Expert Analysis

How The GDPR Changed Data Privacy In 2018

By **Jessica Lee**
December 14, 2018, 2:47 PM EST


Jessica Lee

The European Union General Data Protection Regulation became enforceable on May 25, 2018, bringing in a flurry of privacy notice updates, the shutdown of certain EU-facing websites and advertising activities, and a good amount of heartburn for companies within its territorial scope.

The threat of fines of up to 4 percent of a company's global revenue put a new spotlight on privacy and data protection, and caused a level of panic that was reminiscent of Y2K. Unlike Y2K, however, the road to GDPR compliance will extend well beyond its enforcement date.

What's Happened Since May?

In the past six months, compliance with the GDPR has moved from concept to reality, and both private citizens and data protection authorities, or DPAs, have taken action to enforce its requirements. Data subjects (individuals located in Europe) have started to enforce their rights, and DPAs have reported an increase in individual complaints.

Outside Europe, other countries have started to pass laws that mirror the GDPR's requirements, suggesting that at least some elements of the law may be our new global standard for privacy.

Enforcement Activity

As expected, tech companies have been among the first targets of GDPR enforcement activity. NOYB, a European consumer rights organization founded by Max Schrems, filed four lawsuits[1] against major tech companies the day GDPR went into effect, challenging the companies' consent mechanisms, and arguing that asking users to accept a company's privacy policies in order to access services violates the requirement that consent be "freely given."

In September, Dr. Johnny Ryan, chief policy and industry relations officer of Brave, a web browser that blocks ads and website trackers, filed a complaint[2] with several DPAs, asking them to investigate certain ad tech companies for "data breaches" caused by behavioral advertising. According to the press release, "every time a person visits a website and is shown a 'behavioural' ad on a website, intimate personal data that describes each visitor … is broadcast to tens or hundreds of companies … in order to solicit potential advertisers' bids for the attention of the specific individual visiting the website. A data breach occurs because this broadcast, known as a 'bid request' in the online industry, fails to protect these intimate data against unauthorized access."

In late November, consumer groups across seven European countries filed complaints[3] against another major tech company, alleging that it does not have a lawful basis for processing location data, because its users are not given a real choice about how that data is used. DPAs in France and the United Kingdom have also issued warnings to several ad tech companies, challenging the consent mechanisms used for the collection of location data.

While fines have been issued, they have been limited. A €4,800 fine for illegal video surveillance activities and a €400,000 fine imposed on a hospital after employees illegally accessed patient data are among the few reported fines issued.[4] In Germany, a €20,000 fine was imposed on a social media platform after an investigation following a reported security breach revealed that the company stored user passwords in plain text. The violation of the obligation to guarantee the security of personal data under Article 32 (1)(a) of the GDPR, rather than the breach itself, was cited as the justification for the fine.[5]

Below are some lesson learned from enforcement activities of the past six months.

Warnings Before Fines — For Now

In many cases, DPAs have issued warning letters and notices, rather than fines. In July, for example, the U.K. Information Commissioner's Office (U.K. ICO) issued an enforcement notice[6] to AggregateIQ Data Services Ltd., or AIQ, a Canadian data analytics firm. AIQ was hired to target ads at voters during the Brexit referendum campaign.

Although AIQ used data that was collected prior to May 25, it retained and processed data after that date without having a lawful basis to do so, and without providing adequate transparency. The U.K. ICO alleged that by using this data to target individuals with political advertising on social media, AIQ "processed personal data in a way that those individuals were not aware or, for purposes which they would not have expected, and without a lawful basis for that processing." According to the BBC, AIQ plans to appeal the notice.

Although these warnings have been issued to specific companies, all companies subject to the GDPR should take note. Companies that fail to adjust their practices to meet the standards articulated in these warnings could ultimately be subject to fines.

Beware of Data Subject Complaints

Responding to data subject requests is one of the key elements of GDPR compliance, and one of the greatest sources of risk — a data subject's complaint may put a company on a DPA's radar for enforcement. The CNIL (France's DPA) reported that since May 2018, it has received over 3,000 complaints from individuals, and the Irish DPA also provided figures indicating that, as of July, it had logged 743 complaints.[7]

Prompted by a consumer complaint, the Irish Data Protection Commissioner recently initiated an investigation into t.co, Twitter's link-shortening system. Twitter allegedly declined to provide t.co data in response to the consumer's access request, arguing that to do so would require disproportionate effort.[8]

Provide Consumers a Choice Before Using Location Data for Advertising Purposes

Both regulators and consumer groups have focused on the use of location data in the warnings or complaints issued since May. In July, the CNIL announced[9] formal notice proceedings against Fidzup and Teemo — two mobile ad tech companies — for failing to obtain GDPR-compliant consent from individuals when processing their geolocation data for advertising purposes. (Teemo was also put on notice for retaining geolocation data for 13 months, which the CNIL said was too long to justify the purpose of targeted advertising.)

In each case, the individuals were asked to consent only to the collection of data by the mobile application, not the software development kit, or SDK. Additionally, the CNIL challenged the timing of the consent, finding that the SDK started to collect data upon installation of the app, before consent was obtained. In late October, a similar proceeding[10] was opened involving SingleSpot, another mobile ad tech company. All three proceedings have since been closed.[11]

Each company updated its practices to require its publisher partners to display a banner during the app installation process to give users the choice to opt in to any data collection. These banners inform users of the following: 1) the purpose of the data collection; 2) the identity of controllers receiving that data (accessible via hyperlink); 3) the data collected; and 4) the possibility of withdrawing consent at any time. Teemo also updated its data retention policies so that raw data is deleted after 30 days and aggregate data is deleted after 12 months.

Programmatic Advertising Survives, With New Restrictions

The IAB Europe's Transparency and Consent Framework, or TCF, a protocol for collecting consent and conveying it throughout the adtech ecosystem, is positioned to be the industry's most viable solution for consent management. That said, there continue to be some challenges, particularly in the context of programmatic advertising where the requirement to be "specific" about the various purposes for which data is being collected and the identity of the recipients makes it difficult to draft language that is clear and understandable enough to demonstrate that the consent is also "informed."

At the end of October, the CNIL issued a notice[12] to Vectaury, another mobile ad tech company, for its failure to obtain GDPR-compliant consent for its data processing activities. Vectaury collected data both through its SDK and through real-time bidding offers initially transmitted via auctions for advertising inventory. Vectaury retained the data it received through the bidding offers for use beyond responding to the bid. Although Vectaury implemented a consent management platform as part of the TCF, the CNIL found that the consent language failed to notify the users how their data would be used and who it would be shared with.

Small Companies Won't Escape Enforcement

It is worth noting that the initial actions by the U.K. ICO and CNIL have been directed towards small ad tech companies, confirming that it is the activity of a company, rather than its size, that will determine the likelihood of enforcement.

Legitimate Interests Remains Viable — For Now

In each of the cases involving the collection of geolocation data addressed by the CNIL, the company relied on consent as its lawful basis for processing data.

What has yet to be tested is whether, rather than trying to meet the stringent requirements for consent, ad tech companies may find a better path forward with another lawful basis, such as legitimate interests (at least for processing activities that don’t involve sensitive or special categories of data).

Data Breach Reporting Has Increased and Individuals Have Exercised Their Rights

One of the key changes to European privacy law introduced by the GDPR is the 72 hour window for reporting personal data breaches. The CNIL reported[13] that since May 2018, it has received approximately seven data breach notifications a day involving 15 million individuals.

The Irish DPA also provided figures indicating that, as of July, it had logged 1,184 data breach notifications. According to Microsoft,[14] over five million people from 200 countries have used Microsoft’s new privacy tools to manage their data, and over two million of those requests came from the U.S.

New Guidance on Territorial Scope

The European Data Protection Board, or EDPB, which replaced the Article 29 Working Party as the body in charge of ensuring that the GDPR is applied consistently across the European Union, issued draft guidance[15] on territorial scope. The guidance attempts to clarify that the processing of personal data of individuals in the EU by non-EU companies does not trigger the application of the GDPR, as long as the processing is not related (1) to a specific offer directed at individuals in the EU or (2) to a monitoring of their behavior in the EU.

The draft reinforces previous guidance that the mere accessibility of a website in the EU does not, by itself, provide sufficient evidence to demonstrate the controller's or processor's intention to offer goods or services to an individual located in the EU. With respect to monitoring, the EDPB does not consider that merely any online collection or analysis of personal data of individuals in the EU would automatically count as “monitoring.”

Instead, it will consider the controller’s purpose for processing the data and, in particular, any subsequent behavioral analysis or profiling techniques involving that data. Comments to the guidelines are due by Jan. 18, 2019.

What’s Next?

In the next three to six months, we expect to see more enforcement action (including fines) as the DPAs work their way through pending complaints. In the long term, we expect that more countries will follow Brazil, India and California in passing “GDPR-like” regulations.

More than ever, understanding your data collection, use, storage and deletion practices is crucial so that you are prepared for these and future regulatory developments. Below are a few points to consider as your company prepares for 2019.

Data Mapping

Companies that didn't conduct a data-mapping exercise may consider doing so in 2019. Understanding what data you have, where it is stored, how it is used and to whom it is disclosed will put your organization ahead of the curve in complying with any new privacy regulations.

Ongoing Privacy Assessments

Data protection impact assessments drafted 6 months ago may already be out of date. Implementing an ongoing privacy assessment program will help privacy and business teams work together to manage the privacy risks presented by new projects.

Monitor Enforcement

Use the enforcement actions as a check against your company's practices. Companies may avoid enforcement by learning the lessons imposed on others.

Examine Security Practices

While companies have some flexibility to determine what level of technical and organizational security practices are appropriate for the nature of the data they process, security practices should at least align with industry best practices.

Jessica B. Lee is a partner at Loeb & Loeb LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://noyb.eu/4complaints/.

[2] https://brave.com/adtech-data-breach-complaint.

[3] https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html.

[4] https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/.

[5] Id.

[6] https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf.

[7] https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application.

[8] http://fortune.com/2018/10/12/twitter-gdpr-investigation-tco-tracking/.

[9] https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire.

[10] https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-pour-absence-de-consentement-au-traitement-de-donnees-de.

[11] https://www.cnil.fr/fr/applications-mobiles-cloture-des-mises-en-demeure-lencontre-des-societes-fidzup-et-singlespot.

[12] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037594451&fastReqId=974682228&fastPos=2.

[13] https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application.

[14] https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/.

[15] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.