Skadden

# Privacy & Cybersecurity Update



## GDPR Takes Effect; Survey Suggests Many EU Regulators May Not Be Ready

**On May 25, 2018, the General Data Protection Regulation (GDPR) became effective, marking the beginning of a new era of data regulation for the European Economic Area and companies that collect information from or monitor European Economic Area residents. However, according to a recent *Reuters* survey, GDPR regulators themselves may not be prepared to enforce compliance with the sweeping privacy law.**

While companies and regulators alike have had two years of preparation to comply with the GDPR, there will likely be a period of adjustment for all parties involved in the coming months.

As we reported in our April 2018 *Privacy & Cybersecurity Update*,[1] only a handful of EU member states have passed legislation to harmonize their own local laws with GDPR requirements.

The *Reuters* survey, which polled EU national data protection authorities, suggests this situation had not significantly improved by the time the GDPR came into effect this month. Of the 24 data protection authorities that responded to the survey, 17 reported that they did not have the necessary funding or legislation in place in their jurisdictions to carry out their responsibilities under the GDPR. It should be noted that certain data protection authorities, including the data protection commissioner of Ireland, one of the most active data protection authorities in the EU, declined to take part in the survey.

### Key Takeaways

Companies that are subject to the GDPR may experience varying levels of GDPR enforcement and guidance across EU jurisdictions, at least in the short term. Companies should monitor the legal landscape in the applicable EU jurisdictions to keep abreast of new legislation passed in such jurisdictions that may affect their compliance with the GDPR.

[1] Our April 2018 *Privacy & Cybersecurity Update* can be accessed here.

## ICANN Adopts Temporary Protocol for Continuing Compliance Under GDPR, Restricting WHOIS Database Public Access to Personal Data

**An organization responsible for maintaining vital elements of the internet landscape, the Internet Corporation for Assigned Names and Numbers (ICANN), released a temporary protocol designed to help domain name registry operators continue their current contractual obligations while maintaining compliance under the GDPR. In doing so, the organization restricted public access to domain name-related personal data, making it harder to obtain domain name registration information.**

In the week prior to the GDPR's effective date of May 25, 2018, the Internet Corporation for Assigned Names and Numbers adopted the "Temporary Specification for gTLD Registration Data" (Temporary Specification),[2] which restricts access to the personal information of domain name registrants to users with a legitimate need for such information. Previously, this personal information was publicly available to anyone.

ICANN is an international organization responsible for IP address space allocation, protocol-identifier assignment and coordination of top-level domains used for general purposes (as opposed to country-code domains, which are managed locally). ICANN manages the WHOIS database, which allows users to obtain information about the registration of domain names, including the names and contact information of domain name owners. Under existing agreements with domain name registry operators, ICANN requires operators to collect certain personal information from domain name registrants when selling domain names. The Temporary Specification's goal is to allow ICANN and domain name registry operators to continue to comply with both their existing contractual requirements and the GDPR's new rules.

Under the Temporary Specification, users "with a legitimate and proportionate purpose for accessing the non-public personal data will be able to request such data access through Registrars and Registry Operators," according to an ICANN statement describing the Temporary Specification. Such legitimate purposes include intellectual property and consumer protection, cybercrime and coordinating dispute resolution services for disputes concerning domain names. Without contacting a specific registrar and demonstrating a legitimate purpose to obtain personal data, users of the WHOIS database will only be able to access technical data sufficient to identify the sponsoring registrar of the domain name, the status of the domain name registration, and the creation and expiration dates of the domain name registration. According to ICANN, the sponsoring registrar is obligated to respond to requests for nonpublic data "in a reasonable time." ICANN also implemented complaint mechanisms for users who do not receive responses from registrars in a timely manner.

For the last two decades, the WHOIS system has allowed anyone to obtain data about domain name registrants. On March 26, 2018, ICANN sent a letter to each of Europe's 28 data protection authorities asking them to refrain from enforcing the GDPR against domain name registries for one year while ICANN implements a sufficient new model. In response, the Article 29 Working Party stated that the GDPR does not allow national supervisory authorities or the EU Data Protection Board to create an enforcement moratorium for individual data controllers, stressing that data protection is a fundamental right of individuals. With the GDPR taking effect, domain name registries that violate its rules could face steep fines.

On May 25, 2018, ICANN filed injunction proceedings against EPAG, a Germany-based ICANN-accredited registrar to obtain guidance from the court as to how it should interpret the GDPR as it relates to data collected through the WHOIS database.[3] Prior to ICANN filing the lawsuit, EPAG informed ICANN that when it sells new domain name registrations, it will no longer collect administrative and technical contact information, as it believes the collection of such information violates the GDPR. However, ICANN requires such information to be collected under its contract with EPAG. ICANN seeks a court ruling to ensure that the continued collection of data about domain name registrants, and the distribution of this data to individuals with a legitimate purpose to access it, complies with the GDPR.

### Key Takeaways

ICANN's new system marks a significant change for intellectual property practitioners and will influence trademark and domain name availability analysis, trademark enforcement and due diligence in corporate acquisitions. Combating trademark

[2] For more information, visit ICANN's website.

[3] More information about ICANN'S legal proceeding is available here.

infringement, stopping counterfeiting activities and confirming the ownership of domain names is likely to become more burdensome and time-consuming. As regulators, companies and administrative organizations like ICANN become more familiar with the practical application of the GDPR's requirements in the coming months, and as court rulings like the one ICANN seeks in the EPAG matter are issued, we expect that an accepted treatment of domain name registrant information will eventually emerge. In the meantime, companies engaged in due diligence or intellectual property enforcement matters may find it difficult to access this information in a timely manner.

Return to Table of Contents

## New FTC Commissioner Suggests Increased Enforcement Efforts Against Repeat Corporate Offenders

**A newly sworn-in commissioner of the Federal Trade Commission (FTC) commented on the need for more stringent enforcement policies for repeat offenders of administrative and court orders.**

On May 14, 2018, newly sworn-in Federal Trade Commissioner Rohit Chopra called on the Federal Trade Commission to seek more aggressive penalties against companies that repeatedly violate administrative and district court orders.[4] Commissioner Chopra's published comments suggest that the agency consider a wide breadth of remedies against repeat offenders, including dismissal of senior management and board directors, changes to executive compensation and closure of relevant business lines. Although the new commissioner's comments are not legally binding and do not necessarily reflect the views of the FTC, they provide insight on how the FTC may enforce compliance violations by repeat offenders going forward. Whether this will have an impact on how the FTC pursues companies who violate privacy or cybersecurity orders remains to be seen.

### Structural Remedies to Address Corporate Recidivism

Commissioner Chopra emphasized that in order to maintain its credibility, the FTC needs to enforce its orders and seek penalties when companies repeatedly violate those orders. Although the FTC already has strong tools in place to ensure compliance with its orders[5] — including civil penalties of up to $41,484 per violation of an administrative order — Commissioner Chopra outlined several more aggressive enforcement mechanisms that he believes the FTC should consider when confronted with repeat offenders:

- **Bans on Certain Business Practices.** The FTC has banned select companies from engaging in certain business practices after concluding that such companies could not be trusted to conduct those practices in a lawful manner. For example, Commissioner Chopra cited an FTC settlement that banned the operators of a fake debt-collection scheme from participating in the debt-collection business going forward. Commissioner Chopra suggested that such bans may be appropriate where a company repeatedly and flagrantly fails to comply with laws specific to certain business practices.
- **Closure of Certain Operating Units.** Although companies facing an FTC enforcement action sometimes assert that repeated issues within a specific operating unit can be ascribed to a few rogue employees, Commissioner Chopra suggested that forced closure or divestiture to new ownership and management may be appropriate in certain instances.
- **Dismissal of Senior Executives and Board Directors.** Commissioner Chopra emphasized that the FTC's orders bind not only the affected corporate entity but also the company's officers. He suggested that, when appropriate, the FTC should seek dismissals of executives or board members that oversee conduct in violation of the agency's orders.
- **Dismissal of Third-Party Compliance Consultants.** Commissioner Chopra suggested that the failure of third-party consultants or auditors to detect conduct that violates an administrative order may suggest compromised independence and warrant dismissal of such auditors or consultants.
- **Clawbacks and Reforms to Executive Compensation.** Although Commissioner Chopra acknowledged that equity holders should incur costs when a company violates an order, he also suggested that those costs should be fairly allocated to include recovery of bonuses or compensation from executives who caused or oversaw the offending acts. Specifically, Commissioner Chopra suggested that executive compensation arrangements may need to be amended to reflect a company's commitment to compliance and enable the company to claw back bonuses and/or order forfeiture of unvested grants and options.

[4] Commissioner Chopra's comments are available here.

[5] *See* 16 C.F.R. § 1.98(c).

- **Requirements to Raise Capital.** The agency may consider requiring recapitalization of a company — even if recapitalization dilutes senior executives' stock holdings — in the event that a company's repeated misconduct primarily stems from the need to generate cash to service unmanageable debt.

### Key Takeaways

Although it is difficult to anticipate the penalties the FTC may seek going forward, Commissioner Chopra has made clear his priority to target repeat corporate offenders and incentivize companies, and their officers and directors, to comply with the law. Whether the FTC chooses to adopt his suggested approach remains to be seen, but his remarks could signal increased penalties for repeat offenders.

Return to Table of Contents

## Oracle and KPMG Publish Cloud Threat Report

**Oracle and KPMG released a joint report highlighting the concerns of more than 400 cybersecurity professionals regarding cloud technology issues. The report also detailed the unique challenges the cloud services industry presents in regards to cybersecurity.**

Oracle and KPMG recently published a 2018 Cloud Threat Report, which discusses the implications of the increasingly cloud-enabled workplace on cybersecurity priorities.[6] Enterprise Strategy Group (ESG) partnered with Oracle and KPMG to conduct a research study that forms the foundation of the report. ESG surveyed 450 cybersecurity and information technology (IT) professionals from private- and public-sector organizations in the United States, Canada, United Kingdom, Australia and Singapore between December 4, 2017, and January 10, 2018. The key takeaways of the report are summarized below.

### Cloud Initiatives Not Hampered by Cybersecurity Concerns

An increasing level of confidence in cloud security has accelerated the broad adoption of cloud services among organizations. The survey revealed that 83 percent of respondents believe that their cloud service providers' (CSPs) security is either as good as or better than their own. Many organizations are now so comfortable that they are increasingly storing a portion of their sensitive data assets (*e.g.*, personally identifiable information, payment card data, legal documents, source code and other types of intellectual property) in the cloud.

The report emphasizes that the cloud customer cannot take this growing confidence in CSPs for granted, as cloud security is a shared responsibility that the customer must always keep in mind. For example, the customer is generally responsible for data security, user access and identity management. Customers also should maintain formal policies and procedures, such as conducting a formal cybersecurity review of any CSP prior to engaging it as a service provider, and be mindful of the impact of the movement of data between a CSP's data centers on the customer's compliance with applicable law, such as the GDPR.

### Today's Cybersecurity Threats Are Diverse and Complex

The report reveals that companies are concerned about a diverse range of attacks. Ransomware is cited in the report as a "breakaway" threat over the last few years, with 62 percent of respondents indicating they were hit by a ransomware attack in the past 12 months. In addition to cybercriminals, survey respondents are concerned about the risks presented by malicious insiders who may be able to leverage their escalated privileges and familiarity with the corporate IT environment to steal data and potentially disrupt business operations.

According to the report, the most frequent type of attack is phishing. In addition to traditional phishing via email, companies also should be aware that attackers are now employing other phishing vectors, including "vishing" (the use of voicemail to solicit a return call where the recipient is coerced into sharing personal information) and "smishing" (the use of text messages to lure users into clicking a link that can lead to a phishing webpage).

### Cloud Services Create Unique Cybersecurity Challenges

Survey respondents cited threat detection and response in the cloud as their top cybersecurity challenge. Since cloud customers cannot access the physical network layer, there is a "visibility gap" in the use of CSPs that companies do not face when using infrastructure located on their premises.

[6] The full report is available here.

Failure to deter "shadow IT" is another unique challenge. Only 50 percent of companies surveyed indicated that all cloud services must be approved by their IT/cybersecurity team, while 82 percent of respondents were concerned that cloud-approval policies are being ignored within their organizations. Competitive pressures also may push business leaders within an organization to leverage cloud services without the involvement of in-house IT/cybersecurity teams, bypassing the organization's cybersecurity policies and processes and threatening security.

### Identity and User Access Management Challenges in a Mobile Cloud Environment

Mobile access to cloud storage is convenient because of its accessibility from any device and at any time and location, but it also can present unique security challenges. Survey respondents indicated that mobility access, as well as the need to manage multiple identity repositories, are their two most significant identity access management challenges. According to the report, identity must be the focus of a centralized cybersecurity strategy for the cloud-enabled workplace, and organizations are encouraged to consolidate multiple identity repositories.

### Emerging Technologies May Help

Emerging technologies, such as machine learning and security automation, may improve the efficacy of detecting and preventing threats, such as anticipating and identifying zero-day threats. According to the report, 29 percent of survey respondents are using machine learning on a limited basis, and an additional 27 percent of organizations are either currently deploying, plan to use or are interested in leveraging machine learning for these purposes.

### Key Takeaways

The report reveals that a cybersecurity approach that focuses on people and processes (*e.g.*, end-user awareness training) delivers the best results for maintaining a company's cybersecurity. Survey respondents most often cited employee training as having the most positive impact on cybersecurity in the last two years.

Cybersecurity and IT leaders must strike a balance between cybersecurity concerns and allowing business leaders to take advantage of cloud services in a way that accommodates their business needs. Business and IT/cybersecurity leaders within an organization should collaborate to achieve this balance, with the goal of having each side appreciate both the requirements that are driving the use of cloud applications and the cybersecurity policies, processes and controls that are essential to a secure cloud environment.

Return to Table of Contents

## DHS Unveils Departmental Cybersecurity Strategy

**The Department of Homeland Security (DHS) released a detailed five-year plan to address cybersecurity issues the agency may face. The strategic plan outlines several detailed steps to ensure the nation's economic and physical security in the face of threats both domestic and foreign.**

On May 15, 2018, the Department of Homeland Security released its five-year strategy for combatting cybersecurity threats.[7] The strategy, directed by the 2017 National Defense Authorization Act, calls for enhanced coordination within the department and the federal government at large to adequately prepare for, respond to and recover from cyberattacks by both nation-state and non-state actors.

DHS Secretary Kirstjen Nielsen emphasized the importance of treating malicious cyberattacks as a threat to the nation's security, stating "digital security is now converging with personal and physical security, and it is clear that our cyber adversaries can now threaten the very fabric of our republic itself."[8] The DHS strategy focuses not only on traditional critical infrastructure areas such as energy and financial services but also addresses the challenges posed by large numbers of internet-connected devices and the impact future cyberattacks may have on individual Americans. Secretary Nielsen stated the strategy focuses on "mitigating systemic risk and strengthening collective defense"

[7] A copy of the department's strategy is available here.

[8] *See* Press Release, U.S. Dep't of Homeland Security, Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts (May 15, 2018).

across the government and the private sector.[9] In its strategy, the department sets forth a five-pillar approach to enhancing the department's cybersecurity responsibilities: identifying risks, reducing vulnerabilities, reducing threats, mitigating consequences and enabling cybersecurity outcomes.

First, DHS will devote more attention to identifying modern cybersecurity risks to manage its risk management priorities. Second, DHS will address long-standing vulnerabilities within the federal government's information systems and the country's critical infrastructure to prepare those systems for malicious attacks. Third, DHS will enhance its enforcement capabilities and prioritize the prosecution of transnational criminal organizations and increasingly sophisticated cybercriminals. Fourth, the department will focus its efforts on coordinating an efficient, effective response to cyber incidents to minimize the damage caused by attacks. Fifth, DHS aims to strengthen the areas above in an integrated and prioritized way through international cooperation and recruiting a more talented federal cyber workforce.

Although the department's strategy addresses the need for federal government-wide changes, it also acknowledges DHS is limited in its reach. As a matter of law, DHS has limited authority over federal cybersecurity efforts.[10] Although DHS has overall responsibility for protecting the .gov domain and critical infrastructure, other elements of federal cybersecurity — both protecting federal assets and working with elements of the private sector and countering bad cyber actors — fall within the ambits of other departments and agencies, including the Defense, Justice, Treasury, State and Commerce departments, as well as elements of the intelligence community, such as the National Security Agency and CIA.

The DHS does recognize the need for cross-government coordination and cooperation in several ways. First, it notes that although individual agencies must implement their own risk-management programs, DHS plans to work with the Office of Management and Budget to coordinate these efforts to understand systemic risks and interdependencies among agency systems. Second, DHS plans to prioritize securing the nation's most critical systems in consultation with those responsible for securing military and intelligence networks. Finally, DHS' strategy will seek to ensure that the department will devote significant effort to improving its own cybersecurity practices and capabilities to serve as a first adopter and model for other federal agencies. This would include creatively approaching acquisition and procurement to ensure the department has access to technologies at the forefront of cyber protections.

In addition, the DHS strategy targets not only federal cybersecurity preparedness but also addresses the readiness of critical infrastructure companies across 16 sectors, including businesses related to chemicals, communications, the defense industrial base, emergency services, energy, financial services, food and agriculture, transportation, and water. The department sees the protection of these sectors as essential to ensuring national security and public health and safety as well as U.S. economic security. In this regard, the strategy — as DHS and others have previously done — encourages adoption of cybersecurity best practices, most notably recommending the National Institute of Standards and Technology cybersecurity framework.

Ironically, the DHS cybersecurity strategy announcement coincided with the elimination of the White House cybersecurity coordinator position on the National Security Council. The impact of the White House's decision remains to be seen, but it has been widely criticized given the broad scope of the national cybersecurity challenge and the lack of any single federal department or agency having responsibility or authority over U.S. cybersecurity.

Return to Table of Contents

[9] *See* Authorities and Resources Needed to Protect and Secure the United States, before the S. Comm. on Homeland Security & Governmental Affairs, 115th Cong. (2018) (statement by Kirstjen Nielsen, Secretary of the U.S. Department of Homeland Security).

[10] *See* Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3553(b) (2014).

## 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

**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