Skadden

Privacy & Cybersecurity Update

1 Brazil Passes Its First General Data Protection Law

3 French Data Protection Authority Issues Warning to Two Companies for Potential GDPR Violations

3 DHS Announces New Cybersecurity Center Aimed at Public-Private Coordination of Cyber Operations

4 Sixth Circuit Says Policyholder's Social Engineering Loss Covered by Computer Fraud Policy

5 Japan and EU Announce Adequacy Decision

Brazil Passes Its First General Data Protection Law

Brazil has enacted a new data protection law modeled on the European Union's General Data Protection Regulation.

On July 10, 2018, Brazil's Federal Senate (Federal Senate) unanimously approved the country's first General Data Protection Law (Lei Gerald de Proteção de Dados, or the LGPD),[1] which was signed into law by Brazilian President Michel Temer on August 14, 2018. Much like the European Union's General Data Protection Regulation (GDPR), the LGPD establishes a comprehensive data protection system in Brazil and imposes detailed rules for the collection, use, processing and storage of electronic and physical personal data. The regulation will go into effect in February 2020.

Key Elements of the LGPD

Personal Data

Like the GDPR, the LGPD broadly defines "personal data" to include any information, whether by itself or in the aggregate, that is relatable to an identifiable natural person, and includes certain provisions that govern the collection and use of "sensitive personal data," which is defined as data that inherently places a data subject at risk of discriminatory practices. Sensitive personal data may include information on racial or ethnic origin, religious belief, political opinion, health and other information that allows unequivocal and persistent identification of the data subject, such as genetic data. Anonymized data is not considered personal data.

Extraterritorial Jurisdiction

The LGPD also is similar to the GDPR in its broad extraterritorial application. The Brazilian law applies to companies that: (1) carry out processing of personal data in Brazil; (2) collect personal data in Brazil; (3) process data related to natural persons located in Brazil; or (4) process personal data for the purpose of offering goods or services in Brazil.

[1] No official English translation of the LGPD has been provided.

Legal Basis for Data Processing

The LGPD provides 10 unique legal bases for processing personal data, which include when data processing is:

- done with the express consent of the data subject;
- necessary for compliance with a legal or regulatory obligation;
- necessary for the fulfillment of an agreement;
- necessary for the exercise of rights in a judicial, administrative or arbitration proceeding;
- necessary to protect life or physical integrity;
- necessary to protect health;
- necessary for the implementation of political policies (for processing by the government);
- necessary for purposes of credit protection;
- necessary to meet the legitimate interest of the data controller or third parties; or
- necessary for the performance of historical, scientific or statistical research.

With respect to consent of the data subject, the LGPD provides that consent may be waived where the data subject has "manifestly made public" his or her personal data. Where consent is not waived, a data subject's consent must be informed, revocable and provided for a specific purpose prior to the processing of the data subject's personal data.

Data Protection Officers

The LGPD requires each data controller to appoint a data processing officer (DPO) whose responsibilities will include oversight of the organization's data processing activities and facilitation of data subject requests. This DPO role differs from the data protection officer role under the GDPR in that the LGPD DPO is an independent overseer of the company's data protection activities and, as such, is not liable for such activities. The DPO may be an officer or an employee of the data controller, or of a third party provider, but in each case much perform his or her duties autonomously. In addition, unlike the GDPR, the LGPD DPO requirement applies to *all* controllers, without exceptions for small businesses or small-scale processors, although it is possible that the national data protection authority, once established, may identify certain exceptions to this requirement.

Data Protection Impact Assessment

The LGPD requires companies to generate a data protection impact assessment (DPIA) before undertaking personal data processing activities that may put data subjects at higher risk. The DPIA must document data processing activities that may create risks to data subjects, as well as the measures, safeguards and mitigation mechanisms the company has implemented to address those risks.

Data Transfer Restrictions

The LGPD imposes restrictions on cross-border transfers of personal data. Personal data may only be transferred to countries deemed to provide an adequate level of data protection, or pursuant to standard contractual clauses or other approved mechanisms. These adequacy decisions, standard contractual clauses and other transfer mechanisms will be issued by the national data protection authority when created.

Data Breach Notification

The LGPD requires companies to notify the national data protection authority within a "reasonable" time of any data breach. The period of time defined as reasonable is still to be determined by the data protection authority, though some experts believe that it is likely to mirror the GDPR's 72-hour notice period given the overall similarities between the LGPD and the GDPR. Following receipt of the notice, the data protection authority will determine whether the data subjects must be notified and what mitigating steps must be taken by the company.

Penalties

The LGPD provides that the national data protection authority may impose sanctions for violation of the LGPD, including fines, or potentially even the total or partial prohibition of activities related to data processing. Fines may be up to 2 percent of the company's turnover in Brazil in its last fiscal year, limited in total to 50 million Brazilian reais per infraction (approximately US$12 million).

Key Takeaways

Companies that are already compliant with the GDPR will likely be in a position to comply with the LGPD without significant additional effort, as the two regulations include similar requirements for data processing, DPIAs and data transfers. Companies with data processing activities in Brazil and companies outside of Brazil that collect personal data from Brazilian residents should continue to monitor the implementation of the LGPD by Brazilian officials over the next 18 months so they can tailor their compliance programs accordingly.

Return to Table of Contents

French Data Protection Authority Issues Warning to Two Companies for Potential GDPR Violations

France's data protection authority published a formal warning to two French companies regarding their geolocation data collection and retention practices. The warning provides some clarity on the GDPR's consent and data retention standard.

In late July 2018, France's data protection authority, the Commission Nationale de L'informatique et des Libertés (CNIL), published a formal warning to two companies — Teemo, Inc. (Teemo) and Fidzup SAS (Fidzup) — that allegedly collected and retained geolocation data in violation of the EU's GDPR.[2] The CNIL did not impose any fines on the companies, but stated that Teemo and Fidzup may be subject to penalties if they fail to obtain valid consent from data subjects and set an appropriate retention period for geolocation data within three months.

Teemo and Fidzup's Personal Data Practices

Teemo and Fidzup provide software development kits (SDKs) that can be used in mobile applications to track the locations of users for purposes of sending targeted advertisements. Teemo's SDK enables the collection of users' geolocation data every five minutes. Fidzup's SDK makes it possible to send targeted advertisements to users' mobile phones whenever users are near a point-of-sale system installed by Fidzup.

Teemo and Fidzup maintained that they had received users' consent to collect and process geolocation data. However, the CNIL performed audits and determined that the companies did not obtain users' consent in a manner that would satisfy the GDPR's requirements.

The CNIL found that users who downloaded mobile applications that incorporate Teemo's SDK generally did not receive notice of Teemo's geolocation data collection practices. When users downloaded a mobile application that included Fidzup's SDK, the CNIL found that users generally did not receive any information about Fidzup's purpose for collecting geolocation data or other information required under the GDPR. The CNIL also found that users could not download mobile applications without the SDKs and that users consented only to data processing by the mobile application provider and not for targeted advertising purposes.

Data Retention Under the GDPR

The CNIL's warning to Teemo also provides some insight into how the CNIL views data retention practices under the GDPR. With some limited exceptions, the GDPR requires that personal data be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. The GDPR offers little guidance on how that determination should be made. In its warning, the CNIL stated that by retaining geolocation data for 13 months, Teemo violated its obligations under the GDPR to define and respect a data retention period proportionate to the purpose of the processing.

The CNIL noted that the use of geolocation devices is particularly intrusive with regard to individual freedoms, given that such devices allow companies to follow users permanently and in real time, but did not expressly explain why 13 months is too long a period of time to retain geolocation data for targeted advertising purposes.

Key Takeaways

The warning to Teemo and Fidzup provides some early insight into how data protection authorities like the CNIL may approach GDPR enforcement with respect to the consent and data retention requirement. Companies that must comply with the GDPR should continue to monitor warnings and enforcement actions by EU data protection authorities to inform their data processing practices.

Return to Table of Contents

DHS Announces New Cybersecurity Center Aimed at Public-Private Coordination of Cyber Operations

The Department of Homeland Security (DHS) will create a National Risk Management Center that will focus on protecting critical infrastructure from cyberattacks.

At the National Cybersecurity Summit in New York City on July 31, 2018, the Department of Homeland Security announced the creation of the National Risk Management Center (Center), a new component of DHS's cyber operations. The Center will work directly with federal government and private sector partners to protect infrastructure such as banking, energy and election systems from cyberattacks. The Center will seek to:

- identify and prioritize strategic risks to national critical functions;
- integrate government and industry activities on the development of risk management strategies; and
- synchronize operational risk management activities across industry and government.

[2] A translated version of the CNIL's warning can be found here.

The Center will be a continuation of existing efforts by DHS to protect critical national infrastructure and will work closely with the National Cybersecurity and Communications Integration Center (NCCIC), which was established in 2009. The NCCIC will remain DHS's central hub for sharing threat indicators and providing incident response services. The Center will focus on understanding what threats are truly critical to private companies and the ways in which various public and private entities can communicate more effectively to reduce risk.

During her remarks at the summit, DHS Secretary Kirstjen Nielsen indicated that the creation of the Center was a response to the increasing threat of cyberattacks from foreign actors. Ms. Nielsen referenced Russian interference in the 2016 election and stated that cyberattacks posed a greater risk to national security than physical attacks.

DHS also announced the creation of a task force to be housed within the Center called the Information and Communications (ICT) Supply Chain Risk Management Task Force. The ICT Task Force will recommend solutions for identifying and managing risk within the global supply chain through policy initiatives and public-private partnerships.

At the summit, Secretary Nielsen compared combatting a cyber threats to solving a puzzle. The private sector brings to the table data about trends, implications and effects of an attack on businesses, while the public sector provides intelligence information that can be crucial to identifying the origin of the attack. The National Risk Management Center will focus on engaging both perspectives in hopes of bolstering critical infrastructure systems.

Key Takeaways

The success of the ITC Task Force, and the Center more broadly, may ultimately depend on buy-in from businesses in the private sector. While companies appear to be interested in receiving information regarding potential cyber threats from the government, some remain reluctant to share information with the government for fear of increased exposure to liability. The Center is an indication from the federal government that it recognizes the benefits to be gained from public-private partnerships.

Return to Table of Contents

Sixth Circuit Says Policyholder's Social Engineering Loss Covered by Computer Fraud Policy

On the heels of a widely reported decision by the U.S. Court of Appeals for the Second Circuit holding that an insured was covered by a computer fraud policy for social engineering-related loss, the U.S. Court of Appeals for the Sixth Circuit recently issued a decision extending computer fraud coverage to losses incurred by a company as a result of a fraudulent email scam that wired over $800,000 to the fraudster's account.

On July 13, 2018, the Sixth Circuit reversed a district court decision in favor of Michigan-based tool and die manufacturer, American Tooling Center, Inc. (ATC), concluding that its computer fraud insurer Travelers Casualty and Surety Company of America (Travelers) must cover an $834,000 loss suffered after ATC employees were tricked by an email spoofing scam that caused them to fraudulently wire company money to an imposter's bank account.[3]

The Fraudulent Transfers and ATC's Insurance Claim

The lawsuit, which we discussed in our December 2017 *Privacy & Cybersecurity Update*,[4] arose in 2015, when a fraudster impersonating ATC's Chinese manufacturing vendor, Shanghai YiFeng Automotive Die Manufacturers Co. Inc. (YiFeng), emailed ATC from an address closely resembling YiFeng's and requested payment of over $800,000 in legitimate outstanding invoices to a new bank account that, unbeknownst to ATC, was controlled by the fraudster. After confirming that YiFeng was entitled to payment — but without verifying the new banking information — ATC wired payment to the fraudster-controlled bank account. By the time ATC detected the fraud, the money could not be retrieved.

ATC filed a claim under its Travelers crime policy, which provided computer fraud coverage for any "direct loss" that was "directly caused" by "Computer Fraud," which was defined in part as "[t]he use of any computer to fraudulently cause a transfer." Travelers denied the claim on the basis that ATC's loss was not a direct loss that was directly caused by the use of a computer, and litigation ensued.

The District Court Denies Coverage

The U.S. District Court for the Eastern District of Michigan agreed with Travelers' interpretation of the policy's computer fraud coverage and granted summary judgment in Travelers'

[3] The decision is *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018).

[4] See our December 2017 *Privacy & Cybersecurity Update* here.

favor, holding that ATC's loss was not covered under the policy. The court reasoned that "[g]iven the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds" — ATC's verification that YiFeng was entitled to payment and initiation of the transfers without verifying bank account information — "it cannot be said that ATC suffered a 'direct' loss 'directly caused' by the use of any computer." The court relied on Sixth Circuit precedent stating that "direct" is defined as "immediate" without any intervening events, as well as other district court decisions declining to extend computer fraud coverage to scenarios where an email is merely incidental to a fraudulent transfer.

The Sixth Circuit Reverses

A three-judge panel of the U.S. Court of Appeals for the Sixth Circuit reversed the district court's decision, holding that ATC, not Travelers, was entitled to summary judgment. The panel rejected Travelers' argument that the loss was not a "direct loss" as required under the policy and declined to follow the district court's more narrow interpretation that "defie[d] common sense." The mere fact that ATC legitimately owed $834,000 to YiFeng at the time it made the fraudulent transfer, and that ATC did not realize the fraud (or its loss) until later, did not bar ATC from "direct loss" coverage. The court concluded that there was no intervening event sufficient to break the required "direct" connection and that a direct loss occurred at the time ATC wired money to the fraudster, regardless of the fact that ATC did not find out about the fraud until later.

Similarly, the court rejected Travelers' attempt to limit the meaning of "computer fraud" to "hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer." The policy did not require the fraud to cause the computer's actions and the Sixth Circuit panel refused to limit the definition in this way. Instead, the court held that the money transfer — prompted by the fraudster's email spoofing — was covered by the meaning of "computer fraud" and that the fraud caused the direct loss, as required under the policy, since the ATC employees' actions were all "induced by the fraudulent email." The court declined to apply any coverage exclusions and ultimately reversed the district court's decision, holding that Travelers was required to cover the loss.

On July 27, 2018, Travelers filed a petition for rehearing or rehearing *en banc*.

Key Takeaways

The Sixth Circuit's decision is one of the latest decisions in what appears to be a growing trend in favor of broadly interpreting computer fraud coverage to extend to social engineering scams, even in the absence of a hacking incident or where the loss did not occur immediately after being tricked by the fraudster. Just last month, the Second Circuit similarly found that computer fraud coverage extended to a fraudulent transfer induced by email spoofing.[5]

Policyholders and insurers alike should keep an eye on the growing body of case law addressing coverage for social engineering loss, and insurance policies should be carefully drafted and reviewed to make sure that they properly reflect the parties' intent.

Return to Table of Contents

Japan and EU Announce Adequacy Decision

Japan and the European Union recently announced an agreement to recognize each other's data protection regimes as adequate. Once implemented, the agreement will permit the free flow of personal data between the two jurisdictions.

On July 17, 2018, Japan and the EU agreed to recognize each other's data protection regimes as providing adequate protections for personal data. Once finalized, these "reciprocal adequacy" decisions will allow personal data to flow between Japan and the EU without being subject to additional safeguards. The mutual adequacy finding will enhance the benefits of the Japan-EU Economic Partnership Agreement (EPA), a free trade deal that was announced at the same time.

The European Commission is expected to formally adopt its adequacy decision on Japan in the fall of 2018. In connection with the decision, Japan agreed to implement additional safeguards to align with the EU's standards. Such additional safeguards have not yet been finalized, but will likely include stricter guidelines for the retransfer of personal data that originated from the European Economic Area (EEA) to a third country and additional limitations on the use of sensitive data. Japan also agreed to implement a new mechanism to allow European Economic Area residents to file complaints with Japan's data protection authority if public authorities in Japan unlawfully access their data.

While the discussions between Japan and the EU were ongoing, Japan's Personal Information Protection Commission (PPC) announced draft guidelines regarding the processing of personal data transferred from the EEA following the adequacy recognition.[6] The draft guidelines were published for public comment

[5] The decision is *Medidata Sols. Inc. v. Fed. Ins. Co.*, 729 F. App'x 117 (2d Cir. 2018), which is detailed in our July 2018 *Privacy & Cybersecurity Update* here.

[6] "Guidelines on the Law Concerning the Protection of Personal Information (Handling of Personal Data Transferred by Sufficiency Certification from within the EU)" can be found here. (Japanese only)

in April 2018 and have not yet been finalized. According to the draft guidelines, five major substantive changes will be implemented with respect to the current Japanese regulations, as summarized in the chart below. The guidelines, once finalized, will apply only to personal data transferred from the EEA under the adequacy recognition.

Items in the Draft PPC Guidelines	Current Law in Japan	Proposed Guidelines	Practical Implications
Scope of "Personal Information Requiring Careful Consideration"	Information regarding data subjects' sex life, sexual orientation and labor union membership are not included in "Personal Information Requiring Careful Consideration"	Information regarding EEA data subjects' sex life, sexual orientation and labor union membership shall be treated as equivalent to "Personal Information Requiring Careful Consideration," to align with "sensitive personal data" as defined under the GDPR	Consent of EEA data subject would be required to acquire such information. Provision of such data to a third party by way of an opt-out arrangement would be prohibited (*i.e.*, express consent would be required)
Access rights	Data subjects do not have a right to access their personal data that is to be deleted within six months	Companies shall be obligated to disclose personal data held by them upon the EEA data subjects' request, regardless of the duration for which such data will be held	Companies that collect personal data from EEA residents and retain that data for any period of time will need to comply with requests for disclosure from a data subject
Succession of purpose of use	No specific rules	Personal data of the EEA data subject received from a third party shall only be used in accordance with the purpose for which it was originally collected	Companies will need to confirm and track the purposes for which personal data of EEA residents was originally collected and limit their use of such personal data accordingly. Proper tracking of permitted uses of different data sets may be challenging and may require new technologies or processes with attendant costs
Retransfer of EEA data subject's personal data from Japan to foreign countries	Allowed when: (1) consent of data subject is obtained; (2) adequate steps to ensure the security of the data are taken between the transferor and the transferee; or (3) the transferee is located in a foreign country designated by the PPC	Regarding point (2), protection equivalent to that under Japanese law and the PPC guidelines must be secured as between the transferor and the transferee, either by contract or (when the transferee is a group company) group company's internal rules	The current Japanese law is unclear on the point (2), but the guidelines will clarify that a contract with a third-party transferee is required unless consent of EEA data subject is obtained or the transferee is located in a whitelist country designated by the PPC
Anonymously processed information (that is exempt from certain protections)	Certain data may be treated as "anonymously processed information" even if the information necessary to identify the data subject is kept separately (*i.e.*, the data is readily susceptible to de-anonymization)	In order to be treated as "anonymously processed information," any information from which the EEA data subject can be identified must also be deleted, so that de-anonymization is not possible	To be exempt, companies will need to make sure that any information from which the EEA data subject can be identified should be deleted and not simply separated from the data being processed

Key Takeaways

Today, some companies that transfer personal data from the EEA to Japan do so pursuant to standard contractual clauses (SCC) published by the European Commission. Japanese companies using SCCs might assume they can readily terminate these agreements once the adequacy decision is formally adopted. However, companies should keep in mind that the adequacy decision only applies to EEA-Japan transfers, and SCCs between the EU and other jurisdictions will need to remain in place. Companies also should keep in mind that the EU is likely to issue an updated version of the SCC which complies with GDPR requirements, and which will need to replace current SCCs.

Return to Table of Contents

Privacy & Cybersecurity Update

Contacts

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

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@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

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

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