Skadden

Privacy & Cybersecurity Update

Germany's New Federal Data Protection Act Triggers Uncertainty Over Uniform Privacy Law Throughout the EU

Germany has become the first member state to implement the General Data Protection Regulation (GDPR or Regulation) in its local laws; however, "opening clauses" in the Regulation create an unclear future for the harmonization of privacy law in the EU.

In an effort to conform existing German privacy law with the GDPR, the German Parliament has passed a new version of the country's Federal Data Protection Act (*Bundesdatenschutzgestz* or BDSG), making Germany the first EU member state to adopt national legislation in response to the GDPR.

Implementing 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.

Opening Clauses

In addition to being the first member state to revise its local privacy laws, Germany also is the first member state to introduce additional provisions that supplement the GDPR (to the extent related to personal data of German citizens). As drafted, the GDPR includes a number of "opening clauses" that permit member states to discretionarily customize certain provisions. Some critics consider the use of opening clauses a threat to the promise of the GDPR: namely, increased harmonization in EU privacy law. Moreover, a number of opening clauses reside in provisions that deal with complicated areas of data protection law, including the collection of employee data. For example, Article 88(1) of the Regulation provides that:

> "Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection and freedoms in respect of the processing of employees' persona data in the employment context …"

In effect, the GDPR's opening clauses, such as those governing employee data in Article 88(1), permit member states to individually assert more restrictive obligations than the GDPR requires.

Germany's decision to take advantage of the opportunity offered by the opening clauses is the first example of how a member state may approach strengthening and further specifying the provisions of the GDPR. Summarized below are a few illustrations of how Germany has legislated beyond the GDPR:[1]

- **Processing personal data of employees:** Under Article 88(1), Germany largely has retained its existing rules under the previous BDSG, permitting the processing of employee personal data for: (1) carrying out an employment relationship or (2) complying with obligations under law. Furthermore, consent for collecting an employee's data must be in writing, unless another form is justified due to the circumstances.
- **Processing sensitive data:** Under the GDPR, member states may specify rules for processing sensitive data. Pursuant to the revised BDSG, Germany has created a legal basis for processing sensitive data under the following circumstances: (1) for scientific, statistical or historical research purposes, where the processing is necessary and the interests of the data controller prevail over the interests of the data subject; or (2) where processing of sensitive data is necessary to exercise the rights arising out of the right to social security and social protection.
- **Fines:** Pursuant to Article 84(1) of the GDPR, member states must establish penalties applicable to infringements of the GDPR, in particular for infringements which are not subject to administrative fines pursuant to Article 83. Using this opening clause, Germany has stipulated that those committing administrative offenses by mishandling personal information or failing to inform a consumer within prescribed time limits are subject to fines up to €50,000.

Timing

The latest version of the BDSG was published in the *Federal Law Gazette* on July 5, 2017, and will go into effect simultaneously with the GDPR on May 25, 2018.

[1] The Federal Republic of Germany has yet to release an official translation of the BDSG. This summary is based upon unofficial translations.

Key Takeaway

In addition to planning for future compliance under the GDPR, companies operating in multiple EU member states should consider whether each member states' laws are applicable to their operations. As additional countries take advantage of the opportunity to modify the GDPR's requirements, local requirements in each member state may vary, and these companies should take care to be familiar and compliant with all that apply.

Return to Table of Contents

Loan Facilitator Pays FTC $104 Million Over Unfair and Deceptive Practices

A company that claimed to offer loan services to consumers has agreed to pay the Federal Trade Commission $104 million to settle claims that it engaged in unfair and deceptive practices in connection with its collection and use of loan application information.

On July 5, 2017, the FTC entered into a settlement agreement with Blue Global Media, LLC in relation to the company's collection and use of loan application information from consumers.[2] In connection with the settlement, Blue Global Media agreed to pay the FTC $104 million, as well as to reform its activities. The company and its CEO, Christopher Kay, have since filed for Chapter 7 bankruptcy, and its operations have been shut down.

Background

Blue Global Media operated 38 separate websites such as 100dayloans.com, 1hour-advance.com, cashmojo.com and clickloans.net to advertise to consumers that it would search a diverse network of over 100 lenders to provide applicants with favorable loans, ranging from payday loans to auto loans. Applicants provided sensitive data, including their names, Social Security numbers, birthdates, addresses, employment information, approximate credit scores, applicable bankruptcy information, military status, driver's license identification numbers, incomes, and bank routing and account numbers.

According to the FTC's complaint, rather than seek loans for the applicants, Blue Global Media sold the applicants' information as "leads" to various outside parties, without verifying how those

[2] The proposed order implementing the settlement is available online.

parties would use or secure the information.[3] The first buyer to accept the lead would receive exclusive rights to the information in that loan application. According to the FTC, only 2 percent of loan applications were actually sold to lenders, and the remaining 98 percent were sold or distributed to non-lenders, many that were not legally authorized to offer loans. Further, rather than seeking loans from a network of 100-plus lenders, the FTC found that only 17 lenders, on average, considered any particular application. In the end, each "lead" netted Blue Global Media about $200.

The FTC also alleged in its complaint that, even after consumers complained about misuse of their information, the company took no action to rectify the matter.

FTC Authority

The FTC has broad authority to prohibit "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act.[4] As the FTC explains, its standards, deceptive acts or practices "contain[] a misrepresentation or omission that is likely to mislead consumers acting reasonably under the circumstances to their detriment … deceptive claims are actionable only if they are material to consumer's decisions to buy or use the product [and] the Commission need not prove actual injury to consumers."[5] Unfair acts or practices occur when "an advertisement or trade practice causes or is likely to cause substantial consumer injury that is not reasonably avoidable by consumers themselves and which is not outweighed by countervailing benefits to consumers or competition."[6] With respect to unfairness (but not deception) claims, the FTC also must show substantial injury, which includes financial harm. Earlier this year, the acting FTC chairwoman, Maureen K. Ohlhausen, stated that "substantial injury" should also encompass health and safety risks.

Complaint Against Blue Global Media

In its complaint, the FTC alleged that Blue Global Media engaged in both deceptive and unfair business practices in violation of the FTC Act.

Deception

The FTC alleged that Blue Global Media made a number of false and misleading representations to consumers in its advertising materials and on its websites, including by claiming that it would:

- match consumer loan applications to the lowest interest rate;
- search loan offerings of 100 or more lenders;
- secure consumer data and share it only with lending partners; and
- approve most consumers' loan applications.

According to the FTC, Blue Global Media failed to follow through on any of these assurances.

The FTC's complaint noted that Blue Global Media did make disclaimers regarding its practices that contradicted some of its false promises, but noted that these were "buried in lengthy online terms" and were not as prominent as the deceptive statements made in its advertising. These inconspicuous disclaimers were not enough, in the FTC's view, to overcome the deception in the advertising.

Unfairness

The FTC alleged that Blue Global Media's practice of selling and sharing sensitive consumer data without consumer consent and without regard for who was receiving the data constituted an unfair business practice.

In its complaint and proposed settlement order, the commission did not explain clearly the injury suffered by the consumers — an essential element of an unfairness claim. It did note in its filings the risk of identity theft and fraud due to the information sharing (without citing any examples of these harms), and it noted that some consumers received demands for payment of debts they did not owe from people who had purchased the information from Blue Global Media but, again, did not cite examples of consumers actually being defrauded.

Key Takeaway

The Blue Global Media case illustrates a number of themes in the FTC's ongoing efforts related to data practices. First, companies will be held responsible for complying with promises made to consumers, including those made in advertising and promotional materials. Second, companies should be careful to keep the promises they make to consumers regarding their data practices, in terms of how information is used, who will have access to

[3] The complaint is available online.

[4] 15 U.S.C. § 45(a).

[5] Deception Policy Statement, appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984). Accessible here.

[6] Unfairness Policy Statement, appended to *Harvester Co.*, 104 F.T.C. 949, 1070 (1984). *See* 15 U.S.C. § 45(n). Accessible here.

it and how it is secured. Third, disclaimers — especially those hidden deep in long legal terms — may not be enough to overcome deceptive statements in other forms. Finally, the FTC takes a broad view of the types of injury that consumers must suffer for the commission to bring an unfairness claim — one that is broader than that taken by many courts.

Penalties for noncompliance with Section 5 of the FTC Act can lead to an FTC investigation, costly litigation, hefty fines and damage to reputation. Companies must be mindful of the lessons to be learned from the FTC's cases to date.

Return to Table of Contents

District Court Dismisses Data Breach Lawsuit Against Toymaker VTech

An Illinois court dismissed a data breach lawsuit brought against VTech Electronics, a maker of digital learning toys for children, finding that the plaintiffs lacked standing to sue for identity theft and failed to adequately plead breach of contract and other related claims.

In *In Re: VTech Data Breach Litigation*,[7] the U.S. District Court for the Northern District of Illinois dismissed a lawsuit brought by adults and children affected by a November 2015 data breach of VTech. The court first determined that the plaintiffs had Article III standing to pursue their contract-based claims that the toys were worth less than the purchase price because of the inadequate security, but did not have standing to claim future harm and mitigation expenses as a result of the breach. The court nevertheless dismissed the contract-based claims, which were based on security promises in the Privacy Policy for related online services, ruling that the plaintiffs' payment for the toys did not constitute payment for the separate and complimentary online services that collected and ultimately exposed their personal data.

Background and Claims

Defendant VTech sold electronic educational toys that provided access to an online library of educational games, software and other content. Some of the toys included a communication platform where parents and children could exchange messages. To use the online features of the toys, customers had to submit personally identifiable information, which was stored on VTech's servers. Plaintiffs alleged that VTech's privacy policy promised that the customer data would be encrypted and stored offline, but that VTech failed to follow through on those promises.

The lawsuit arose from a breach in November 2015, when a hacker accessed VTech's servers and downloaded the personally identifiable information of 4.8 million adults and 6.3 million children, including names, e-mail and mailing addresses, IP addresses, download and purchase histories, passwords and answers to security questions. The data also included childrens' names, genders, birthdates, photos, and the communications between children and parents from VTech's online systems. To investigate the breach and update its data security protocols, VTech suspended all online access for almost two months following the incident. VTech later restored some, but not all, of the online services.

The plaintiffs brought claims for breach of contract, breach of the implied covenant of good faith and fair dealing, breach of the implied warranty of merchantability, and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act. In particular, the plaintiffs claimed they faced increased exposure to identity theft and worried about their children's safety. They also claimed they would have paid less for the products or not purchased them if they had known of VTech's inadequate security.

The Court's Decision

On July 5, 2017, Judge Manish S. Shah granted VTech's motion to dismiss without prejudice. As an initial matter, the court rejected on standing grounds the plaintiffs' contentions about future identity theft, holding that the plaintiffs "fail[ed] to make the connection between the data breach they allege[ed] and the identity theft they fear[ed]." In doing so, the court distinguished two leading Seventh Circuit cases in which data breach plaintiffs were found to have standing: *Lewert v. P.F. Chang's China Bistro*[8] and *Remijas v. Neiman Marcus Grp., LLC*.[9] The court emphasized that, unlike in *Lewert* and *Remijas*, the plaintiffs did not allege the exposure of their credit or debit card information or fraudulent transactions resulting from the data breach. The court did, however, find that the plaintiffs had standing to allege overpayment for VTech's products. Citing a recent Eighth Circuit case,[10] the court held that an economic injury sufficient to confer standing "can result from being given a different, less valuable product than the one that was promised and paid for."

[7] No. 15-CV-10889, 2017 WL 2880102 (N.D. Ill. July 5, 2017). A copy of the opinion and order can be found here.

[8] 819 F.3d 963 (7th Cir. 2016).

[9] 794 F.3d 688 (7th Cir. 2015).

[10] *Carlsen v. GameStop, Inc.*, 833 F.3d 903 (8th Cir. 2016).

Despite finding standing, the court nevertheless rejected each of the plaintiffs' claims for relief. Even though VTech allegedly failed to abide by the promises in its Privacy Policy regarding cybersecurity, the court found that there was no breach (actual or implied) because the plaintiffs' purchases of the toys did not include simultaneous purchases of the online services: "[T]here is a difference between selling a product that combines both a physical toy and a service, and selling a physical toy whose features may be supplemented by a separate service that VTech provided for free." Because the online services were not part of the original purchase, they did not bear on the plaintiffs' claimed harm of overpayment. The court also emphasized that the plaintiffs had agreed to a provision in the terms of the online services in which VTech reserved the right to suspend or terminate the online services. Finally, the court found that the children plaintiffs were not third-party beneficiaries to the contract between VTech and the adult purchasers.

Key Takeaway

This decision marks a potential limit to significant rulings from the U.S. Court of Appeals for the Seventh Circuit on Article III standing in data breach cases. Those prior rulings had found standing in cases involving the theft of payment card data, reasoning that the presumed purpose of the theft was to make fraudulent charges or engage in identity theft. According to the court, that rationale did not extend to VTech because the breach did not expose payment card information, even though other sensitive information was exposed. This ruling also serves as a reminder that companies should ensure that they abide by promises made to customers about cybersecurity and data privacy. Although VTech escaped liability in this instance, the court's decision rested on a narrow distinction that most companies will not be able to rely on to secure the dismissal of a lawsuit.

Return to Table of Contents

Recent Report Highlights Cyber Insurance as Key Component of Cyber-Readiness Strategy

A recent report on the results of a multi-industry cybersecurity survey shows that respondents expect cyberattacks to continue to rise and highlights the importance of cyber insurance in a company's overall cyber-readiness strategy.

The steady rise in cybercrime has prompted businesses across the globe to adopt cybersecurity protocols to protect against and mitigate the damaging effects of cyber incidents. A recent report commissioned by analytics firm FICO and written by Ovum Consulting (Report)[11] examines what businesses are doing to improve their cybersecurity positions based on the results of a multi-industry survey of IT directors, senior managers and a mix of security managers at businesses across North America and Northern Europe. It also identifies areas in which improvements are needed to enhance cyber readiness. The Report concludes, among other things, that cyber insurance coverage should be "a key part of an enterprise security strategy" and, to this end, proposes solutions to increase cyber insurance take-up and ultimately improve the cybersecurity positions of businesses worldwide.

Report Findings

When questioned about their organizations' cyber threat experience over the last 12 months, nearly all survey respondents (99 percent) said that cyberattacks either have increased or remained the same, the Report indicates. Prior cyberthreat experience drove respondents' expectations for future cyberthreat levels: According to the Report, 99 percent of respondents said that they expected the level of cyberthreats against their organizations either to increase (62 percent) or remain steady (37 percent) over the coming year. The telecommunications and financial services industries had the highest percentages of respondents say that they expected to see an increase in cyberattacks against their organizations (81 percent and 76 percent, respectively).

Against this backdrop, the vast majority of respondents said that their organizations plan to manage cybersecurity threats either by maintaining the same level of cybersecurity spending as the previous year (52 percent) or increasing such spending (48 percent), Ovum reports. Respondents in the financial services industry reported the highest level of increase in investment (56 percent), while respondents in the health care industry reported the lowest (37 percent). In terms of cybersecurity spending, the Report states that 70 percent of respondents are making use of security monitoring, scoring and reporting products. According to the Report, other reported cyber-readiness strategies included data breach response plans (utilized by 51 percent of respondents' organizations) and board level cybersecurity oversight (utilized by 59 percent of respondents' organizations).

Cyber Insurance

The Report suggests that cybersecurity spending also should extend to cyber insurance, which, in Ovum's opinion, "has a vitally important role to play" in improving businesses' cybersecurity positions because it "provides enterprises with a means

[11] Andrew Kellett, "What the C-suite Needs to Know About Cyber-readiness" (2017).

of transferring financial and business risk away from the organization." According to the Report, cyber insurance take-up is on the rise, with 60 percent of respondents reporting that their organizations had some form of cyberrisk insurance and 23 percent of respondents reporting that their organizations plan to introduce cyber insurance in the next year. The Report cautioned, however, that there are still significant strides to be made with respect to cyber insurance, citing that 17 percent of respondents' organizations had no plans to purchase cyber insurance and only 20 percent of respondents whose organizations do have cyber insurance considered the coverage to be "comprehensive."

The Report posits that businesses may be reluctant to incorporate comprehensive cyber insurance into their cybersecurity strategies due to pricing and the lack of clarity with respect to premium calculations. Indeed, when asked for their views on cyber insurance pricing, only 25 percent of respondents said their organizations' cyber insurance premiums were based on business assessments that accurately reflected their organizations' risk profile. About 30 percent of respondents said that the premium calculations for their organizations' cyber insurance either were unclear or were based on business assessments that did not accurately reflect their organizations' risk profile.

In order to increase the number of businesses with cyber insurance and thereby improve cyber readiness, the Report concludes that greater clarity is needed from the cyber insurance industry with respect to pricing structures. According to the survey results, only 23 percent of respondents said that the insurance industry is "clear and transparent" about pricing. The remainder of respondents said that the insurance industry could help businesses better understand pricing in the following ways: Provide clear guidelines to show how premiums are determined (27 percent), introduce industry standards to benchmark cybersecurity risk (26 percent) and offer clearer explanations as to why premium adjustments occur (23 percent). The Report also suggests that business organizations can help improve the transparency and efficiency of the pricing process by using the cyberrisk assessment tools made available by many insurers, which "would help insurers target their pricing more accurately."

Overview

While there is no one step that businesses can take to ensure cyber readiness, as the Report acknowledges, the inclusion of cyber insurance in a company's overall cybersecurity strategy serves to improve cyber readiness and help mitigate the negative impact of cyber incidents.

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

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

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

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

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