THOMSON REUTERS
Westlaw®

Non-profit activists' strategic pursuit of alleged GDPR violations spurs compliance developments

By Michelle Reed, Esq., Natasha Kohne, Esq., Jo-Ellyn Sakowitz Klein, Esq., and Rachel Kurzweil, Esq., *Akin Gump**

MARCH 22, 2019

This alert discusses two recent developments in relation to compliance with the European Union's General Data Protection Regulation (GDPR) that came about as a result of complaints filed by NOYB — European Center for Digital Rights,[1] an Austria-based, non-profit organization founded by Max Schrems, a well-known privacy activist. Schrems is best known for filing the case that led to the demise of the U.S.-EU Safe Harbor data-sharing agreement in 2015.

First, on January 18, NOYB filed a series of strategic complaints with the Austrian Data Protection Authority against eight companies (on behalf of 10 users), including Apple Music, Amazon Prime, YouTube, Netflix, Spotify and others (collectively, the "Companies"), for violations of the GDPR.

Second, on January 21, the French Data Protection Authority (Commission Nationale de l'informatique et des Libertés or CNIL) fined Google €50 million (about $57 million) for GDPR violations.[2]

The CNIL's fine arose out of an investigation initiated in response to complaints filed by NOYB and a French digital rights group. Below, we provide a brief overview of the claims alleged in the recent NOYB complaints and in the CNIL/Google case.

These recent developments suggest that NOYB and other activist non-profit organizations may play an influential role in driving GDPR enforcement moving forward. NOYB's recent complaints indicate that it, and likely other activist non-profit organizations, is strategically testing companies' compliance with different parts of the GDPR.

NOYB'S COMPLAINTS TO THE AUSTRIAN DATA PROTECTION AUTHORITY

NOYB's most recent complaints generally allege that the Companies failed to properly respond to consumers' requests for data that the Companies collected about consumers. The complaints demonstrate that activists are proactively testing companies' response systems and may go after noncompliant companies.

Article 15 of the GDPR grants data subjects a "right to access" personal data that has been collected about them, and Recital 63 of the GDPR notes that data subjects must be able to exercise that right easily and at reasonable intervals.

Under this framework, data subjects are entitled to a copy of all raw data that a company holds about the data subject, including information about the sources and recipients of the data subject's data, the purpose for which the data is processed, the countries where the data is stored and how long the data is stored.

The recent NOYB complaints allege that, when individual users sought to exercise this right by requesting information from the Companies, each Company provided either a deficient response or no response at all. Accordingly, NOYB filed complaints on behalf of the individuals against each Company for several violations of the GDPR.

Under Article 83, the violations could carry a maximum fine of €20 million or 4 percent of the worldwide turnover (whichever is higher) — which NOYB estimates translates into a potential combined maximum penalty of €18.8 billion across the 10 complaints.[3] To date, none of the fines sought by data protection authorities have reached the statutory maximum.

NOYB argues that the Companies have engaged in a pattern of structural violations by building automated systems that provide deficient responses to data access requests.

Specifically, NOYB alleges that each Company's automated responses violate the GDPR by failing to do one or all of the following in response to a data subject's request:

- Provide information about the exact purpose for which the data subject's personal data is undergoing processing, as required by Article 15(1)(a).
- Provide information about the recipients of the data subject's personal data, as required by Article 15(1)(c).
- Provide information about the envisaged personal data retention period, as required by Article 15(1)(d).
- Provide information about the data subject's right to request rectification or erasure, the right to restrict the processing of personal data, or the right to object to such processing, as required under Article 15(1)(e).
- Provide information about the data subject's right to lodge a complaint with a supervisory authority, as required under Article 15(1)(f).

- Provide information about the sources of the data subject's personal data, as required under Article 15(1)(g).
- Provide information about appropriate safeguards for transfers of data to third countries, as required under Article 15(2).
- Provide the data subject with raw data in a format that was concise, transparent, intelligible and easily accessible, as required under Article 15(3).

NOYB asked that the Austrian Data Protection Authority (1) investigate each Company; (2) find that the complainants' rights were violated; (3) compel each Company to fully and correctly respond to the complainants' access requests; and (4) impose an "effective, proportionate and dissuasive fine" on each Company of up to 4 percent of their worldwide revenue. It remains to be seen what actions the Austrian Data Protection Authority will take in response.

The cases could be a bellwether for similar noncompliance claims in other EU states, as well as in other jurisdictions that have adopted statutes with similar data subject request obligations. The 2018 California Consumer Privacy Act, for example, also requires companies to provide consumers with certain information in response to verifiable consumer requests.

NOYB'S MAY 2018 COMPLAINTS AND CNIL'S ACTION AGAINST GOOGLE

In May 2018, shortly after the GDPR took effect, NOYB filed a series of complaints against several large tech firms in a number of European jurisdictions. Shortly thereafter, La Quadrature du Net (LQDN), a French advocacy group that promotes digital rights, filed similar complaints against some of the same defendants.[4]

The complaints generally alleged that the large tech companies violated the GDPR by failing to disclose to users how their personal information is collected and processed, by forcing customers to agree to their privacy terms or not use their services, and by not having a valid legal basis to process the personal data of the users of its services (particularly for ads personalization purposes).[5]

Notably, in response to the complaints NOYB and LQDN filed against Google with the CNIL, the CNIL initiated an investigation. The CNIL's investigation analyzed the browsing pattern of users and the documents that users can access when creating a Google account during the configuration of mobile equipment using the Android operating system.[6]

On January 21, the CNIL announced that it had fined Google €50 million for failing to disclose to users how their personal information is collected and processed.[7] The CNIL also found that Google did not properly obtain users' consent for data collection or processing.

The CNIL found two violations of the GDPR: lack of transparency and invalidly obtaining user consent for ads personalization.

Lack of transparency

Various portions of the GDPR require companies to process personal data in a transparent manner (*see* Art. 5), provide information to data subjects in a transparent and easily accessible format (*see* Art. 12), and provide specific information to data subjects when data is collected (*see* Art. 13).

The CNIL found that the information provided by Google to users about its processing activities was not easily accessible for users, nor was it clear and comprehensive because:

- "Essential information" that should have been provided to users when their data was collected (e.g., the data processing purposes, data retention periods or the categories of personal data used for ad personalization) was disseminated across several documents and accessible only after several steps.[8]
- The listed purposes of the processing operations carried out by Google and the categories of data processed for those purposes were "described in a too generic and vague in manner."[9]
- The information communicated to users "was not clear enough so that the user could understand that the legal basis of processing operations for ads personalization is the consent, and not the legitimate interest of the company."[10]

Invalidly obtaining user consent for ads personalization

The GDPR requires companies to have a lawful basis for processing personal data (*see* Art. 6(1)). One such way to meet this obligation is for a company to obtain a data subject's consent to process his or her data (*see* Art. 6(1)(a)).

The CNIL found that the consent that Google obtained from users was not validly obtained because:

- Users were not "sufficiently informed" about Google's processing activities because the information that Google provided was diluted in several documents and did not effectively enable a user to be aware of the extent of the processing activities and the "plurality of services, websites and applications involved in [Google's] processing operations."[11]
- User consent to Google's processing was not "unambiguous" because users have to click on a "more options" button to access the company's personal ads configuration, and the display of the ads personalization is a pre-ticked box.[12]

- User consent was not "specific" because it was not given distinctly for each of the processing operations purposes carried out by Google (i.e., for ads personalization, speech recognition), but rather asked users to tick boxes agreeing to Google's Terms of Service and Privacy Policy when they set up an account, requiring users to give consent in full, for all processing operations.[13]

Other data protection authorities in EU jurisdictions outside of France are still carrying out investigations related to the complaints filed by NOYB and LQDN.

Google has indicated that it will appeal the CNIL fine. The company has informed media outlets that it "worked hard to create a GDPR consent process for personalised ads that is as transparent and straightforward as possible, based on regulatory guidance and user experience testing."

CONCLUSION

The recent CNIL fine is indicative of the powerful result that can flow from activists' pursuit of alleged GDPR violations. NOYB's most recent string of complaints indicate that it is monitoring companies' compliance with the GDPR and is actively testing consumer-facing compliance frameworks to find weaknesses.

These developments highlight the need for companies to quickly and effectively respond to consumer requests for information and to evaluate how they disseminate information about processing activities and obtain user consent, in particular.

NOTES

1 https://noyb.eu/

2 https://bit.ly/2CrQhfV

3 https://bit.ly/2JoNpX5

4 https://bit.ly/2W8rh4Y

5 https://bit.ly/2CrQhfV and https://bit.ly/2ETc2np

6 https://bit.ly/2FDztWt

7 *Id.*

8 *Id.*

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

ABOUT THE AUTHORS




(L-R) **Michelle Reed** is a partner in **Akin Gump**'s Dallas office and co-head of the firm's cybersecurity, privacy and data protection practice. She helps companies and boards navigate the ever-changing cybersecurity and data privacy landscape, advising on breach preparedness and response, conducting comprehensive privacy and security risk assessments, and developing policies and procedures to mitigate and remediate cybersecurity threats. **Natasha Kohne** is a partner in Akin Gump's San Francisco and Abu Dhabi offices and also co-heads the firm's cybersecurity, privacy and data protection practice. She maintains a cutting-edge international legal practice that focuses on investigations, litigation, regulatory and compliance, often involving complex multijurisdictional and cross-border challenges. **Jo-Ellyn Sakowitz Klein** is senior counsel at Akin Gump in Washington D.C. and a leader in the firm's cybersecurity, privacy and data protection practice. She handles privacy, data security, data breach preparedness and data breach response matters for clients across many industries, with a special emphasis on the health sector. **Rachel Kurzweil** is a Washington-based associate in Akin Gump's health care and life sciences practice and a member of the firm's cybersecurity, privacy and data protection practice. She advises a broad-based group of companies on regulatory and transactional matters related to health care regulatory compliance, privacy and data protection with a specific focus on the EU General Data Protection Regulation. This article was first published Jan. 25, 2019, on the firm's website. Republished with permission.