GDPR: Nine Months Later – The Impact in the EU on Enforcement and Compliance and in the US on Discovery

Paul Lefebvre
Hanotiau & Van Den Berg
Brussels, Belgium
paul.lefebvre@hvdb.com

Jonathan Monheit
Microsoft Corporation
Redmond, Washington
jmonheit@microsoft.com

Melissa Ventrone
Clark Hill PLC
Chicago, Illinois
mventrone@ClarkHill.com

GDPR: Nine Months Later – The Impact in the EU on Enforcement and Compliance and in the US on Discovery

The European Global Data Protection Regulation (GDPR) established a new framework for the collection, storage and use of personal data obtained from European Union (EU) residents. GDPR applies to all businesses domiciled in an EU Member State and non-EU domiciled companies that meet the criteria of Article 3. GDPR (EU) 2016/679. As the first comprehensive breach response regime for the EU, GDPR requires controllers to notify the supervisory authority within 72 hours of becoming aware of a breach of personal data that is likely to result in a risk to the "rights and freedoms of natural persons." Companies that fail to comply with the GDPR can be subject to penalties up to 4% of worldwide turnover. Regulatory bodies began enforcing the GDPR on May 25, 2018. Several months have passed since that date, and despite many people's fears, there have been few fines. however, understanding this activity can provide companies with useful information on compliance activities.

Information Commissioner's Office in the United Kingdom issues first enforcement action:

In September 2018, the Information Commissioner's Office (ICO) in the United Kingdom (UK) issued the first formal enforcement action under the GDPR and the UK's Data Protection Act 2018 (DPA) on Canadian data analytics firm AggregateIQ Data Services Ltd (AIQS). The enforcement action requires AIQS to "cease processing of any personal data of UK or EU citizens obtained from UK political organizations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes."

Clients of AIQS include several UK political organizations that provide AIQS with personal data which is used by the company to retarget patrons through online advertising and social media platforms. AIQS is not established in the EU, however the ICO determined that AIQS fell under the GDPR's territorial scope provisions of Article 3(2)(b) because AIQS' activities relate to the monitoring of data subjects' behavior when that behavior takes place within the EU.

AIQS was found to be in breach of Articles 5(a) – 5(c) and Article 6 of the GDPR for processing personal data in a way that data subjects were not aware of, for a purpose they would not have expected and without a lawful basis for processing. In addition, AIQS failed to provide the transparency information required under Article 14 of the GDPR.

This is an important example that non-EU domiciled companies would be well advised to consider, as it should be taken as a signal that the regulators intend to scrutinize non-EU companies with the same kind of focus as EU companies. AIQS has appealed the finding.

Portuguese Supervisory Authority Issues Fine:

Next was the Portuguese Supervisory Authority, which imposed two fines totaling 400,000 euros ($453,910) on a hospital for violating the GDPR. The first fine of 300,000 euros was assessed for failing to limit access to patient data and failure to respect patient confidentiality. The investigation determined that hospital workforce members had access to patient information

through false profiles. The hospital had 985 registered doctor profiles, but only 296 active doctors. Doctors also had access to all patient files, regardless of their specialty.

The second fine, 100,000 euros, was assessed for the hospital's failure to have appropriate technical and organizational measures to protect patient data. In its defense, the hospital noted that it used the IT system provided to public hospitals by the Portuguese Health Ministry. However, the supervisory authority found that the hospital did not consult with the Ministry of Health concerning any suspected security deficiencies. It also failed to implement adequate controls for creating user accounts. and did not remove former doctors' accounts.

With this fine, we see that it is not sufficient to simply rely on third parties for IT security, companies must have adequate vendor management programs in place, and maintain sufficient oversight of the vendor's performance.

Austrian Regulator Issues Fine:

At the beginning of October, the Austrian regulator issued its first fine for illegal video surveillance. An entrepreneur had installed a CCTV camera that monitored a large part of a public sidewalk. The CCTV was not sufficiently marked, which meant that the transparency requirements were not met. Additionally, monitoring large portions of public sidewalks is in violation of the GDPR. The fine, however, was a modest 4,800 euros ($5,447). News outlets in Austria found the fine especially interesting, as the Austrian Data Protection Act states that the regulator will at first only exercise remedial powers, which is generally limited to reprimands for first-time offenders. (Need cite, obtained this off of blog posts and IAPP).

Germans Issue Fine:

Most recently, the State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg (LfDI) imposed the first fine under the GDPR in Germany. In September, a social media company was hacked and email addresses and passwords of approximately 808,000 individuals were compromised. The company provided timely notification to the supervisory authority and notified individuals directly of the compromise. The investigation found that the social media company stored the passwords of its social media users in unencrypted plain text. The supervisory authority found that the company failed to meet its obligation to implement appropriate security measures to ensure a level of security appropriate to the risk. In its official press release, the supervisory authority stated: "By storing the passwords in plain text, the company knowingly violated its obligation to ensure data security pursuant to Art. 32 para. 1 lit a DS-GVO when processing personal data." (need cite). The German Supervisory Authority assessed a fine of 20,000 euros ($22,703).

When assessing its fine, the supervisory authority did take into consideration that the social media company reported the incident immediately after discovering the compromise, notified individuals directly, and cooperated with the investigation. The company also significantly improved its level of IT security after the attack.

This investigation and fine show us that companies will be expected to encrypt or otherwise protect passwords; and failure to do so will most likely result in a fine. On the other hand,

immediately notifying the supervisory authority and subsequently informing affected individuals, cooperating with any investigation and enhancing security measures after an attack will reduce potential fines.

Further Guidance on Applicability of GDPR to Non-EU Domiciled Companies:

Non-EU domiciled companies are struggling with determining whether their activities fall under the GDPR. Article 3(2) outlines the territorial scope of the GDPR, which applies to companies outside the EU that offer goods or services to EU residents or monitor the behavior of EU residents when the behavior takes place within the EU. In November, the European Data Protection Board (EDPB) released draft guidelines on the territorial scope under Article 3. Comments are requested through January 18, 2019.

The EDPB clarified that Article 3(2) applies to someone who is in the EU at the moment the "trigger activity" occurs, such as when the goods or services are offered, or behavior is monitored. However, simply processing personal data of someone located in the EU without the "targeting activity" does not bring the organization's activities under the jurisdiction of the GDPR.

The EDPB further outlines what might be considered as "offering goods and services" to EU residents noting this type of analysis is fact based. With respect to monitoring the behavior of an EU resident, the EDPB states that this concept is broader than simply tracking someone on the internet. Tracking someone through other types of technology, like wearable devices and other smart technology, could also be considered sufficient to bring a company under the scope of the GDPR. The EDPB was careful to note that not all online tracking arises to the level of "monitoring" contemplated by the GDPR. There should be some purpose behind the collection and a subsequent use of this information, such as creating a profile.

Non-EU domiciled companies should carefully review their activities to determine whether they fall under the scope of the GDPR and take steps towards compliance. As noted above, supervisory authorities are not shy about investigating non-EU residents to ensure the data subjects' information is being treated appropriately.

Interesting Cases:

It is also worth reviewing some of the recent court rulings coming out of the European Courts, although the most recent rulings are analyzed under the Data Protection Act of 1998. Cases applying GDPR have not yet worked their way through the court system. In *WM Morrison Supermarkets PLC*, the court found Morrisons' liable for the actions of its employee. In the normal course of business, an employee had obtained payroll information of 99,998 Morrison employees. That employee then took this information and posted it on a file sharing website under the name of another employee in an attempt to frame their colleague. That same employee, then sent a CD containing the payroll information and a link to the file sharing site to three newspapers in the UK. The employee was later arrested and sentenced to eight years in prison.

The High Court found that Morrisons' had met the data protection standards in place at the time of the breach under the Data Protection Act of 1998 but found Morrison's vicariously liable for

the actions of its employee. Morrison's appealed to the UK Court of Appeal, which upheld the High Court's ruling.

Interestingly, the UK Court of Appeal addressed Morrisons' argument about the catastrophic effect of finding it vicariously liable for the criminal acts of its employee by referencing insurance:

> "There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees. We have not been told what the insurance position is in the present case, and of course it cannot affect the result. The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments put forward by [counsel] on behalf of Morrisons."

Morrisons intends to appeal to the Supreme Court, but companies would be wise to incorporate internal threat monitoring capabilities into their overall data protection frameworks.

Other Complaints and Activities:

Preliminary data shows that people and organizations have not been shy about filing complaints against companies for their data practices. There were 6,281 complaints filed with the ICO between May 25, 2018 through July 3, 2018 which more than doubles the previous year's total of 2,417. France's CNIL agency reported in October 2018 that 3,767 complaints had been filed since May 25, 2018, a 64% increase from the same period the previous year, when a record (at that time) 2,294 complaints were filed. 600 data breach notifications had also been reported.

The Irish Times reported that through July 2018, the Irish Data Protection Commission was reported to have received 1,184 data breach reports — up significantly from the previous year. The Irish Data Protection Commission also received 743 complaints since May 25, 2018 as well.

Additionally, the ICO's website reports that there was a total of 4,056 data security incidents reported during Q2 of 2018.

Recently, consumer groups in seven European countries filed complaints with their respective data protection regulator against Google, complaining that Google's application of the location feature violates the GDPR.

Pay Your Processing Fee or Pay Up

Penalties assessed for GDPR non-compliance are not the only way companies can run afoul of data protection regulators. In November, the ICO released news that it was issuing penalty notices for over 100 companies that have yet to pay the new data protection fees. Controllers are required to pay an annual fee to the ICO unless they are exempt. Under a new three-tier structure unveiled earlier this year, controllers pay a sliding scale depending on size, annual turnover,

public or private entity, whether they are a charity, or provide a small occupational pension scheme, with large companies paying just under £2,900 ($3,659) to £40 ($50) for the smallest companies. Companies that receive the penalty notice are required to pay within 28 days or face further legal action. Fines range from £400 ($504) to £4,000 ($5,047) depending on the size and turnover of the organization.

Ethical Legal Obligation

Attorneys must also be aware of their legal obligations to protect their clients' data, and the attorneys' obligations if they discover client data is breached. The American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 483 outlines an attorney's responsibilities after a data breach. First, Model Rule 1.6 has been interpreted to require lawyers use technology "competently" to safeguard confidential information against unauthorized access or loss. This also requires the lawyer to use reasonable efforts to monitor "technology and office resources connected to the internet, external data sources, and external vendors providing services related to data and the use of data."

If a lawyer discovers a breach, they are required to stop the breach, take steps to mitigate damages, and as necessary restore the system. Development and implementation of an incident response plan is also recommended. Lawyers are required to take reasonable steps to determine what occurred, and evaluate any compromised data.

Notably, a lawyer's ability to preserve a client's confidentiality is "not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable." Instead, reasonable efforts should be made to maintain confidentiality. The difficulty arises in determining what, specifically, constitutes "reasonable efforts". However, reasonable efforts at a minimum include a process to assess risks, identify and implement measures responsive to the risks, verify implementation, and update measures in response to new developments. See *ABA Cybersecurity Handbook*.

On discovering a breach, a lawyer must evaluate whether the breach has a reasonable possibility of negatively impacting a current client's interests. This might involve misappropriation, destruction, or compromise of client confidential information that significantly impairs the lawyer's ability to perform legal services for the client. Thus, where a data breach involves or likely involves material client confidential information, the lawyer has an obligation to inform the client of the incident.

For former clients, the Committee declined to require lawyers to notify a former client of a breach as a matter of legal ethics absent a "black letter provision requiring such notice." However, lawyers should evaluate whether the breach of a former client's data would otherwise trigger notice requirements under law or by contract.