SAUL EWING ARNSTEIN & LEHR LLP

Alert

CYBERSECURITY AND PRIVACY PRACTICE

MAY 2019

**AUTHORS**

ALEXANDER R. BILUS

PATRICK M. HROMISIN

# GDPR Year One: Hot Spots for Enforcement Activity

## SUMMARY

**What can organizations learn from the first year of enforcement of the European Union's General Data Protection Regulation (GDPR)? Quite a bit, if you pay attention to what the EU government regulators are doing.**

Over the course of the GDPR's first year, numerous enforcement proceedings have taken place throughout Europe. These actions have been leveled at companies ranging from a Danish taxi company to a Portuguese hospital to the multinational tech giant Google. The penalties dished out by regulators have ranged from orders to stop or limit data processing, to nominal fines, to a fine of €50 million.

These enforcement proceedings show how regulators are prioritizing the myriad new obligations that the GDPR imposes on controllers and processors of personal data. As organizations continue working to understand and comply with GDPR provisions that are sometimes broad and ambiguous, these proceedings provide some helpful concrete examples of how the rubber has met the road. The following are some key aspects of the GDPR that have served as the basis for enforcement actions.

<u>EU Regulators Are Focusing on These Areas of Concern</u>

***Validity of Consent***

Several organizations have run into enforcement problems in connection with the GDPR's consent provisions. The GDPR requires organizations to obtain consent from individuals for a number of processing operations, including the processing of sensitive personal data (such as biometric data) or certain cross-border data transfers. Organizations also choose to use consent as their "lawful basis" for a wide variety of other data processing purposes. But consent must be "freely given, specific, informed, and unambiguous," and must be manifested by "a clear affirmative action." And it must be as easy for an individual to withdraw consent as it is to give it.

In January of 2019, CNIL (the French data protection authority) fined Google €50 million, the largest fine issued under the GDPR to date, on the basis that Google was not adequately getting its Android phone users' consent relating to personalized ads and speech recognition. CNIL found that the consent wasn't valid for two reasons. First, Android users were not adequately informed because Google spread information about its processing across multiple documents relating to multiple software platforms, meaning a user would have to navigate through each document prior to giving consent in order to understand the scope of the consent. Second, Google used a pre-checked "I agree" box on its consent form, which did not satisfy the GDPR's requirement of a clear affirmative "opt-in" action by a user. CNIL also issued an enforcement order against a smaller company called Vectuary in November of 2018, finding that it had also failed to obtain valid consent for location data used in targeted advertisements.

Similarly, in May of 2019, the United Kingdom Information Commissioner's Office ("ICO") issued a finding that Her Majesty's Revenue and Customs ("HMRC"), the U.K. analogue to the IRS, had violated the GDPR because it didn't obtain valid consent from users for voice identification it offered on its telephone help line. The ICO determined that consent was required because the voice data counts as "biometric data." And it further found that the users' consent was not valid because HMRC didn't give them sufficient information about how their biometric data would be processed, or give them an opportunity to withdraw their consent.

***Security of Personal Data***

Other enforcement actions have concentrated on data security. The GPDR requires organizations to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" and process personal data "in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing."

In December of 2018, the Portuguese data protection authority, CNPD, fined a hospital €400,000 because the hospital hadn't done enough to ensure the security of the personal data it was processing. The CNPD found that the hospital had over 900 users in its system with the access privileges granted to doctors, but only 296 doctors practiced at the hospital during the relevant period. The CNPD also found that doctors could access patient data too freely, and that the hospital hadn't adequately documented procedures for ensuring the security of patient data. Notably, the CNPD initiated its investigation based on a media report, exemplifying the numerous ways that data privacy issues can come to regulators' attention.

A German regional data protection authority issued a €20,000 fine against a social media platform called Knuddels in November of 2018, after the platform suffered a breach that exposed the personal data of over 300,000 users. One of the factors leading to the breach was Knuddles' storage of user passwords in clear text. According to the regulator, the fine was relatively small because after the breach Knuddles cooperated with the government and implemented stronger security measures.

In April of 2019, the Italian data protection authority, Garante, similarly issued a €50,000 fine against a company that administered websites related to the political party known as the Five Star Movement. Garante found that the company employed insufficient security practices, including obsolete security systems that could not be patched, inadequate encryption of user passwords, and improper sharing of users' credentials. And in the same month, the Norwegian data protection authority, Datatilsynet, issued a €170,000 fine to the municipal government of Bergen, finding that it had not adopted strong enough security measures to safeguard the personal data it was processing.

***Notices to Individuals***

Another regulator has addressed an organization's failure to provide adequate notice to individuals about the processing of their personal data. The GDPR requires that controllers of personal data provide a plethora of information to individuals about their processing of that data, including the purpose of the processing, the lawful basis for the processing, how long the data will be stored, and a recitation of the individuals' rights under the GDPR.

In March of 2019, the Polish Data Protection Authority, PUODO, fined a company €220,000 for not providing privacy notices to individuals whose data it was processing. The company is a provider of business verification services that relies heavily on public records, and in the course of its business, it acquired personal data concerning at least 6.5 million individuals. Under the GDPR, a controller is required to provide privacy notices even when it doesn't collect data directly from individuals, and in this case, the company only provided notices to the roughly 500,000 individuals for whom it had email addresses. The company argued that the cost of providing notices by mail would nearly equal its annual revenue, but PUODO nevertheless determined that it was required to provide notices to all individuals whose data it was processing.

***Data Retention***

Finally, one regulator has issued a fine in connection with improper retention of personal data. The GDPR requires controllers of personal data to abide by the principle of "storage limitation," which means that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

In March of 2019, the Danish data protection authority levied a fine of 1.2 million Kroner (roughly $180,000) on a taxi company in part because it improperly retained personal data. The company's own data retention policy stated that it needed to retain data collected during a taxi ride for two years. But after two years, the company only deleted the name associated with the ride and kept all other data relating to the ride, including date, GPS coordinates, and payment information. Further, the company associated the ride data with the customer's phone number in its records for an additional three years.

## Looking Ahead

While much can be learned from the enforcement actions that have happened to date, more is yet to come: we know that regulators are still in the process of ramping up their enforcement activities. For example, the Irish Data Protection Commissioner has stated that her office's first enforcement decisions will be issued in the summer of 2019. CNIL issued forty-nine orders concerning personal data protection shortfalls by the end of 2018, with only ten instances of monetary penalties. The ICO has imposed no monetary penalties under the GDPR thus far, though it has issued notices of violation in some cases, and it has reported receiving over 19,000 complaints from the public since the GDPR became effective. Each data protection authority is likely to conduct more investigations and issue more penalties over the coming years.

Enforcement actions in year one of the GDPR have emphasized the importance of complying with broad principles such as consent and security, but also with detailed provisions such as privacy notice requirements. As authorities, individuals, and companies continue to reckon with the obligations imposed by the GDPR and the enforcement authority it provides, there will surely be no shortage of notable enforcement actions in the upcoming year. For more information, please contact the authors of this Alert.

This Alert was written by Alexander R. Bilus, Vice Chair of the Firm's Cybersecurity and Privacy Practice, and Patrick M. Hromisin, Associate in the Firm's Cybersecurity and Privacy Practice. Alexander can be reached at 215-972-7177 or alexander.bilus@saul.com. Patrick can be reached at 215-972-8396 or patrick.hromisin@saul.com. This publication has been prepared for information purposes only.