# Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

## A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny

May 30, 2019

A year ago, on May 25, 2018, the European Union's General Data Protection Regulation (**GDPR**) came into force. With its extraterritorial scope and detailed requirements, the GDPR aimed to change the approach to personal data around the world. We have closely monitored GDPR-related investigations and enforcements actions, as well as guidance published by regulatory authorities across the European Union (**EU**). During the GDPR's first year, based on our monitoring, it appears that several trends have emerged with regard to enforcement and regulation. Below, we discuss these trends and outline five key recommendations for ongoing compliance with the GDPR.

Regulatory Developments Over the Past Year

On May 22, 2019, the European Data Protection Board (**EDPB**)—a European body made up of the heads of the national data protection authorities (**DPAs**) and the European Data Protection Supervisor that promotes the consistent application of data protection rules throughout the EU—published the results of its latest survey in relation to the GDPR (**EDPB Survey**). The EDPB Survey found that most DPAs across the EU are reporting an increase in queries and complaints received compared to 2017 and that, since the GDPR came into force, over 144,000 queries and complaints and over 89,000 data breaches have been logged. Not every query, complaint and data breach will be subject to investigation, and it is uncertain how many investigations there are under way as not every DPA publishes figures; however, in light of these numbers, it is likely that scrutiny by the DPAs will increase.

Our monitoring has shown that certain DPAs appear to have been more active than others, such as the UK's Information Commissioner's Office (**ICO**), the Irish Data Protection Commission and the German DPAs (of which there are 16). Importantly, the DPAs are not solely focusing on big-ticket cases. Organizations of varying sizes in a broad array of industries have been subject to investigations, even including those in the charitable sector. Enforcement actions have taken place against health care entities and governmental departments, political campaigning organizations and funeral homes, taxi companies and retailers alike. Further details appear in the Developing Trends section below.


**Contact Information**

**If you have any questions concerning this alert, please contact:**

**Natasha Kohne**
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

**Michelle A. Reed**
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

**Davina Garrod**
Partner
davina.garrod@akingump.com
London
+44 20.7661.5480

**Ezra Zahabi**
Partner
ezra.zahabi@akingump.com
London
+44 20.7661.5367

**Jenny Arlington**
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

**Diana Schaffner**
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

In addition to investigations and enforcement actions, the DPAs have been active in publishing guidance on the GDPR. The guidance issued since May 2018 covers a range of topics beyond general GDPR implementation, such as regulatory frameworks for social media, human resources management and whistleblowing, standards for biometric testing in the workplace and guidance on cookie walls. Overall, we have seen country-specific guidance that has been published by the DPAs in over 20 countries across the EU. Additionally, the EDPB has published recent guidance on a range of topics, including on the territorial scope of the GDPR, the data implications of a No-Deal Brexit and legitimate processing methods.

Developing Trends

We have seen several trends develop while tracking GDPR investigations and enforcement actions across the EU, each discussed below.

A. DPAs and other authorities continue to monitor whether businesses are transparent about their processing activities and data subjects are paying closer attention to the issue.

In the past year, there have been several complaints, investigations and enforcement actions related to transparency under the GDPR. In particular, companies have faced scrutiny for not providing data subjects with required information where personal data is collected from the data subject.

For example, France's DPA, the Commission nationale de l'informatique et des libertés (**CNIL**), fined Google €50 million (approx. $57 million) for "lack of transparency, inadequate information and lack of valid consent regarding ads personalisation" (see our previous client alert). In addition, the UK's ICO issued its first enforcement notice under the GDPR to the Canadian data analytics firm, AggregateIQ Data Services (**AIQ**), for processing personal data without a lawful basis and failing to provide transparency information to the individuals to whom the data referred. Though not established in the EU, AIQ was within the remit of the GDPR because its processing activities involved monitoring data subjects' behavior in the EU as it was processing personal data of UK individuals on behalf of UK political organizations. The ICO ordered that AIQ erase any personal data that it retained on its servers within 30 days, indicating that a fine amounting up to €20 million or 4 percent of its annual turnover (whichever is higher) could be levied if AIQ failed to do so.

Recently, the Polish Personal Data Protection Office fined a company that aggregates personal and other data from publicly available sources 1 million Polish Zloty (approx. $260,000) for failing to provide information on its processing activities to data subjects.

Competition authorities are also increasingly investigating alleged anticompetitive behavior involving data. For example, in February 2019 the German Bundeskartellamt made an order against Facebook in relation to its use of data and in December 2018 the Italian competition authority issued a fine against the company in the context of personal data use. Furthermore, the UK Government's Report into Unlocking Digital Competition published radical recommendations in order to protect users of digital platforms, including creating a Digital Markets Unit which would promote data openness and mobility (underscoring the right to portability in the GDPR), monitor machine-learning algorithms to help prevent personalized discriminatory pricing and work with the ICO, CMA and OFCOM to intensify enforcement against data-related infringements.

## Contact Information

**If you have any questions concerning this alert, please contact:**

**Rachel Kurzweil**
Associate
rkurzweil@akingump.com
Washington, D.C.
+1 415.765.9507

**Sahar Abas**
Trainee Solicitor
sahar.abas@akingump.com
London
+44 20.7012.9859

© 2019 Akin Gump Strauss Hauer & Feld LLP

B. In circumstances where it is appropriate to rely on consent as a lawful basis, DPAs continue to consider carefully whether valid user consent has been obtained.

Under the GDPR, both the circumstances in which it is appropriate to seek consent from data subjects for processing their data and the way in which such consent may be obtained were revamped.

Where consent would be an appropriate lawful basis for processing data (which is not always the case), the DPAs have focused on whether the conditions for obtaining valid consent under the GDPR have been met. Even central government authorities have been penalized for non-compliance. In May 2019, the UK tax authority HM Revenue and Customs was issued with an enforcement notice ordering it to delete data it continued to hold without valid consent after its voice authentication service failed to inform callers properly as to the use of their data. Although this enforcement notice was issued under the pre-GDPR regime, the notice added that the action was taken in relation to contravention of data protection principles set out in the GDPR and the ICO's investigation was carried out under the GDPR.

Further, in November 2018, the CNIL issued a warning notice to the mobile ad network Vectuary for failing to obtain properly the consent of more than 67 million people and ordered that the company change its consent practices and erase all data collected on the basis of its invalid consent.

C. DPAs and other authorities have fined businesses for not meeting GDPR security standards.

We have seen several enforcement actions and investigations under the GDPR on the basis of a lack of adequate security measures. In July 2018, the Portuguese DPA issued its first fine under the GDPR of €400,000 (approx. $446,000) against a hospital authority on the basis of inadequate technical and organizational measures to prevent unlawful access to personal data. In May 2019, it was the lack of adequate security measures that resulted in the Italian DPA (**Garante**) issuing its first fine under the GDPR of €50,000 (approx. $55,000) against the Rousseau Association, an online platform operating several websites affiliated with an Italian political party. The Garante noted that though Rousseau had updated its privacy information notice, it failed to adopt several security measures, including having a system in place to strengthen passwords used for creating accounts, properly storing log files regarding activities performed by IT support personnel and measures aimed at anonymizing activities.

In particular, cybersecurity is now broadly seen as integral to financial institutions' regulatory compliance. The emergence of cybersecurity as one of the key focus areas for financial regulators means that data protection is inexorably connected to compliance with the financial regulatory framework. In the UK, the Financial Conduct Authority (**FCA**) and the ICO have signed a Memorandum of Understanding with a view to actively share information about potential and ongoing investigations with a data protection dimension. In 2018, the FCA and the ICO carried out a joint investigation into Equifax[1] for data protection breaches and, separately, the FCA fined Tesco Personal Finance plc over £16 million (approx. $20 million) for systems and controls-related failings following a cyber-attack that the FCA considered "largely avoidable".

© 2019 Akin Gump Strauss Hauer & Feld LLP

D. Certain DPAs continue to consider company cooperation as a mitigating factor when evaluating fines.

We have seen several DPAs encourage cooperation with investigations and particularly with data breaches, which has at times resulted in reducing the amount of fines levied. For example, in November 2018 the German State Commission for Data Protection and Freedom of Information Baden-Wuerttemberg (**LfDI**) issued its first fine under the GDPR, in the amount of €20,000 (approx. $22,300), against Knuddels.de for violations of data security obligations after a hack of more than 300,000 email addresses and passwords. The LfDI stated that the company had benefitted significantly from immediately informing the authority as well as its customers about the hack. The company's "exemplary cooperation" and significant improvement to its IT security in the aftermath of the investigation resulted in a relatively low fine, in light of the maximum potential fine which could have been applied to Knuddels.de under the GDPR (either €10 million or up to 2 percent of worldwide annual turnover). In contrast, in a relatively minor misdemeanor, the Hamburg Commissioner for Data Protection and Freedom of Information issued a fine (rather than simply a warning, for example) against a small shipping company, Kolibri Image, for violating the provision of the GDPR which requires that third parties processing data must use an additional data protection contract to detail the security measures taken by that third party. It was noted that steps had deliberately not been taken to rectify the procedures once the company had been made aware of its duties under the GDPR, as it reportedly tried to shift the responsibility at the feet of another contractor.

E. Some DPAs are halting processing activities in addition to fines.

The risk of fines and reputational damage in the case of noncompliance has been accompanied by the possible temporary or indefinite suspension of processing while an investigation is underway. For example, the Maltese DPA imposed a temporary sanction on the Malta Land Authority while it investigated a data processing breach. The Dutch DPA similarly sanctioned the Dutch tax authority and has indefinitely prohibited the processing of national identification numbers for value-added tax purposes.

F. Common GDPR-related complaints are related to telemarketing, promotional emails and video surveillance.

Finally, we have observed that one of the most common bases for GDPR-related complaints has been with respect to telemarketing, promotional emails and video surveillance. For example, the first fine issued by the Austrian DPA was on a small establishment with a surveillance camera that also recorded individuals who passed on the public sidewalk. Reports have shown that as of February 2019, almost 100 fines have been handed down to contravening parties across the EU, with many investigations still underway. In the 12 months since the GDPR has been in force, the number of spam emails have generally been reduced.

Five Recommendations to Help Limit Regulatory Scrutiny

In light of the trends displayed over the past 12 months, there are actions that can be taken to further develop a business's GDPR compliance program and mitigate the risks of noncompliance.

© 2019 Akin Gump Strauss Hauer & Feld LLP

First, remember that the GDPR is a journey, not a destination, and ongoing compliance is required. In particular, keep abreast of recent developments, enforcement actions, investigations and guidance. Decisions issued by the DPAs, such as the fine against Google (if it remains in force, as it is currently under appeal), will be informative as the GDPR has garnered momentum.

Second, do not assume that the GDPR applies to the "big fish" only. In March 2019, according to a survey commissioned by the UK's Institute of Directors, 39 percent of small and medium-sized enterprises (**SMEs**) did not know who the GDPR affected. In addition, a further 10 percent of SMEs did not think that consumers had any new rights following the introduction of the GDPR. As shown above, however, a large variety of industries and business sizes have been subject to investigation.

Third, implement education and training programs for employees on a regular basis. Many of the recent enforcement actions, as discussed above, have resulted in less onerous penalties for businesses that had proper compliance procedures in place. Consider business-wide training but also targeted training for employees who handle personal data, such as HR, IT, sales and marketing personnel.

Fourth, make sure your incident-reporting and breach notifications programs continues to be adequate. Adopting proper security measures and ensuring that internal controls are at satisfactory levels will help minimize the risk of a breach. With cybercrime on the rise, focus should be placed on what procedures the business has adopted in order to comply with its obligations if and when a breach takes place.

Fifth, take legal advice. In December 2018, 50 percent of regulated organizations were not compliant with the GDPR, according to the International Association of Privacy Professionals. However, with the deadline of complying with the California Consumer Privacy Act (**CCPA**) looming, businesses would be well advised to consider how to leverage compliance programs they have already carried out (and carry them out, if they have not yet done so) under the GDPR in order to achieve compliance with the CCPA.

## Conclusion

A year in, and it appears European regulators are only beginning to exercise their new enforcement powers and there is no sign European regulators plan to slow down anytime soon. All eyes are on privacy issues, as the Unites States Congress considers federal legislation that could incorporate aspects of the GDPR, and as the CCPA, modelled in part on the GDPR, races toward its January 1, 2020, enforcement date. We are continuing to monitor these and other developments in the EU. We are also continuing to track developments in the United States as they relate to the CCPA and potential federal privacy legislation.

1 As the breach occurred under the pre-GDPR framework the fine was limited to the pre-GDPR maximum of £500,000. Were it to occur under the current sanctions framework, it would likely be significantly higher.

akingump.com

© 2019 Akin Gump Strauss Hauer & Feld LLP