Skadden

European Data Protection and Cybersecurity in 2019

Contributing Partner

Ingrid Vandenborre / Brussels

Counsel

Eve-Christie Vermynck / London

Associate

Shannon Togawa Mercer / London

Data protection laws in Europe evolved substantially in 2018, with the implementation of the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive) becoming national law at the member state level. These legislative developments come on the heels of impactful international data breach and cybersecurity incidents. Together, they catalyzed calls for increased data protection and cybersecurity awareness through further proposed and enacted regulations. In 2019, the focus will transition from theory to practice, as implementation gives way to enforcement.

Far-Reaching Territoriality and Increased Data Protection Awareness

In November 2018, the European Data Protection Board (EDPB) disseminated guidelines, subject to public consultation, on the territorial scope of the GDPR, which brought long-awaited certainty to businesses outside the European Union.

First, the GDPR applies to controllers or processors with an establishment in the EU that process personal data in the context of the activities of that establishment, whether the processing happens in the EU or not (the establishment criterion). The EDPB clarifies that the applicability of GDPR to a non-EU data controller is a fact-based evaluation and not automatic. For instance, if a U.S.-based company makes one-off use of an EU-based processor, the processor can comply with its GDPR obligations without those obligations necessarily attaching to the U.S. company.

Second, the GDPR applies when a controller or processor not established in the EU processes personal data in connection with the offering of goods or services to data subjects in the EU, or monitors data subject behavior in the EU (the targeting criterion). The guidelines clarify that for the GDPR to apply to an establishment outside the EU, the establishment must demonstrate the intention of targeting a data subject in the EU and must target the subject on the basis of it being in the EU. This standard excludes de minimis processing and thus insulates a company from liability in the case of a non-EU data subject's incidental presence in the EU (*e.g.*, a U.S. mobile network company will not have to comply with GDPR solely because a U.S. data subject is using its roaming services while in the EU).

Despite further clarity on GDPR's reach, companies will need to consider what obligations they may have under the myriad new or revised national data protection laws outside the EU (*e.g.*, Brazil, India and California as well as Japan, which awaits an EU adequacy decision). Data protection awareness is a global trend to watch in the coming year.

Impact of GDPR on Corporate Transactions, Investigations and E-Discovery

Data protection legislation will, and in many cases already has, necessitated new steps in corporate transactions and litigation. Companies must now design and document more stringent methodologies and security measures in line with newly codified accountability and data minimization principles.

This article is from Skadden's *2019 Insights*.

Four Times Square
New York, NY 10036
212.735.3000

In transactional work, the due diligence and post-closing phases will inevitably include new dimensions to address the processing of personal data. Parties should pay special attention to data governance, privacy policies and notices, and cybersecurity standards. Corporate litigation processes should be mindful of the nature of data flows, prior information obligations to custodians, and the data minimization principle applicable to collection and review of personal data.

While steps toward GDPR compliance may seem onerous, investment at the outset will lead to more efficient internal workflows and procedures. Especially in markets with increasing appetites for data protection, companies are likely to continue streamlining data protection operations and policies and may view the GDPR as a standard-setting regulation for data protection globally in 2019.

Security and Cyberrisk

The NIS Directive, which aims to protect critical national infrastructure, is a cornerstone of EU cybersecurity. EU member states were required to transpose it into national law on May 9, 2018, and identify operators of essential services by November 9, 2018.

The NIS Directive legislates the improvement of cybersecurity infrastructures at the state and company levels, through "safeguarding obligations" (appropriate safety measures) and "information obligations" (community sharing and notification obligations). It also requires EU member states to implement structural changes, including the designation of a competent national NIS authority. The directive aims to create a culture of security through transparency and accountability.

Another step toward a more robust cybersecurity infrastructure is the European Central Bank's cyber resilience oversight expectations (CROE), published on December 3, 2018, as part of larger efforts to enhance cyber awareness and resiliency throughout the financial sector. The CROE provides specific instructions and clear expectations through a new framework for compliance.

In October 2018, the European Council called for the reform and improvement of EU cybersecurity policy. In December 2018, EU ambassadors approved a proposed Cybersecurity Act that would enable the creation of a permanent EU Agency for Cybersecurity and an EU-wide cybersecurity certification scheme. Developments in 2019 will further illustrate that cybersecurity and data protection go hand in hand, especially in sectors such as health care and transportation.

GDPR and Competition Law

Competition agencies are focusing increasingly on the value and use of personal data as a commodity with competitive significance, blurring the boundaries between competition and data protection laws. In 2016, the German Federal Cartel Office (FCO) began an investigation into Facebook for its alleged abuse of dominance in its collection of user data through third-party apps and websites. The FCO's preliminary assessment is that Facebook is abusing this dominant position by requiring users of its social network to allow it to limitlessly amass every kind of data generated by those users' third-party websites and then merging it with the user's Facebook account, not only from services owned by Facebook such as WhatsApp or Instagram, but also from websites and apps of other operators with embedded Facebook application program interfaces. According to the FCO, Facebook's terms of service violate data protection provisions to the disadvantage of its users, which in turn is deemed to constitute an abuse of the company's allegedly dominant position based on the Facebook network.

In the U.S., the Federal Trade Commission (FTC) is similarly focused on data issues. The FTC held a two-day hearing on the "intersection of Big Data, Privacy and Competition" in November 2018. At issue for U.S. authorities is whether existing antitrust and consumer protection rules are fit to address new challenges relating to big data and privacy as well as data collection and advertising practices by two-sided platforms.

Greater clarity on how competition issues involving the use of data are perceived by the European Commission and authorities of the EU member states as well as in the U.S. is expected in 2019.

GDPR Enforcement

While administrative fines under the GDPR (up to 4 percent of total worldwide annual turnover) were one of 2018's hot topics, the regulation also introduces another source of potential liability: It grants any individual the right to compensation for damage caused by a data controller or processor's breach of the GDPR requirements. Individuals who bring claims for data breaches have the option of assigning their claims to a not-for-profit, public interest group established to protect individual privacy rights. In addition, individual EU member states may legislate to provide a mechanism for individuals to litigate via collective action complaints or class actions. Exposed to both administrative and civil liability for data breaches, the financial risk for companies could be very high.

Within a short period after GDPR implementation in May 2018, enforcement became a reality: France's Commission Nationale de l'Informatique et des Libertés has multiple pending investigations and has mandated remediation actions, and the U.K.'s Information Commissioner's Office has issued warnings and small fines. Meanwhile, the Portuguese Comissão Nacional de Protecção de Dados has imposed the first GDPR fine — €400,000 — on a hospital for noncompliance with GDPR.

Enforcement actions in 2019 will reveal the contours of data protection legislation.

Click here for a full list of cybersecurity and privacy-related articles authored by Skadden attorneys in the last year.