Skadden

Privacy & Cybersecurity Update

EU Launches GDPR Guidance Website

The EU has launched a website with compliance and other information regarding the GDPR.

The European Commission has released a website with information and guidance on complying with the new General Data Protection Regulation (GDPR). The website includes information for data processors, data subjects, member states and data protection authorities, and is intended to educate the EU about the GDPR.

The website, which includes FAQ, infographics and other easily digestible content, should prove to be a valuable resource for businesses concerned with GDPR compliance.

The website is available here.

Return to Table of Contents

Polish Data Protection Authorities Considering Broad Exemption From New EU Data Law

On January 23, 2018, Polish data protection authorities announced they were considering broad exemptions to the key parts of the European Union's GDPR for small- to medium-sized businesses. The potential exemptions have caused alarm among some privacy advocates and threaten to undermine one of the GDPR's core principles: to establish privacy uniformity across EU member states.

Implementing the GDPR

Unlike the EU's predecessor privacy law, Directive 95/46/EC, which required member states to pass enabling laws to implement its requirements, the GDPR is a regulation that is directly applicable to all EU member states. As a result, members do not need to pass laws to enact the GDPR. Instead, they must simply enact laws that annul their current data protection laws in order to comply with the regulation.

Article 23 of the GDPR, however, allows member states to implement restrictions on certain GDPR rights and obligations that are "necessary and proportionate" to safeguard certain key interests, such as the member state's "important economic or financial interest." Under the article, though, the restrictions also must include a number of elements intended to protect and give notice to data subjects, such as safeguards against abuse.

The Polish Proposed Restrictions

The Polish proposal would exempt small- to medium-sized businesses (those with less than 250 employees) from certain requirements, such as the obligation to inform data subjects how long their data will be stored and what their rights are with respect to the stored data. The government previously had suggested it also would exempt these businesses from requirements such as allowing data subjects to request copies of their data being processed, informing data subjects about rectification, erasing or restricting of processing, or disclosing risky personal data breaches to the data subjects, but it is not yet clear whether it will follow through on these suggestions.

According to previous arguments by the government, the exemptions are aimed at companies that only use personal data to conclude contracts or in the course of accounting, though the announcement does not make that clear.

The government justified the exemptions on the basis of protecting its financial interest, saying it would be difficult for these companies to provide all the information required by these obligations — particularly over the phone.

Reaction From Privacy Advocates

Privacy advocates have expressed grave concerns over the Polish announcement. They note that the exemption as announced does not include the types of protections required under Article 23. It does not, for example, include measures to safeguard against abuse. In addition, they have noted that the exemptions undermine the GDPR's core values of consistency and transparency: consistency of laws across the EU and transparency with respect to the use of personal data. Finally, they have argued that the scope of companies covered by the exemption is too large. According to these commentators, a significant portion of Polish companies have less than 250 employees, which would mean a large portion of data processors would be exempt.

If Poland pursues the exemptions, it may face challenges from the EU Commission for failing to follow the law's requirements, but given that Article 23 allows countries a degree of flexibility, any such challenge likely would focus on complying with the article's other requirements (*e.g.*, notice and safeguards).

Key Takeaways

The proposed Polish exemptions to the GDPR highlight one of the key difficulties in enacting EU-wide rules on privacy issues: Member states may take advantage of the flexibility in the GDPR to deviate from its requirements, thus undermining the goal of consistent laws across the region. When the GDPR takes full effect on May 25, 2018, other countries may be tempted to introduce their own changes to the law.

Return to Table of Contents

OCC Identifies Cybersecurity as Key Risk Area for US Banks

The OCC has issued recommendations for U.S. banks facing increasingly sophisticated cyber security threats and warns against unsupervised reliance on financial technology service providers.

On January 18, 2018, the United States Office of the Comptroller of the Currency (the OCC) released its Semiannual Risk Perspective for Fall 2017, which highlighted key risk areas facing banks, including vulnerable operating environments, cybersecurity threats and a growing reliance on financial technology service providers. The OCC regulates and supervises national banks and federal savings associations to ensure they operate in a manner that is protective of customers and in compliance with laws governing financial institutions. Consistent with its regulatory mission, the OCC's recently issued report focuses on those issues that threaten the soundness of U.S. financial institutions and relies on bank financial data as of June 30, 2017.[1]

Operational and Compliance Risks

The OCC has recognized that U.S. banks operate in a rapidly evolving risk environment. Cybersecurity threats put large swaths of personally identifiable information and proprietary

[1] The OCC's report is available here.

intellectual property at risk. In an effort to combat sophisticated cybersecurity threats (*e.g.*, phishing), the OCC has recommended that banks implement a layered security approach, which would include strong risk-based authentication, effective network segmentation to prevent further damage should intrusions occur and management of high-value user access. The office also pointed to the use of unpatched, unsupported or out-of-date software and hardware by banks and their service providers as a key risk that can expose data or enable breaches. To mitigate these risks, banks should ensure they operate sound systems that require regular maintenance and system updates, as well as response plans.

The OCC has warned that U.S. banks' growing reliance on third-party financial technology service providers has introduced not only innovative products and services to customers, but also potential risks. In a technology landscape where a limited number of financial technology companies service large segments of the banking industry, operational vulnerabilities and intrusions at these larger service providers put wide segments of the financial industry at risk.

Moreover, the office pointed to the increased use of a limited number of third-party service providers for specialized services (*e.g.*, merchant card processing, denial-of-service mitigations, or settlements and custody) as an area where concentrated points of failure result in systemic risk to the financial service sector that banks can proactively address through due diligence and oversight. The OCC indicated that companies providing, for example, information technology products and services are increasingly the targets of attackers, and, if successfully attacked, these third-parties provide direct access to a bank's operations. This trend, according to the OCC, led to many of the largest breaches in 2017. To decrease vulnerabilities faced by banks due to their use of third-party service providers, the OCC has reiterated that third-party risk management remains a supervisory focus for banks.

Finally, the OCC further pointed to the compliance risk faced by U.S. banks. Where consumer protection regulations rapidly evolve in response to new cybersecurity threats, banks risk lagging behind such regulations and face difficulty creating systematic approaches to remaining in compliance. Banks are obligated to be aware of regulatory changes and have compliance risk management systems commensurate with the risks inherent in their products and services. A bank's inability to keep pace with the increasing complexity of the regulatory and risk environments in which they operate invites regulatory and public scrutiny of its consumer protection activities. The OCC recommended that management understand the risk exposure associated with an inability to comply with regulations and should adopt measures to address them appropriately.

Key Takeaways

The OCC's report highlights some of the key risks facing all organizations, not just those within the OCC's jurisdiction. In particular, the increased use of third-party service providers, and the limited number of commonly used service providers in certain key areas, can pose a significant risk of attack through these third parties' systems. Companies should examine their security and compliance processes to ensure they are addressing the evolving threats, and they should ensure their security reviews encompass their third-party vendors.

Return to Table of Contents

Internet-Connected Toymaker Settles COPPA and FTC Act Charges

In its first action involving internet-enabled toys, the FTC has settled a case with toymaker VTech involving alleged violations of the FTC Act and the Children's Online Privacy Protection Act.

On January 8, 2018, Hong Kong-based electronic toy manufacturer VTech Electronics Limited and its U.S. subsidiary (VTech) agreed to settle charges by the Federal Trade Commission (FTC) that they violated the FTC Act and the Children's Online Privacy Protection Act (COPPA). The settlement provides valuable guidance on the applicability of U.S. privacy law to internet-connected devices, especially with respect to devices directed to children under the age of 13.[2]

FTC Authority and Guidance on Internet-Connected Devices

The FTC has broad authority under Section 5(a) of the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce."[3] The FTC also enforces COPPA which — among other matters — requires companies that provide a website or service directed to children under the age of 13 to:

- provide a clear and conspicuous privacy policy detailing their information practices;
- obtain verifiable consent from parents before collecting personal information from children;
- provide parents an opportunity to review and delete any personal information collected about their children; and

[2] The FTC's press release and related documents are available here.

[3] *See* 15 U.S.C. § 45(a).

- implement reasonable procedures to protect children's personal information.[4]

In June 2017, the FTC updated its guidance on COPPA to clarify that the statute applies not only to websites and online services, but also to internet-connected devices.

VTech's Internet-Connected Devices

VTech sells portable devices known as "electronic learning products" throughout the world. It markets the products as appropriate for children aged three to nine. On these devices, VTech offers a platform similar to an app store that allows customers to download child-directed apps, games, e-books and other online content developed by VTech. By November 2015, more than 2 million parents created accounts for almost 3 million children. VTech also offers an app on the platform called "Kid Connect," which allows children to send text messages, audio messages and photos to other children and to adults who download the version of the app for adults on Apple's App Store or Google Play. Before children could use Kid Connect, parents had to register on VTech's platform and submit their full names and email addresses, along with their children's names, dates of birth and genders.

FTC Claims Against VTech and Settlement

The FTC alleged that VTech violated Section 5(a) of the FTC Act when it falsely represented that most personal information submitted by consumers and all registration information on its platform and Kid Connect would be transmitted in an encrypted form. In fact, according to the FTC's complaint, VTech did not encrypt such information in transmission.

With respect to COPPA, the FTC made the following allegations:

- **Privacy Policy Visibility:** VTech failed to (1) post its privacy policy in a conspicuous place (it was included in a small link with blue font in the bottom right corner of the Kid Connect registration page); (2) link its privacy policy in each area of the Kid Connect app where personal information was collected from children; and (3) link its privacy policy on the landing screen of the Kid Connect parent app.
- **Privacy Policy Content:** VTech failed to disclose in its privacy policy (1) its address and email address (so that parents could contact VTech); (2) a full description of the types of information collected from children; and (3) information about parents' right to review or delete their child's personal information.
- **Failure to Provide Parents With Direct Notice:** VTech failed to provide a direct notice of its information practices to parents.
- **Unreasonable Data Security:** VTech failed to (1) implement or maintain a comprehensive information security program; (2) implement a detection system for unauthorized access to its network; (3) implement a tool to monitor for attempts to export personal information stored on its network; (4) perform vulnerability or penetration testing of its environments; and (5) implement reasonable guidance and training for employees regarding data security and the safeguarding of personal information.

As a result, according to the FTC complaint, an individual gained unauthorized access to VTech's network and stole personal information about children and parents. Most of the information was stored in clear text. Although VTech stored passwords and children's photos and audio files in an encrypted format, a database accessed by the intruder included decryption keys for the photos and audio files, which would have allowed the intruder to access those files and link them to the name and address information stored in clear text.

Settlement and Substantial Fine

The FTC recently announced a settlement with VTech over these issues. According to the terms of the settlement, VTech agreed to pay $650,000. It also will have to submit its data security program to independent audits for the next 20 years. The size of the fine and the length of the audit obligation suggest that the FTC takes privacy issues involving children very seriously.

Key Takeaways

This was the FTC's first case involving children's privacy rights and internet-connected toys. The case highlights the stringent rules — and heavy penalties — associated with the collection and use of children's information in violation of COPPA. Although the complaint and settlement may be most useful in guiding companies that offer children's products, companies that offer internet-connected devices for general audiences still can gain insight from the FTC's complaint and settlement in this case. The FTC alleged claims not only under COPPA, but also based on the deceptive statements made by the company.[5] To avoid claims under the FTC Act, companies that offer internet-connected devices should consider both the representations they make to consumers and their data security practices.

Return to Table of Contents

[4] *See* 16 C.F.R. § 312.3.

[5] The FTC did not allege that VTech's inadequate data security constituted an "unfair" practice under Section 5(a).

British Electronic Goods and Mobile Phone Retailer Fined for Data Breach

British privacy authorities have levied a fine of more than $500,000 against a British company that suffered a data breach.

On January 10, 2018, Britain's Information Commissioner's Office (ICO) announced its decision to fine Carphone Warehouse £400,000 ($559,450) for a 2015 data breach that compromised the personal data of its customers.

Data Breach

Carphone Warehouse is a British electronic goods and mobile phone retailer. In 2015, hackers accessed Carphone Warehouse's online system through an old version of its website on content host Wordpress using valid login credentials. Hackers gained access to names, addresses, phone numbers, dates of birth and marital status for more than 3 million customers, as well as the payment information of more than 18,000 customers. Some Carphone Warehouse employees' personal data also was accessed, including car registration details. Affected customers and employees were informed of the attack at the time. The ICO and Carphone Warehouse have found no evidence of fraud or identity theft as a result of the breach.

Fined for Inadequate Cybersecurity Practices

According to the ICO investigation, the Wordpress installation on one of Carphone Warehouse's websites was out-of-date and exposed and suffered from multiple vulnerabilities. The attacker was able to scan the system using what the ICO considered a relatively commonplace penetration tool for testing security issues such as outdated software and other vulnerabilities. In addition to this oversight, the attacker was able to locate credentials in plain text (information that was inadequately protected by encryption) that he or she used to search large databases for personal and payment information.[6]

The ICO fined Carphone Warehouse £400,000 ($559,450), which it described as among its largest fines to date.[7] In a statement, Information Commissioner Elizabeth Denham said: "Carphone Warehouse should be at the top of its game when it comes to cyber-security and it is concerning that the systemic failures we found related to rudimentary, commonplace measures." She went on to comment that "a company as large, well-resourced, and established as Carphone Warehouse should have been actively assessing its data security systems, and ensuring systems were robust and not vulnerable to such attacks."

Key Takeaways

The ICO's steep fine against Carphone Warehouse reflects both the office's view of the importance of incentivizing strong cybersecurity measures for companies that hold personal information, as well as its critical assessment of Carphone Warehouse's practices in particular. Companies that operate in the United Kingdom should take heed of this action and carefully review their cybersecurity practices to avoid facing similar sanctions.

Return to Table of Contents

Aetna Pays $18.2 Million to Settle Non-IT Data Breach Claims

Insurance giant Aetna has agreed to pay more than $18.2 million to settle two separate data breach claims arising out of the inadvertent disclosure of health information due to the layout of the envelopes it used for customer communications.

On January 17, 2018, Aetna announced it had agreed to pay $17.1 million to settle claims related to a data breach that may have revealed customers' HIV status information. One week later, the New York attorney general announced that Aetna agreed to pay an additional $1.15 million to settle claims related to that breach, as well as a separate breach the office discovered while investigating the initial breach. The $17.1 million settlement appears to be among the largest per-person payments for cases involving security breaches, likely owing in part to the nature of the data released.

Non-IT Breaches

The data breach in question did not involve access to any electronic database, but rather to the type of envelope Aetna used to send information to customers in July 2017. Specifically, certain HIV-positive Aetna customers received letters from the company using an envelope that featured a clear window. Due to the layout of the information on the enclosed letter, the recipients' HIV status was visible through the window, without opening the envelope. In all, the incident affected nearly 12,000 people.

[6] For more detailed information on the investigation, please see the ICO's Monetary Penalty Notice here.

[7] The final cost of the fine is expected to be £320,000, since the ICO offers a 20 percent discount on penalties that are paid less than a month after being issued.

According to the complaint, Aetna also released the names of more than 13,000 people to its counsel and a vendor without proper authorization in connection with the potential litigation over the envelopes.

As the New York Attorney General's Office investigated the first breach, it discovered a second, similar issue arising out of mailings sent to individuals suffering atrial fibrillation. Again, the clear plastic window on the envelope allowed people to see information revealing the health status of the intended recipients.

Settlements

A class action suit was filed against Aetna, claiming as harm the disclosure of the customers' HIV status and the resulting attacks and other repercussions against them. Aetna settled the case, agreeing to pay $17.1 million, which includes $12 million that will be used to pay up to $500 to each person who received the revealing letter. In addition, Aetna will set up a fund to pay an additional amount of up to $20,000 to those who experienced financial or emotional distress. Aetna also agreed to develop and implement best practices when handling personal health information in connection with litigation.

The per-customer payments are higher than have been reported for other data breaches, which typically involved unauthorized electronic access to credit card or other information. The increased amount is likely due to the sensitive nature of the information involved.

Separately, the company agreed to pay the New York attorney general $1.15 million to settle claims related to the HIV and atrial fibrillation breaches.

Key Takeaways

The Aetna disclosures and related settlements highlight the need for companies to address privacy issues for both electronic and non-electronic data. While hacks of electronic records may elicit more press coverage, the risks associated with mundane non-electronic tasks can be significant.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000