CARTER/LEDYARD

our resources

An Update on the EU's General Data Protection Regulation (GDPR)— Six Months Later

December 05, 2018

Client Advisory
December 5, 2018 by Matthew D. Dunn

Six months have now passed since the European Union's (EU) General Data Protection Regulation (GDPR) became effective on May 25, 2018.[1] Companies throughout the world continue to wrestle with compliance with the regime's data-protection and privacy framework (summarized in our April 2018 Advisory), and many companies remain unprepared. In addition, member states' data protection authorities continue to adjust to the increasing demands and enforcement-related responsibilities of this broad regulation with a global reach.

While there have been relatively few enforcement actions in the first few months, several important observations can be made. EU authorities will pursue enforcement against companies, even small companies outside the EU, where circumstances require it. There has been a significant increase in complaints by data subjects, and many investigations are ongoing. In addition, there has been a significant increase in the reporting of data breaches by companies of all sizes. Finally, there appears to be a significantly increased risk of consumer protection and securities fraud litigation that is tied to GDPR violations or weaknesses. 2019 is likely to be a big year for data privacy enforcement, and companies should continue to prioritize GDPR compliance.

Global Reach and Severe Penalties

As set forth in our April 2018 Advisory, the GDPR applies to every business in the world that uses, possesses, or otherwise processes personal data of EU persons (data subjects), and provides data subjects with rights enforceable against any business or organization that stores or otherwise processes their personal data. The Regulation requires companies in possession of data, under certain circumstances, to obtain consent of the data subjects, provide various disclosures to data subjects relating to the use of their data, and report data breaches to the authorities and the data subjects.

What caused the most attention, however, were the severe penalties and strong enforcement mechanisms available under the GDPR. Enforcement not only can involve temporary or permanent bans on the processing and use of EU personal data, but also can involve financial penalties of up to the higher of EUR 20 million or 4% of annual worldwide gross revenues. For large global companies, this could translate into fines in the billions of dollars. Ultimately, however, each member state is responsible for monitoring and enforcing the regulation through its data protection authority, and thus enforcement approaches are likely to vary.

Failure to Obtain "Consent" of Data Subjects

On May 25, 2018, the first day of GDPR enforcement, privacy crusader Max Shrems, through his non-profit entity None of Your Business (NOYB) and on behalf of data subjects, filed complaints with the data protection authorities in France, Belgium, Germany, and Austria against Google (Android), Facebook, Instagram, and WhatsApp, primarily claiming that the companies' practices of asking users to check a box to consent to

privacy policies relating to their personal data in order to access services violate the GDPR requirement that consent be particularized and freely given (see GDPR Article 7). While the GDPR allows data subjects to file private court actions against companies for damages, these complaints were directed to the data protection authorities and requested that the authorities investigate the allegations, prohibit all processing operations based on invalid consent, and fine the companies up to the maximum fines permitted. The complaints seek maximum fines under the GDPR—against Google of EUR 3.7 billion (approximately $4.2 billion) and Facebook (which operates Instagram and WhatsApp) of EUR 3.9 billion (approximately $4.4 billion).

Lack of Transparency and Notice to Data Subjects

The first GDPR enforcement notice was issued in July 2018 by the United Kingdom's data protection authority, the Information Commissioner's Office ("ICO"), against Canada-based data analytics company AggregateIQ (AIQ). According to reports, AIQ was a subcontractor to Cambridge Analytica and was involved in using data in connection with the Brexit leave campaign in the UK which resulted in the 2016 vote to leave the EU. It seems that the ICO had been investigating AIQ well before the GDPR went into effect in May 2018, and thus the GDPR conveniently provided UK authorities new legal authority to reach this Canada-based company of only 20 employees.

The enforcement notice indicates that AIQ was processing (even if merely storing at that point) personal data (that had been used in the past) without disclosing to data subjects the uses being made of the data and without a lawful basis for processing the data. The penalty was limited to an order that AIQ "cease processing any personal data of UK or EU citizens obtained from UK political organizations or otherwise for the purposes of data analytics, political campaigning, or any other advertising purposes," but severe financial penalties would be assessed for failure to comply with the cease order. AIQ has appealed the notice.

Given that the UK is scheduled to leave the EU on March 29, 2019, it is not yet clear whether the UK will continue to enforce the GDPR or some similar regulatory framework and how that will affect the appeal. The main takeaways from this action are that (a) EU authorities will not hesitate to enforce the GDPR against non-EU entities, including small entities, especially those companies in the data analytics, data mining, and big data industries, and (b) data protection authorities may utilize cease orders in lieu of imposing severe financial penalties.

The Irish Data Protection Commissioner recently published a report, indicating that in the first part of 2018 (before the GDPR became effective) it concluded an audit of LinkedIn in response to a consumer complaint, and determined that LinkedIn had obtained email addresses for 18 million non-user data subjects for use in targeting advertisements on Facebook without transparency to the data subjects. The complaint was settled, with LinkedIn being required to implement corrective action and cease the non-transparent processing. No fine was imposed—in part, perhaps, because the GDPR had not yet become effective.

Most recently, in late November, EU consumer protection agencies filed GDPR complaints against Google for its allegedly deceptive practices in tracking user locations on Google smartphones. The complaints came after a report by Norway's Consumer Council and a class action lawsuit filed in the U.S. District Court for the Northern District of California relating to the same practices. The complaints, filed with data protection authorities in the Netherlands, Poland, the Czech Republic, Greece, Norway, Slovenia, and Sweden, assert that Google violates the GDPR by tricking users into activating location tracking features, that Google lacks a valid legal ground under the GDPR for processing the location data, and that any user consent is not freely given. Google could face fines in the billions.

Lack of Security Safeguards

In October, it was reported that Portugal's Supervisory Authority had imposed the first GDPR-related fine of EUR 400,000 (approximately $455,000) in July on a Portuguese public hospital for its failure to have in place technical and organizational safeguards to protect patient data as required by the GDPR. An investigation revealed that hospital staff members had unrestricted access to all patient files (even when such

access was not necessary) and thus violated the GDPR (see Articles 5 and 32) for failing to ensure appropriate security of personal data, notwithstanding that the IT system was provided by the Portuguese Health Ministry. The hospital is contesting the fine.

In October, Austria's data protection authority issued its first GDPR-related fine against the owner of a retail establishment for the use of a surveillance camera in front of its location which allegedly was capturing video of a sidewalk area beyond the immediate storefront without proper notice of the surveillance. The GDPR requires that personal data collected or processed be limited to what is necessary and that data subjects be provided notice of the collection and processing. The company was fined the relatively modest amount of EUR 4,800 (approximately $5,500), consistent with its size and revenues.

Data Breach

The GDPR (Article 33) requires that data breach incidents (where personal data has been lost, stolen, or otherwise accessed by unauthorized third parties) be reported to the applicable member state's data protection authority within 72 hours after the data controller becomes aware of the data breach, unless deemed "unlikely to result in a risk to the rights and freedoms of natural persons." And, under Article 34, if there is a "high risk" of the breach adversely affecting individual "rights and freedoms" such incidents must be reported to the data subjects "without undue delay"—which may be even sooner than 72 hours after the data controller learns of the breach.

EU authorities have confirmed a significant increase in the reporting of data breaches since the GRPR went into effect. In many cases, out of an abundance of caution, breaches have been reported that do not meet the threshold for reporting under the GDPR. However, there have also been significant breaches that were reported, such as Facebook's July report to Irish authorities of a massive breach potentially affecting 50 million users and British Airway's September report of a hack affecting the payment card details of 380,000 customers.

In just the last few days Marriott reported a massive data breach of its Starwood brand database which it discovered had been ongoing since 2014 and involved exposure of personal data, including passport details and in some cases payment card information, for 500 million people. Class actions have already been filed in the U.S., and there has been speculation that this could lead to a significant fine under the GDPR.

In November, Uber was fined by the Dutch and UK data protection authorities for its 2016 data breach affecting 57 million customers' names, email addresses and phone numbers. Reports indicate that Uber failed to disclose the massive data breach and tried to quietly pay off the hackers. This led to a multi-state investigation in the U.S. which was settled in September, with Uber agreeing to pay $148 million to all 50 states and the District of Columbia. The subsequent fines in the EU, fortunately for Uber, were issued under the pre-GDPR privacy regimes—with the Dutch and EU authorities fining Uber a total of just over $1 million.

Also in November, Germany's Baden-Württemberg Data Protection Authority issued a fine of EUR 20,000 (approximately $22,700) to German social media and dating service Knuddels.de in connection with a data breach. Knuddels was the subject of a cyber hack in the summer months which exposed over 800,000 email addresses and 1.8 million user names, with the perpetrators then publishing the personal information on the web. The investigation revealed that the Knuddels website stored personal data in plain text with no safeguards. Accordingly, the German regulator determined that the company violated Article 32 of the GDPR by failing to ensure data security in the processing of personal data. The German Data Protection Authority indicated that the company would have received a more severe fine if not for its cooperation and transparency during the investigation and the corrective security measures that the company implemented since the incident. The company was credited for self-reporting the breach to its users and to the authorities as required by the GDPR. This German case demonstrates the importance of cooperation, remediation, and compliance with the reporting requirements of the GDPR.

U.S. Litigation

GDPR-related suits have also surfaced in U.S. courts. In August 2018, a putative class action was filed in the federal District Court for the Southern District of New York against Nielsen Holdings alleging violations of U.S. securities fraud laws for allegedly misrepresenting its preparedness for the GDPR and downplaying the effects that the GDPR would have on its business model. This is not a claim for violations of the GDPR. Instead, the general theory is that Nielsen, a publicly traded consumer analytics firm which relies on data from big data firms and other analytics providers, publicly reported that the GDPR would not negatively affect its business, but it then failed to meet revenue expectations (and its stock price fell) after the GDPR went into effect as a result of data providers restricting access to consumer data in order to comply with the GDPR.

Looking Ahead

It is likely that there will be more enforcement actions before the end of 2018, and certainly in 2019 after many ongoing investigations are concluded and as new complaints and breaches are reported. Many countries may begin to proactively conduct audits of GDPR compliance, with Germany and France specifically indicating an intention to do so. There is also speculation that enforcement actions and breach reporting will lead to GDPR-related class actions by consumers seeking damages for economic and noneconomic loss (such as emotional distress or reputational damage).

Privacy compliance will continue to be a global issue, as other non-EU countries have enacted or proposed privacy regimes similar to the GDPR. In June, the State of California passed an expansive consumer privacy law, the California Consumer Privacy Act of 2018 (CCPA),[2] which, although not as broad as the GDPR, similarly gives California residents basic rights relating to their personal information and applies to companies (even those outside of California) that collect personal data of California residents. The CCPA is due to go into effect on January 1, 2020. There have also been some significant discussions amongst lawmakers regarding a U.S. federal privacy framework, and that momentum may continue into 2019.

Organizations are encouraged to consult legal counsel to assist in assessing whether they are subject to the GDPR or other privacy laws, interpreting the various provisions, and creating or adapting a privacy plan to ensure compliance.

For more information concerning the matters discussed in this publication, please contact the author Matthew Dunn (212-238-8706, mdunn@clm.com), another member of Carter Ledyard's Cybersecurity practice group, or your regular Carter Ledyard attorney.

---

[1] The text of the full regulation is available at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

[2] CAL. CIV. CODE § 1798.100 *et seq*.

---

related professionals

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com