GDPR at One Year: What We Heard from Leading European Regulators

By Caitlin Fennessy, Senior Privacy Fellow

iapp

On May 25, 2019, the EU General Data Protection Regulation turns one. Like a toddler who's learning to stand on her own two feet, GDPR at one is still a work in progress. For this report, the IAPP collected figures from the primary "guardians" of the young upstart, some of Europe's leading data protection authorities, and questioned them about their main areas of focus for the next year.

It's been a busy first year for GDPR. Companies and regulators alike worked hard to prepare for and then implement GDPR requirements. EU DPAs saw increases in staff and resources, but those paled in comparison to the influx of complaints, data breach notifications, and data protection officer registrations they received.

500,000+ registered DPOs
280,000+ cases
144,000+ complaints
89,000+ data breach notifications
440+ cross-border cases
56,000,000+ euros in fines

What can privacy professionals learn from these numbers and the intense activity that surrounded them? What do DPAs forecast as the focus of their year two and where will they concentrate their enforcement powers?

For this report, we reviewed European Data Protection Board and DPA reports and sought input from regulators in Austria, France, Ireland and the United Kingdom on five key issues: the number and nature of complaints, investigations and DPO notifications over the first year of GDPR, as well as the technical challenges and guidance needed in the year ahead. Here's what we learned.

The IAPP appreciates the information provided by the offices of:

Andrea Jelinek, DSB, Austria

Helen Dixon, DPC, Ireland

Marie-Laure Denis, CNIL, France

Elizabeth Denham, ICO, UK

Individual complaints

How many individual complaints have DPAs received since GDPR went into effect? What do they tell us about individuals' top concerns?

According to the EDPB, **281,088 "cases"** were reported by DPAs in 27 EEA countries in the first year of the GDPR. Of these, 144,376 were **"complaints"** whereas 89,271 were **"data breach notifications."** Top complaint categories appear to be similar across countries, though terminology used by DPAs to characterize them differs. The major complaint themes included the right to access data and to prevent processing as well as concerns regarding disclosures and unauthorized processing.

The Austrian DPA reported receiving 1,658 complaints between May 25, 2018 and mid-April 2019. Data subject rights topped complaint categories in Austria, followed by data breaches and then procedures on administrative fines. Eighty-seven percent of complaints had a national scope, while the remainder were international.

In 2018, the CNIL received a total of 11,077 complaints. The majority focused on data subject rights (73.8%). Broken down further, the diffusion of personal data across the Internet was the subject of the highest number of complaints (35.7%). This category includes "right to be forgotten" complaints. Processing of data for marketing purposes ranked second among complaint topics (21%), including the use of SMS for sales prospecting. Employee privacy complaints ranked third (16.5%), including concerns related to video surveillance and geolocation.

Yann Padova

IAPP Country Leader, France

According to these trends, the CNIL has decided to focus its annual enforcement program, including dawn raids, on the following three topics: data subjects' rights violations, controller and processor's roles and relationship and the protection of children's online privacy rights. This program is the first important decision from CNIL's new chair. Another striking figure is the relatively low level of data breach notifications in France, around 10 times less than in the UK or in the Netherlands. Such a discrepancy remains unexplained but clearly reveals a high level of under-notification in France.

The Data Protection Commission received 2,864 complaints between May 25, 2018 and December 31, 2018. Of these, 1,928 were GDPR-related. The largest category of complaints related to access rights (30%), followed by those concerning unfair processing of data (15%) and disclosure (11%). 2018's top complaint categories closely tracked those in prior years, though the quantity of complaints increased by more than 50%. While most complaints were amicably resolved, 18 resulted in formal decisions. Thirteen upheld the complaint and five rejected it. The DPC also recorded 3,542 data breaches, the vast majority of which were unauthorized disclosures. Thirty-eight of these breaches related to 11 multinational technology companies. The DPC reported that many of these resulted from bugs in software supplied by service providers.

The UK Information Commissioner's Office received 39,825 "concerns" between May 25, 2018 and April 2019 in the form of requests for assessment. While this is a staggering number even given the UK's size, the ICO noted that some could be in relation to events that preceded the GDPR's entry into force and so would be handled under the prior legislation. The UK's complaint website outlines the wide variety of issues on which individuals can submit concerns to the ICO, including nuisance calls and messages, the use of cookies, access to information from public authorities, the right to be forgotten and cross-border transfers, among others. The top three issues raised by individuals over the past year were: data subject access to personal data, disclosure of data, and the right to prevent processing.

Investigations and enforcement

How many investigations and enforcement actions have DPAs initiated under GDPR? What do they suggest regarding DPAs' priorities moving forward?

The EDPB's February 2019 report to the European Parliament indicated that **11 countries** had imposed **GDPR fines totaling approximately €56 million**. Poland's first GDPR enforcement action **and €220,000 fine** followed soon after the EDPB report. Details regarding the total number or scope of enforcement actions across the EU were elusive. While some DPAs publicize actions to share lessons learned or as part of the punitive measure, others do not. The characterization of investigations and how those relate to complaints also differs across the EU.

The Austrian DPA noted that it was the first authority to issue a fine under the GDPR, one that, at €7,000, was proportional to the size of the company and the violation. Each of the more than 1,600 complaints received by the DPA led to an investigation. An additional 143 investigations were launched on the DPA's own initiative. More than 50 enforcement actions were finalized (33 related to individual complaints or investigations, 11 resulted in fines and eight in warnings). **The DPA's investigative priorities are guided by incoming complaints, which cover a wide variety of topics, and data breach reports.**

The CNIL's annual report cites 310 investigations in 2018. Two-hundred and four of these were onsite investigations (including 20 investigations of CCTV systems), 51 were online investigations, 51 were document-based investigations and four were hearings. In most cases, the orders issued by CNIL resulted in the organizations' compliance. Forty-nine orders were adopted in 2018. Two sectors were particularly targeted: five orders were in the insurance sector; four orders concerned companies specialized in targeted advertising via mobile applications. Eleven sanctions were issued, ten of which included monetary penalties. **In 2019, the CNIL plans to focus on complaints and three main themes: the exercise of rights, sharing of responsibilities between processors and subcontractors, and children's data.**

The DPC has launched 52 formal statutory inquiries under the GDPR, either based on complaints or of its own volition. According to the DPC, these are proceeding

through the investigation phase. The scope of these investigations covers a cross-section of GDPR requirements, including transparency, lawful basis for processing, security of processing, and data breach notification requirements. Of the inquiries launched, the DPC has recently indicated that 18 involve large tech companies. Decisions in some of those cases are expected this summer. Shortly after the GDPR entered into force, the DPC launched 31 inquiries into public sector surveillance of citizens for law-enforcement purposes through the use of CCTV, body cameras, drones and other technologies. While the DPC has not yet exercised its corrective powers on any GDPR cases, the Commission has continued to bring enforcement actions under the prior legal regime, as required by law in cases that preceded the GDPR's entry into force. The DPC is currently involved in more than 15 litigation matters relating to cases under the previous legislation. The DPC also engaged directly with companies in 2018 on the processing of location data, the transfer of personal data from third-party applications, processing of telemetry data, and the sharing of personal data within a corporate group. **The ad tech sector was and will continue to be a focus for the DPC due to concerns regarding profiling, particularly using sensitive data, the use of location data, and lack of lawful bases for or individual awareness of processing.**

The ICO cited fairness as an overriding theme in its investigations and enforcement actions, noting inquiries into unfair processing and lack of transparency. **In terms of priorities moving forward, the Commissioner said the ICO is looking at data brokers, the processing of children's data, and ad tech.** While the ICO has begun to bring enforcement actions under the GDPR, the vast majority of actions taken since May 25, 2018 were brought under prior data protection law due to the timeframe of the violations.

Giles Watkins

IAPP Country Leader, UK

It is encouraging that the UK ICO has chosen to focus on working with the business community to address potential problem areas rather than automatically resorting to fines and enforcement actions. Nowhere is this more apparent than in the areas of emerging technology and innovation.

However, I sense that there is only a limited time for organizations to put their houses in order before the commissioner does revert to the enhanced penalty regime, with potential enforcement actions perhaps being even more significant to businesses than the monetary fines.

This surely means more work for privacy professionals within their organizations, but also more training and homework! Privacy compliance will become more automated, with privacy engineering receiving an even greater focus: building controls into applications and processes, rather than putting cumbersome, expensive and less-effective manual procedures around data flows. With the increasing need for the DPO to have a view across the whole organization, and to communicate effectively from Board level to the technologists, I wonder how long it will be before regulators start to consider both the capabilities and the independence of the vast number of newly minted data protection officers.

DPO registrations

How many data protection officers are available to address these complaints, breaches and investigations? Do they have the support they need?

The IAPP estimates that approximately **500,000 organizations have registered DPOs** across the European Economic Area. This EEA-wide estimate is based on **376,305 documented DPO registrations by organizations** in 12 EU member states that shared registration numbers with the IAPP (Austria, Bulgaria, Denmark, Finland, France, Germany, Ireland, Italy, the Netherlands, Spain, Sweden, and the United Kingdom). Approximately half of these registrations were made in Germany alone, where DPO registration requirements preceded GDPR.

The numbers of complaints, data breaches and investigations launched across Europe suggest that even with the significant number of DPOs to address them, additional support will be needed.

After sharing the IAPP's research on DPO registrations publicly, we were quickly asked how many DPOs we thought *should* be registered. While that is not a question we can answer at this stage, it is one that at least one of the DPAs we interviewed is also exploring.

Speaking at the IAPP Global Summit, Austrian Data Protection Commissioner Andrea Jelinek stated that "the importance of the DPO cannot be overstated." She cited the important role DPOs play in building support for data protection within companies and in ensuring that individuals' rights are protected. As of mid-April, 5,142 organizations had registered DPOs in Austria. Thirty-five had done so in 2017, 4,754 in 2018 and 353 in 2019. Looking at the number of organizations that registered a DPO as a percentage of total company presence in each country, Austria represented almost exactly the European average (excluding Germany).

In France, 51,866 organizations had registered a DPO as of mid-April. This number increased from a total of 39,500 at the end of 2018, highlighting the fact that registrations have continued into 2019. Within this population, the CNIL found a significant pooling effect. Among the 51,866 organizations that had registered, the actual DPO population was only 17,905, meaning many organizations chose to share DPOs. Sixteen-thousand of the organizations that submitted a DPO registration were public bodies.

As of mid-May, the DPC has received 1,185 DPO notifications. Eight-hundred and seventy-four of these were from private-sector organizations, 176 were from public-sector organizations and 135 were from not-for profits. In Ireland, the pooling effect was less dramatic with over 900 different DPOs serving the 1,185 organizations that registered a DPO with the DPC. The DPC has conducted an initial analysis of public sector notifications and plans to remind those that have yet to register DPOs of their obligations in the near term. The DPC will conduct a similar exercise with regard to private sector bodies. Citing the position's importance, the DPC launched a consultation soliciting input from DPOs on their experience with GDPR during its first year. The DPC plans to establish a Data Protection Officer Network in 2019, "to facilitate the sharing of good practice and lessons-learned through peer-to-peer DPO support."

Kate Colleary

IAPP Country Leader, Ireland

Since this time last year, many Irish organisations have finalised their GDPR projects and are now moving to a more strategic, business as usual model. Privacy notices are being reviewed and tweaked to reflect a more sophisticated understanding of what is required by GDPR and how it impacts the organisation's business model.

Organisations that spent time and effort in developing a GDPR programme are now reaping the benefits of that good work and are confident in their systems and processes. They have embedded the CPO or DPO role into the organisation, have developed a privacy training programme for staff, and can clearly articulate decisions they have made and the reasons and legal basis for those decisions.

Organisations that did not lay the groundwork for GDPR often find themselves scrambling to respond to DPC queries (which are often wide ranging), particularly if they suffer a notifiable breach. These organisations may also be under the DPC's spotlight if they have not appointed a DPO where required to do so. The DPC is extremely active and it has become clear that there is no shortcut to GDPR compliance – it's about proper resourcing, expert knowledge and applying that knowledge to systems in the organisation.

The ICO had received DPO registrations from 32,863 organizations as of the beginning of May. While a significant number, it is worth noting that more than 600,000 organizations had registered with the ICO by the same date as organizations "that process personal information." This registration and the applicable fee is required by the UK's 2018 data protection law (as it was under the prior law), unless the organization is exempt.

Technical challenges

What do DPAs view as the top technical challenges for data protection?

The EDPB's 2019-2020 strategic work program identifies **several technical challenges to tackle** in the years ahead. Having endorsed guidelines on the interpretation of new provisions introduced by the GDPR, the EDPB now aims to focus more on specific issues and technologies. The EDPB's work program contains an ambitious and broad cross-section of projects and planned guidelines. These include the development of guidelines on **connected vehicles** and **video surveillance** and potential projects related to **blockchain** and the use of new technologies, such as **artificial intelligence** and **connected assistants**.

As the Chair of the EDPB, the Austrian Data Protection Commissioner pointed to the technical challenges outlined in the EDPB's 2019-2020 work program, on which her office will continue to focus in coordination with authorities across Europe. The Commissioner cited the value of the EDPB platform in debating such pan-European challenges and successfully identifying more encompassing solutions than might be possible for individual DPAs.

Sebastian Kraska

IAPP Country Leader, DACH

Whilst the DPAs were drowning in data breach notifications, complaints about companies and DPO registrations in the first year, companies tried to focus to address the "minimum standards" of GDPR by implementing proper privacy management systems and focusing on the aspects of records of processing activities, IT security and vendor management.

Enforcement has been relatively conservative so far – seeming to follow a "one-year grace period" after May 25, 2018. But Data Protection Authorities especially in Germany are expected to drastically increase their SME audits in Q3 and Q4 to ensure level playing field.

The German DPAs also took a progressive position on website tracking basically requiring explicit opt-in for all types of individualized tracking (re-targeting etc.), even when based on pseudonymized data. Should this become an EU wide standard (and the EDPB is likely to have a say on this as well) it might become close to irrelevant for most companies whether we see an additional ePrivacy-Regulation at the end of the day or not. We expect this decision to be challenged in courts.

The CNIL plans to focus on issues related to **video surveillance**, including those concerning remote viewing of CCTV images and installation of cameras in care units. Other emerging trends under consideration include use of **the right to data portability by bank customers and online content service users** as well as the **type of data mobile applications access on smartphones**.

The DPC views **artificial intelligence, machine learning, encryption, digital ledger technology, digital assistants, identity management, and authentication technologies** as top technical challenges for data protection in 2019. The areas of **facial recognition and location-based services** are also priorities. To help it tackle these challenges with the necessary expertise, the DPC established and staffed a new Technology Leadership Unit. The work of the TLU combines research and analysis with enforcement. The TLU will collaborate with supervisory and regulatory authorities, academics, standards bodies, and other professional groups. Research is already underway with Boston College on cybersecurity, the International Working Group on Data Protection in Telecommunications (also known as the Berlin Group), researchers at Queen Mary University of London and the University of Cambridge on cloud computing challenges, the Future of Privacy Forum on ad tech, the Adapt Centre on next generation digital technologies and with the Cybersecurity Centre in University College Dublin. On the enforcement front, the TLU launched a "sweep" survey focused on the transparency of information provided to data subjects on the processing of contact list data by mobile applications and is examining the lawful basis for that processing.

The ICO has prioritized efforts to address technical challenges associated with data protection, launching a much-lauded regulatory Sandbox in March. It will enable organizations developing innovative and beneficial products or services to work in concert with ICO specialists during the design phase to ensure they are complying

with data protection rules. The ICO also published its first Technology Strategy, outlining its priorities for 2018-2021. In it, the Commissioner cites changes in technology as "one of the key drivers" of the regulatory reform which led to the GDPR and notes that "the ICO's approach to technology will be underpinned by the concept that privacy and innovation are not mutually exclusive." The strategy identifies three priority areas: **cybersecurity; AI, machine learning and big data; and web and cross-device tracking**. Separately, the ICO pointed to data mapping as a persistent technical challenge and area in which additional work is needed. It noted that many data controllers still have only a rudimentary understanding of information lifecycles. While the requirements of GDPR Article 30 are useful, developing a full and practical understanding of the personal data that an organization holds and how it is processed is difficult for many organizations. Building a complete accountability framework is even harder.

Guidance needed

In which areas do DPAs believe additional business guidance is needed?

The **EDPB's two-year work program includes more than two dozen planned guidelines or topics to consider**. In the next few months, the EDPB will focus on accreditation requirements, sector-based codes of conduct, and the concepts of controller versus processor. Additional topics for future guidelines include: delisting, certification and codes of conduct as a tool for transfers, data protection by design and default, targeting of social media users, children's data, legitimate interest, and data subjects' rights, among others. In addition to EDPB guidelines, many member state DPAs are also developing their own guidance, fact sheets and other tools.

As Chair of the EDPB, the Austrian DPA plans to support the board's work to develop guidelines on accreditation, codes of conduct, and controller/processor distinctions, among other efforts.

The CNIL has identified two main groups in need of GDPR guidance: public organizations and startups. To assist public organizations, the CNIL plans to conduct local awareness-raising activities, develop a practical guide to the GDPR, dedicate a section on its website to public authorities and engage with network and association heads. To support start-ups, the CNIL will continue its work in partnership with French Tech Central de Station F, a public booster for start-ups. In 2018, the CNIL organized 19 thematic workshops for start-ups. Topics included data portability, health, security, fintech and connected objects. The CNIL is currently preparing content related to the needs and questions faced by start-ups, which will soon be available on its website.

The DPC's Guidance and Policy Development Unit develops its plan for future guidance based on trends in frequently asked questions, complaint handling and responses to prior guidance. Based on these criteria, in the near term, the DPC plans to publish more detailed guidance on the use of CCTV, breach notification procedures, subject access requests, and the factors controllers should consider when assessing the legal basis for processing. During 2018, the DPC conducted extensive consultations on the processing of children's data and the rights of children under the GDPR. In the months ahead, the DPC plans to use the input received to develop guidance and codes of conduct for organizations that process the

personal data of children and young people. The DPC plans to draft GDPR guidance for local public authorities, charities and volunteers. Its Technology Policy Unit plans to release guidance on AI, adtech, device identification settings and cybersecurity. To complement its DPO Network initiative, the DPC will publish guidance aimed at DPOs this summer. The DPC noted that due to positive response to its informal myth-busting blogs, it plans to continue that series as well as its "Know Your Data" podcast series.

The ICO noted that understanding how to derive value from large personal data sets in privacy respectful ways is a challenge for organizations and an area in which guidance is needed. The ICO pointed to the promise of advancements in anonymization, pseudonymization, homomorphic encryption and differential privacy in combination with efforts to improve organizational controls, including internal divisions, data trusts, and commercial initiatives related to privacy-protective data analytics. The ICO plans to review its Anonymization Code of Practice in the second half of 2019 to ensure it reflects this rapidly evolving work. Ad tech is another area the ICO is exploring, currently focusing on programmatic advertising and real-time bidding. Earlier this year, the ICO held a fact-finding forum on ad tech and, based on the feedback received, plans to issue guidance in this area.

Paul Jordan
Managing Director, IAPP Europe

Concluding Comments

It has been a year since the GDPR came into application. For Europe, and indeed beyond through its extraterritorial nature, there was never any doubt that the GDPR would have a profound influence on how organizations process EU personal data in an increasingly data-driven global economy. Most recently, the European Commission referred to the regulation's introduction as a 'cultural revolution'; the GDPR goes well beyond the compliance obligations of organizations, in that the privacy rights of EU citizens and consumers are core to the regulation in practice.

One thing is certain: There's been no shortage of debate around GDPR. It has stimulated wholesale change in organizational governance and privacy policy generally and will continue to do so across Europe. The advent of the DPO function has been a catalyst for change within working culture as data protection has increasingly become a strategic driver for businesses. This is a beginning, and while accountability is key to GDPR implementation, the establishment of a DPO is not sufficient for effective privacy continuity. Organizations will need to ensure that DPOs and related support privacy functions are sufficiently trained and qualified.

The GDPR regulatory environment is also maturing, and while enforcement has been limited to date, it is still early in the life of the regulation. Expect enhanced frequency of activity in 2019, and going forward, both at the member state level and through the EDPB. Any grace period afforded organizations in this nascent timeframe is truly at an end. We have seen the commencement of GDPR enforcement, and there is much work to be done both at the organizational and regulatory levels.