
## THE MAY 25 GDPR COMPLIANCE DEADLINE HAS PASSED

# WHAT DOES ENFORCEMENT REALLY LOOK LIKE?

**Batya F. Forsyth and Everett Monroe** Hanson Bridgett LLP

The European Union's General Data Protection Regulation went into effect on May 25, 2018. While very high-profile complaints were lodged with some European Data Protection Authorities (DPAs), the agencies themselves have focused more on providing guidance for EU businesses, both as individual agencies and through their reconstituted body, the European Data Protection Board. As the DPAs plan meetings and continue to discuss key issues, enforcement has settled on the fundamentals of the regulation. A particular focus is being paid to those industries where companies regularly collect personal data on a large scale and those in a position to reveal intimate details about a data subject's life. Meanwhile, non-EU organizations continue to struggle with whether and how GDPR applies to them, while DPAs prioritize providing guidance to businesses in the EU.

GDPR succeeds the now defunct Data Protection Directive that required EU member states to pass laws to control how personal data could be collected and used. The new regulation maintains much of the substance of the original directive, but substantially increases penalties for violations, seeks to improve uniform application of rules across the EU, and expands the territorial scope of the regulation to include non-EU businesses offering goods and services to EU data subjects or monitor the behavior of EU data subjects.

GDPR has multiple avenues of enforcement. The long-established national DPAs are still empowered to bring actions in their member countries. Additionally, individuals may submit complaints to the DPAs to which the DPAs must review and respond. Individuals may also bring civil suits in EU member state courts for damages caused by GDPR violations. Injured parties may also assign their legal rights to a non-profit or civil society organization to bring suit collectively for a group of data subjects.

Private consumer complaints from EU data subjects currently drive enforcement activities within the European Union. The non-profit organization noyb (an acronym of "none of your business") filed the most prominent of these complaints, alleging GDPR violations against Google, Facebook, and two of Facebook's subsidiaries, WhatsApp and Instagram. noyb's founder and chairman, Max Schrems, was the named party in the 2013 case Schrems v. Data Protection Commissioner that invalidated the EU-U.S. Safe Harbor legal framework that Facebook used to transfer personal data from the European Union to the United States. Then, when Facebook switched its compliance mechanisms for international data transfer to EU standard contract clauses, Schrems challenged the data transfers on that basis as well.

The core of noyb's current complaints is about consent—namely, that consent obtained from data subjects for the use of their data is invalid because it is a pre-condition for using the service at all. At least at first glance, this would appear to be contrary to guidance from DPAs providing that consent for processing personal data cannot be tied to the provision of a service that does not require that processing to function.

DPA-initiated enforcement actions against companies remain more limited in scope with a focus on ensuring the protection of data subject rights from serious or systemic harms. The Irish data protection commissioner has announced its office will prioritize enforcement towards large-scale data processing activities that constitute a high risk to data subjects. Sweden's DPA has sent out enquiries to organizations that collect and process more sensitive personal data, seeking to determine whether those organizations have appointed a data protection officer as the GDPR requires of companies handling large volumes of sensitive personal data.

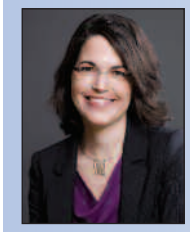
So far, other DPAs seem more intent on providing guidance for compliance rather than pursing enforcement. For example, the United Kingdom's Information Commissioner's Office has published extensively on compliance topics Collectively, DPAs have worked together through the new organizing body, the European Data Protection Board (EDPB). The EDPB replaces the Data Protection Directive's Article 29 working party, and has been granted more formal powers to address issues of GDPR interpretation with an eye toward uniformity and consistency. In its first meeting, the Board focused on revising and adopting its previous guidance from the Article 29 Working Party, and has issued new guidelines regarding exceptions applicable to international data transfers.

DPAs, individually or collectively, have not focused attention on GDPR's expansion of territorial scope. GDPR expanded its territorial scope to include businesses outside the EU offering goods and services to EU persons, and monitoring the behavior of persons in the EU. Because these territorial scope provisions were not in the Data Protection Directive, there is little guidance on how DPAs plan to interpret that provision, and there has not yet been an attempt to bring an enforcement action against a company based on the new expanded scope.

That uncertainty, combined with additional legal responsibilities for EU businesses to ensure adequate protections for personal data from their contractors and vendors has drawn the most attention in the United States. While there is reason to believe that GDPR's expanded scope is focused on preventing the tracking of a user's web browsing activities across websites, the letter of the regulation is written broadly enough to include even innocuous behaviors like keeping track of the items in a user's online shopping cart or remembering the preferences of a user on a customizable webpage. As a result, many U.S. businesses that may fall within that definition are taking incremental steps to comply with GDPR. In the alternative, some companies are implementing changes in order to avoid GDPR, either by disabling website technologies that could be considered "monitoring behavior," or by preventing EU users from accessing their services altogether.

Many U.S. companies that were not necessarily concerned about GDPR's direct application are now receiving compliance inquiries from their EU business partners. Some companies have been expected to accept additional addendums to their service agreements requiring them to ensure that they will also agree to respect the rights of data subjects whose data is in their care, requiring them to agree to auditing and cooperation with EU data protection authorities. Some U.S. contractors, in an effort to maintain some uniformity in commitments to their clients, have written their own forms that give effect to GDPR's contractual assurances requirements.

While many organizations in the EU and the U.S. braced themselves for a wave of lawsuits and severe enforcement actions, it appears that serious enforcement has been limited to a small number of high-profile cases. While DPAs do appear to want to move companies towards compliance, it seems for now that their current strategy is much more focused on providing guidance and advice than it is on starting aggressive enforcement campaign. Ultimately, this gives all organizations that process personal data an additional opportunity to take a thoughtful approach to GDPR compliance before enforcement begins in earnest.

*Batya Forsyth is the chair of Hanson Bridgett's Litigation Section and co-chair of the Privacy, Data Security and Information Governance group. She is a Certified Information Privacy Professional (US) with the International Association of Privacy Professionals (IAPP.org). Batya counsels clients regarding privacy policies, compliance issues, data breach response and related insurance coverage issues, across multiple industries and jurisdictions.*

*Everett Monroe's litigation practice at Hanson Bridgett focuses on data privacy and intellectual property disputes and counseling, two areas in which his technical background as an electrical engineer join with his legal experience to serve clients in a range of complex matters. Everett is also an Adjunct Professor at the University of San Francisco, teaching Information Privacy Law.*