example, special categories of personal data (on health care, religion, and more) require a higher level of security and may not be processed, unless strict conditions are met.

Regulatory non-compliance may have consequences. Based on various reasons, not complying with data privacy provisions in Europe turns out to be risky business. The GDPR comprises all the ingredients for this qualification, indeed. In a nutshell: the law reflects a complex set of rules, with the actual threat of very high administrative fines to be imposed by data protection authorities, plus leaving an additional door open for individual and class action compensation claims brought before a court of law. Hereunder we highlight two personnel data privacy cases and two relating to primarily customer data.

Deploying an Illegal Database with Personnel Data

The German data protection authority of the state of Hamburg, Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI), imposed on 1 October 2020 a fine of more than 35 million euros to H&M Hennes & Mauritz online shop A.B. & KG. The ground: violating the privacy of its staff. Since at least 2014, parts of the workforce have been subject to extensive recording of details about their private lives, which information was permanently stored on a network drive. The data protection authority stated: '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 Swedish clothing company held all kinds of detailed and talks with personnel of the service center in Nuremberg. The information was recorded and stored on a network drive, to which 50 managers worldwide had access. After absences such as vacations and sick leave — even short absences — the supervising team leaders conducted 'Welcome Back Talks' with their employees. After these talks, in many cases not only the employees' concrete vacation experiences were recorded, but also symptoms of illness and diagnoses. In addition, some supervisors acquired a broad knowledge of their employees' private lives through personal and floor talks, ranging from rather harmless details to family issues and religious beliefs.

Next to a meticulous evaluation of individual work performance, the data collected in this way was used, among other things, to obtain a detailed profile of employees for measures and decisions regarding their employment. The existence of the unlawful database with personnel data became known by chance, through a configuration error at the end of 2019, with the result that for a few hours all data were available to all employees.

A String of Measures

For the record, healthcare data are a special category of personal data, of which processing by employers is prohibited. In addition to (i) paying the monetary penalty, the company made (ii) apologies and paid also compensation to the staff, and (iii) introduced a new data protection concept, which included:

- a newly appointed data protection coordinator;
- monthly data protection status updates;
- increasingly communicated whistleblower protection; and
- a consistent concept for dealing with the access rights of stakeholders.

Unlawfully Forwarding Email Correspondence from a Former Employee

On 12 February 2021, a Norwegian company was fined by the national authority, called Datatilsynet, with Euro 20,000 for unlawfully *forwarding* e-mail correspondence from a former employee. In addition to the fine, the company must document in writing the procedures for accessing the email accounts of employees and former staff. The employee discovered that email for his personal email address within the company was automatically forwarded. This forwarding took place for several months, however without the former employee having been informed. The employee then filed a complaint with the national DPA, which conducted an investigation and concluded that automatic forwarding of e-mail is in violation of regulations for employers and access to inboxes and other electronic material.

Although Norway is not an EU member state but a member of the European Economic Area (EEA) the country followed different procedure before the GDPR became part of Norwegian law. It enacted The Act on the Processing of Personal Data of 15 June 2018, which, together with the GDPR, took effect on 20 July 2018. According to the Norwegian DPA the unnamed company violated the applicable privacy legislation on the following grounds:

- Lack of a legal basis for the forwarding;
- the employee has not been informed nor given the opportunity to appeal;
- regulations for the removal of personal data have not been complied with.

Need for Extensive Email Management

This case mimics a data privacy incident in Belgium, where on 29 September 2020 the national DPA fined a small family business with Euro 20.000 for the *continuation* of the email addresses of a former CEO. This fine is based on the violation of the GDPR privacy principles of purpose limitation and data minimization (limitation of the conservation). Thus, both continuation and forwarding emails of former staff and management may lead to legal liability when not managed properly.

Operating an Unsecure Website for Airline Ticketing

Airline British Airways has been fined 20 million GBP for a large data breach in which users' payment details were stolen. The British data protection authority Information Commissioner's Office (ICO) announced this on 16 October 2020. In 2018, attackers had modified an external script that ran on the British Airways website. The malicious code added to the script allowed personal and payment information entered by customers to be sent to the attackers. More than 420,000 people were affected by the attack. The attacker is believed to have potentially accessed the personal data of over 400,000 customers and staff, including names, addresses, payment card numbers and CVV numbers of 244,000 BA customers.

According to the ICO, the attack was said to have started in June 2018, but the airline did not detect it for more than two months. ICO investigators found that BA did not detect the attack on 22 June 2018 themselves, but were alerted by a third party more than two months afterwards on 5 September. Once they became aware BA acted promptly and notified the ICO. It is not clear whether or when BA would have identified the attack themselves. This was considered to be a severe failing because of the number of people affected and because any potential financial harm could have been more significant.

An Active Tour of Security Duty

The investigation shows that bad security arrangements at the company could have caused data to be stolen. According to the DPA, the airline should have found and remedied the security vulnerabilities with security solutions available at the time. Had the airline done this, the 2018 attack could not have happened that way. These include:

- limiting access to applications, data and tools to only that which are required to fulfil a user's role;
- undertaking rigorous testing, in the form of simulating a cyber-attack, on the business' systems;
- protecting employee and third party accounts with multi-factor authentication.

Because the BA breach happened in June 2018, before the UK left the EU, the ICO investigated on behalf of all EU authorities as lead supervisory authority under the GDPR. The penalty and action have been approved by the other EU DPAs through the GDPR's cooperation process.

A Long-Term Hidden Data Breach of 340 Million Customers

On 30 October 2020, ICO fined Marriott International with 18.4 million GBP. Investigations of the data protection authority in the United Kingdom revealed that errors were made in taking appropriate technical and organizational measures to protect personal data from infringement, as the GDPR requires. The hotel chain estimated that no less than 339 million guest records were leaked after a 2014 cyber-attack on Starwood Hotels and Resorts Worldwide, which competitor Marriott International acquired in 2016. However, the data breach remained unnoticed until September 2018. Threat actors therefore had unauthorized access to the information systems for a period of four years. Important to notice: the fine only relates to the infringement from 25 May 2018; the date that the AVG was declared applicable. Because violation of the privacy law took place before the United Kingdom left the European Union, the ICO investigated this incident on behalf of all EU authorities as the leading supervisory authority under the GPR.

Mergers & Acquisitions

The need for a thorough *digital* due diligence process at a merger and acquisition, joint venture or other financial transaction of weight, such as participation, is without doubt. After all, today the investigative process is no longer limited to the traditional bookkeeping and reporting statements, since IT and electronic data processing are being conditional for every company. Part of this is a study concerning the processing of *personal data* and meeting the statutory regulations, starting with the GPR. Network and information security measures may come to mind first, but do not forget for example the audit of the appropriate permission to deploy personal data for direct marking, as follows from the Muscle Foods case. On 3 March 2021, the ICO imposed a monetary penalty of 50,000 GBP for sending 135 million marketing emails and 6 million text messages to recipients, without their prior consent over a period of seven month.

More Takeaways from Enforcement and Compensation Actions

Applying a helicopter view to the broad legal domain of personal data processing under the regulatory framework of the GDPR and related regulations, we made additional analyses.

- Starting from the dichotomy personnel data and customer data, we note a broad variety of data privacy infringement cases in both fields. It is of importance to understand the difference between a violation of the GDPR at large (noncompliance) and a data breach, which exclusively constitute an *infringement of the regulatory protection measures.*

- Although both unintentionally carelessness and criminal intentions occur in the practice of data breaches, the criminal variant increases sharply. In addition, the attacks are often particularly focused on organizations that process personal data on a large scale, while the nature of the attack demonstrates advancement and sophistication.

- Enhancing appropriate organizational and technical security measures are unavoidable, with the comment that internal access rules to corporate data are often overlooked. As a result, employees have more and broader access applications, data and tools than they need for their work. That mere fact constitutes a data breach under the GDPR and may lead subsequently to criminal intent actions, inside or outside the organization.

- In the perspective of the stunning amount of data privacy-related cases, data protection authorities in general have to little staff and financial means, and seem to be overworked, but they do investigate incidents and enforce the law. In the wording of Information Commissioner Elizabeth Denham: ‘The law now gives us the tools to encourage businesses to make better decisions about data, including investing in up-to-date security.’

- Every DPA has the competence to impose high fines (up to 20 million euros or 4% of the worldwide turnover of a company), but it is notable that the ICO in the British Airways and Marriott International data breach cases initially issued a notice of its intention to fine a plurality of the finally imposed amount (184 and 99 million GBP). Considering the economic impact of COVID-19 apparently lead to substantial lower fines.

- Furthermore, we note that even small and unlikely violations of the GDPR may lead to DPA interventions, including imposing fines. In Spain, on 20 May 2019 an association of home-owners was fined Euro 15.000 for posting the minutes of an assembly in paper in an elevator.

- Also of importance: imposing an administrative fine by a data protection authority does not need to be end of a data breach since *data subjects hold an independent statutory right to litigate* in order to claim compensation. Moreover, we see the advent of privacy class actions suits in Europe, making non GPDR compliance an even larger boardroom risk than based on regulatory complexity.

Conclusion

In the time period leading to the applicability of the GDPR in Europe on 18 May 2018, organizations had to prepare for implementing the new privacy rules and policies for the greater part of their business processes; both internal and external. That was phase one. Now the time for a thorough update has arrived. Based on the pointers derived from the many privacy-related incidents — whether or not enforced by a data protection authority and through litigation — every entity must enhance and fine-tune its corporate data policies and subsequently its work and business processes. Phase two should also take into account the regular published guidelines of the European Data Protection Board (EDPB). In the end, processing personal data seems to become more of a risk and liability that only can be mitigated by advanced and integrated management programs.

About Hitachi Vantara

Hitachi Vantara, a wholly owned subsidiary of Hitachi, Ltd., guides its customers from what's now to what's next by solving their digital challenges. Working alongside each customer, we apply our unmatched industrial and digital capabilities to their data and applications to benefit both business and society. More than 80% of the Fortune 100 trust Hitachi Vantara to help them develop new revenue streams, unlock competitive advantages, lower costs, enhance customer experiences, and deliver social and environmental value.
www.hitachivantara.com.

About Data Matters

Data Matters designs and delivers sustainable archiving solutions and services with an integrated management for paper-based archives and digital preservation, including a digital repository with all the functions defined in the OAIS model. These solutions and services are based on years of expertise, in-depth multi-disciplinary knowledge, and industry-leading products and services from select innovative and reliable technology manufacturers. Data Matters has long-standing partnerships with Hitachi Vantara, Star Storage, and others.
www.datamatters.nl

About the author

Victor Alexander de Pous is a senior corporate lawyer, analyst and strategist who has been working in the domain of the legal aspects of digital technology, electronic data processing and the information society since 1983. Selective Bibliography: http://thelegallook.nl/

Version: March 2021