Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

GDPR | Companies facing mounting pressure

An e-Book publication sponsored by CONDUENT

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

CONDUENT

Conduent delivers mission-critical services and solutions on behalf of businesses and governments – creating exceptional outcomes for its clients and the millions of people who count on them. Through people, process and technology, Conduent solutions and services automate processes, improve efficiencies, reduce costs and enable revenue growth. It's why most Fortune 100 companies and over 500 government entities depend on Conduent every day to manage their essential interactions and move their operations forward.

Conduent's differentiated services and solutions improve experiences for millions of people every day, including two-thirds of all insured patients in the U.S., 11 million employees who use its HR Services, and nearly nine million people who travel through toll systems daily. Conduent's solutions deliver exceptional outcomes for its clients including $16 billion in medical bill savings, up to 40% efficiency increase in HR operations, and up to 40% improvement in processing costs, while driving higher end-user satisfaction. Learn more at www.conduent.com.

Inside this e-Book

Regulators expect maturity in GDPR processes

Regulators at the Compliance Week Europe 2019 conference in Amsterdam stressed importance of data protection officers and good-faith efforts to comply with GDPR. **Dave Lefort** has more.

Regulators who spoke at the recently concluded Compliance Week Europe conference in Amsterdam acknowledged businesses were still very much in the "awareness" phase of implementation of the EU's complex new set of data privacy rules, but that doesn't necessarily mean they're shielded from sanctions.

In fact, data protection authorities (DPAs) from at least 23 of the 28 EU member states have issued fines under the General Data Protection Regulation, three of which have topped $50M. The exact number of actions is not known, but it's more than 100.

The question you might be asking, then, is if you're among the many organizations still trying to fully grasp the rules and wrap your head around all of the data your organization collects, should you expect the "carrot" of guidance from regulators or the "stick" of enforcement if you've been found to be in violation?

"If there is a complaint, we're going to investigate," insisted Ventsislav Karadjov, deputy chair of the European Data Protection Board and chairman for the Bulgarian DPA. "We cannot say there is a grace period and we're not going to sanction you. If the infringement is very severe, and it concerns a lot of people, the remedy for these people would be a sanction.

"But if we identify that the [data] controller is responsible and has done his (or her) utmost to be compliant, then there is a good opportunity that the controller is not sanctioned, but with some of the instruments of the regulation will be advised what to do, how to do it, and be prescribed a period of time to take actions. After that time, if he doesn't undertake the actions, he'll be sanctioned."

In other words, if you can prove you've demonstrated a good faith effort at implementing the rules and understanding which data is collected across your organization and for what purpose, you're much more likely to get the carrot than the stick.

Ali Shah, the head of technology policy for the U.K.'s DPA, the Information Commissioner's Office (ICO), took issue with the carrot versus stick characterization, saying it's "more nuanced" than one or the other, but agreed with the idea that the more you can show efforts to protect data across your organization, the better you'll be viewed in the eyes of regulators.

"If a complaint comes in or we determine there's an issue, we need to investigate and to understand," said Shah. "Sometimes the answer is talking to the organization and advising them on how to resolve the issue. Or, depending on the nature of the issue, it could lead to a compulsory audit, stop notices, fines—all of the range of enforcement powers."

Specifically, regulators will look at whether you're taking a mature approach to how you manage data.

"We understand it's a journey, but what we won't accept is that the work is not being done in all parts of the organization to try and become more mature," Shah said. "You have to be on that journey and demonstrate that."

Empower your DPO

An engineer by trade with a specialty in machine learning, Shah has been with the ICO for just over nine months and brings a valuable outsider's perspective. He said a company's data protection officer (DPO)—a role required for every company impacted by the GDPR—is critical, and that whoever fills those

shoes needs to be empowered by their organization's leadership in order to be truly effective.

"It's a tough environment," Shah said. "Not only do you have to wrestle with what the law says, but you also have to go and convince your leadership about why this matters, alongside all of the employees who are dealing with your customers and the different ways that your customers might be interacting with you. That can feel like a tall order."

It's an especially tall order without headline-grabbing enforcement actions that can scare senior management into empowering the compliance function. The ICO has issued the two biggest fines under the GDPR so far—£183 million (U.S. $230 million) for British Airways and £99 million (U.S. $124 million) for Marriott—both in the wake of massive data breaches. Aside from those two, there haven't been the kind of big fines many predicted for 2019. Thus, DPOs in some organizations face an uphill battle in their quest both to take stock of all the data the company holds on customers (and whether they need to hold it) and to implement the data protection measures required by the GDPR.

Shah's advice for DPOs: "Start to make the rest of the organization understand it's no longer possible to tick compliance and have it rest just on the data protection officer. This has to go upwards and downwards and across the board. Raising awareness within the organization about why it's necessary for everything from product and engineering, through to the InfoSec security teams through to the leadership. Being aware of the intrinsic nature of personal data in your business and what risks that might carry if there is noncompliance, that's important."

Find your data privacy champions

That perspective was backed up by Angela Bardenhewer, the DPO at Fusion for Energy, an EU institution that is governed by a slightly different set of rules from the GDPR but that is generally very similar.

She pointed out most of the principles of the GDPR are not new, "but what has really been changed is this shift of culture" that is required.

Her strategy is to delegate across her firm to create data privacy coordinators across all silos of the business—HR, finance, procurement, product management, etc.—and hold them accountable. It's a strategy endorsed by Shah and Karadjov wholeheartedly.

"If you identify like-minded people in product and engineering and elsewhere, they will act as your champions because they will feel motivated," Shah said. "Fundamentally, most people just want to do the right thing, but they're not necessarily going to get energized by conversations about compliance. But they will get energized if you say, 'Let's work on your product idea and try and [figure out] how you can achieve what you want to achieve with your innovation but make sure it fits on what we all have agreed as a society about the laws that represent us.' "

During the panel discussion, Karadjov briefly took off his regulator hat and put himself in the shoes of a DPO, offering examples of the questions he'd ask his company and how he would approach one of the most difficult jobs in compliance. "First thing is, you need to have a clear understanding of all of the activities of the business," he said. "You have to understand that clients are data subjects as well. What is the minimum data you need to provide the service you're providing? DPOs should talk to departments to see if [the personal data] they are collecting is reasonable. Is it excessive? Keep in mind, every data subject may request this data to be deleted.

"Second, you have to know what every department is doing, what data they are collecting, for what purposes, to whom they are delivering the data outside the organization, and why they are doing it. And you have to document all of this."

It's a daunting task, but one Karadjov explains will benefit the company in a number of ways. Not only will the DPO be able to create a comprehensive data blueprint and perform a risk assessment for each department, but he or she will also be able to respond promptly to data subject requests: "You'll immediately know on what legal grounds you are processing this data and can immediately respond instead of doing the analysis on each request." ■

What we can learn from the biggest GDPR fines so far

Recent fines for GDPR violations levied on British Airways and Marriott offer a look at where GDPR is headed. **Neil Hodge** reports.

Following the first major GDPR-related financial penalty against internet giant Google, the world waited with bated breath for the next major fine to dwarf the €50 million (U.S. $56.3 million) France's data regulator meted out in January 2019.

That wait came to an end in July, when the U.K. Information Commissioner's Office (ICO) fined British Airways £183.4 million (U.S. $230 million) and Marriott £99.2 million (U.S. $124 million) on back-to-back days for data breach-related violations—the two largest issued under the EU's data regulation so far.

The British Airways penalty resulted from data breach that saw around 500,000 customers' details—including log in, payment card, and travel booking information—being diverted to and harvested by a fake Website between June and September 2018. Marriott's cyber-breach originated in another hotel chain that Marriott subsequently bought. It appears that IT security vulnerabilities may have been present as far back as 2014 when the Starwood hotels group's IT systems were first compromised—some two years before Marriott acquired the company. Around 339 million guests' personal details were leaked.

And, because the breach was reported to the ICO in November 2018—once the GDPR regime was up and running—Marriott's coffers were hit much harder for the company's failure to carry out appropriate due diligence post-acquisition. Under the previous Data Protection Act, superseded by the GDPR in May 2018, the maximum penalty was just £500,000 (U.S. $627,000). Marriott was therefore handed a fine nearly 200 times larger for reporting a 4-year-old breach 6 months late.

Takeaways from the ICO's fines

Michael Hughes, a partner at Haines Watts and non-executive director at cyber-security firm CyberQ

Group, says the Marriott case is a stark warning to companies to check not only their own data protection protocols and controls, but also those of third parties. "Organizations are finding it a challenge to ensure GDPR compliance internally, and there is a significantly greater challenge to obtain assurance that their full supply chain is GDPR compliant," says Hughes.

Both British Airways and Marriott are contesting the penalties. The ICO is taking views from other EU data protection authorities to see whether its judgment and penalty are in line with EU guidelines. To overrule its decision, two-thirds of data regulators represented by the European Data Protection Board (EDPB), the body that reviews and provides guidance about how the GDPR should be applied across the European Union, need to agree that the original penalty or finding was incorrect. The process can take up to 16 weeks to complete. According to an ICO spokesperson, the process is ongoing.

Nicola Howell, senior compliance and EU privacy attorney at Dun & Bradstreet, says both have justification to feel they got a raw deal. "BA was externally hacked, and no customer suffered any financial loss, yet it has received the biggest GDPR fine to date—four times more than Google's," she says. "Marriott, on the other hand, has been fined massively for IT security failings that were present before it even bought the company. It's hard not to feel some sympathy for either of them."

Howell is also unsure whether the penalties issued will be reduced on appeal. "It's a tough call," she says. "If the fines are reduced—especially by a significant margin—then there is a question mark about the regulator's credibility. The main problem, however, is that there is no detail within the penalty notice as to how the figures were arrived at, which makes it difficult to assess how a penalty is commensurate with the level of neglect or control failures and the harm caused."

Emma Roe, partner and head of commercial at law firm Shulmans, says while the ICO "is not going to let an organization off the hook for the breach being the work of an external party or because that organization is the victim of a criminal hack," she believes British Airways' fine has been set lower than the maximum of 4 percent of turnover because it was a result of an external hack rather than an internal leak.

"Clearly, the ICO has left itself room to issue bigger fines when it finds culprits with even less of a handle on their data use and security," she says.

Karl Foster, legal director at U.K. law firm Blake Morgan, says that "the fines are no longer just about security breaches, but failures of transparency and failures to follow procedures. It is notable that the headline fines have been levied at multinationals with deep pockets and recognizable brands." In 2018, the ICO handed out £3M (U.S. $3.76M) in fines. This July alone it handed out over £280m (U.S. $351M) worth.

Some have expressed surprise that it is a "traditional" company that has been the most severely penalized first. "By announcing its intention to issue a record fine to a company outside the technology sector, the ICO is putting businesses on notice that GDPR enforcement is coming for all manner of organizations in all sectors," says Tim Hickman, data protection lawyer and partner at global law firm White & Case.

While the ICO has "greatly surpassed" all other EU supervisory authorities in levying fines under the GDPR, Robert Lands, partner at the law firm Howard Kennedy, says the regulator's new-found reputation as Europe's highest fining enforcer could be short-lived.

"In future it is likely that record-breaking fines toward the maximum end of the range will go to severe breaches by companies whose business models rely on the exploitation of personal data, such as some of the well-known tech giants," says Lands. "It's quite likely that the record set by BA this summer will be dwarfed before long."

Lawyers generally expect an uptick in the number of GDPR penalties from now on, pointing out it has taken regulators probably more time than they realized to process GDPR complaints, particularly those involving large companies. The British Airways case, for example, took almost 14 months to complete and provide notice of a fine. According to Foster, as of April this year, data regulatory authorities had resolved only 52 percent of the backlog of cases under the GDPR. ■

GDPR enforcement varies widely by country

Below is an exploration into how various countries manage consumer data.

The introduction of the GDPR has seen a general increase in complaints and breach notifications, though this does not mean that data protection rules have been broken. Simply, growing awareness has resulted in an uptick of reports and a responsibility by regulators to review them and investigate where necessary.

According to the European Data Protection Board (EDPB), the body that reviews and provides guidance about how the GDPR should be applied across the EU, there were 281,088 cases logged by the various supervisory authorities in the first year of the GDPR's application. Of these, 144,376 related to consumer complaints and 89,271 related to data breach notifications by data controllers. The Netherlands, Germany, and the United Kingdom reported the largest number of breaches, respectively; Liechtenstein, Iceland, and Cyprus reported the lowest. The three areas that have been subject to the most consumer complaints are telemarketing, promotional emails, and CCTV/video surveillance.

Yet, according to law firm DLA Piper's "GDPR Data Breach survey" released in February, just 91 GDPR fines had been handed out across the European Economic Area within the first eight months of the GDPR coming into force. That figure has now risen—but not by much, say experts. The EDPB's February 2019 report to the European Parliament indicated 11 countries had imposed GDPR fines totaling approximately €56 million (U.S. $63 million)—including the €50 million (U.S. $56.3 million) levied against Google by France's CNIL.
Most EU countries have issued fines under GDPR (those that have not are Ireland, Czech Republic, Denmark, Finland, Italy, Slovakia, and Slovenia). For the most part, the quantum to date has been in keeping with the old regime, meaning relatively modest penalties. Leaving aside headline cases, up until this February the average fine levied was around €66,000. That figure will likely go higher once the BA and Marriott fines are accounted for.

Determining which countries are the toughest enforcers depends on one's viewpoint. Before mid-July, the United Kingdom hadn't issued a single fine; now it's in pole position with a penalty tally over four times more than the rest of Europe put together. A lot depends on the approach of each supervisory authority. Many have preferred to educate and cooperate, rather than punish, using the GDPR's first year as a grace period to promote compliance (Belgium, Cyprus, Finland, and Latvia are some examples). Some, like Austria, have decided to target general, low-level abuses that could apply to a wider range of organizations, rather than aim for big tech firms as a priority. For example, in September 2018, the Austrian supervisory authority, the DSB, fined a sports betting café €5,280 (U.S. $5,900) for installing a CCTV camera that recorded passers-by, in contravention of the GDPR's ban on large-scale monitoring of public spaces.

Some of the more severe penalties to date have focused on technology misuse at one end of the spectrum and general data sloppiness at the other. For example, the national soccer league in Spain, La Liga, was fined €250,000 (U.S. $280,000) for offering an app which—without their knowledge or consent—accessed the microphones of users' mobile phones for the purpose

of detecting whether pubs that were screening soccer matches had actually paid a fee to do so. Meanwhile, a Portuguese hospital was fined €400,000 (U.S. $449,000) after an investigation revealed the hospital's staff, psychologists, dieticians, and other professionals had unlimited access to patient data through false profiles. A subsequent audit carried out revealed that the hospital had 985 registered doctor profiles despite only having 296 doctors. Elsewhere, in September the Polish DPA hit electronic goods retailer Morele.net with a €645,000 fine for lacking the appropriate organisational and technical safeguards to prevent a breach that affected 2.2 million people from occurring, or from being able to respond adequately once it unfolded.

As of this summer, Germany's 16 data supervisory authorities have been the most proactive enforcers, handing out a total of 75 fines since the GDPR was implemented. The first was in November 2018, when the LfDI Baden-Württemberg fined the social media platform Knuddels €20,000 (U.S. $22,000) for storing passwords in plaintext, following a data breach in which approximately 330,000 users' personal data was compromised. The Baden-Württemberg authority also issued an €80,000 (U.S. $89,000) fine to a healthcare organization that exposed sensitive personal data—at the time the highest penalty imposed (since eclipsed this October by the Berlin Commissioner for Data Protection and Freedom of Information, which issued a fine of around €14.5 million (U.S. $16.1 million) against German property company Deutsche Wohnen for using an archive system to store tenants' personal data indefinitely, and without providing the possibility for them to ask for personal information to be removed or deleted when it was no longer necessary to hold onto it. The penalty was Germany's first multimillion euro fine for a GDPR violation).

Hungary, meanwhile, has handed out the largest fine in respect to proportion of an organization's turnover. The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) issued a HUF 30,000,000 fine (U.S. $103,000) to the organizers of the Sziget multicultural music and arts festival over their security procedures, which involved photocopying IDs of hundreds of thousands of festival-goers and taking photos at the entry gate. The penalty represented 2.3 percent of the company's net revenue.

While the Netherlands has issued very few fines, it has dealt out one sizeable, high-profile one. In 2018, the Dutch Data Protection Authority hit taxi-app firm Uber with a €600,000 (U.S. $673,000) penalty for "violating the Dutch data breach regulation" by failing to inform the regulator within 72 hours of discovery it had suffered an unauthorized breach that affected 57 million Uber users worldwide (of which 174,000 were Dutch citizens). It also came to light that Uber had paid the attackers $100,000 to destroy the data, which included the names, e-mail addresses, and telephone numbers of customers and drivers they had downloaded.

Karen Holden, founder of London legal practice A City Law Firm, says GDPR regulators have generally set out several conditions considered when issuing fines, such as the nature of the infringement (external hack, negligence, or both); what type of data was compromised; what actions were taken; and how cooperative the company was with regulatory and authoritative entities. "It is clear that each case is judged on its own merits and is very much dependent on the facts of each case," says Holden. "In the case of Knuddels in Germany, for example, the company was spared a much harsher penalty due to its effective strategy in responding to and dealing with the data breach," she says.

—Neil Hodge

Country-by-country look at GDPR enforcement trends

Below is a look at countries' data privacy protocols in response to the U.K. General Data Protection Regulation as of July 2019.

Austria

Austria operates a system whereby first breaches of the GDPR can basically only be sanctioned by a warning—the Austrian DPA only imposes fines from the second breach onwards. By the first anniversary of GDPR, the regulator had handed out just three fines, all of which involved illegal video surveillance. And the penalties were all relatively lenient, ranging from €300 to €5,280 (U.S. $333 to $5,858).. That has since changed, however. In October the Austrian DPA imposed an administrative fine of €18 million (U.S. $20 million) on Österreichische Post, the country's largest postal service, for processing personal data based on the subject's alleged political affinity, and for also using customer data relating to the number of packages they received (or were relocated) to inform the company's direct marketing efforts.

Denmark

Even before May 25, 2018, it was clear that the Danish DPA would not impose large-scale GDPR fines from the beginning, as Danish constitutional law means that the regulator cannot issue penalties under the new data rules until the Danish courts have established an adequate level for fines for the various types of breach of GDPR. However, the Danish DPA has referred one particular case to the Danish Prosecution Service. Following an inspection visit at a Danish taxi company, the Danish DPA found that it had stored personal data (mainly phone numbers) from approximately 9 million taxi rides without a legitimate reason. Consequently, the Danish DPA has suggested a fine of DKK 1.2 million (U.S. $180,000) be imposed.

France

The French Data Protection Authority (CNIL) imposed a €50 million (U.S. $56.3 million) GDPR fine on Google on Jan. 21 for two counts of violating data protection rules. It was found that the internet giant failed to provide adequate transparency information to individual users and failed to provide a valid lawful basis for the processing of user data as the consent it had obtained did not meet the enhanced requirements of GDPR. Other large fines that the regulator has handed out include Bouygues Telecom (€250,000; U.S. $280,000), Uber (€400,000; U.S. $449,000), Dailymotion (€50,000; U.S. $56,000) and Optical Center (€250,000; U.S. $280,000)—all of which relate to a lack of technical measures securing client data. Generally, however, the CNIL has not yet imposed fines as vigorously and as widely as many people feared: instead, it has preferred to provide information, guidelines, e-learning training and various tools about the new regulation on its Website. It has also treated smaller companies with more leniency. Complaints to the CNIL have increased by 32.5 percent compared with 2017.

Germany

In Germany, the DPAs are organized on a German state level, which means that there are 16 data regulators. In total, German DPAs have issued 75 fines since the GDPR was implemented, totaling just €449,000 (U.S. $504,000)—the largest single fine being €80,000 (U.S. $90,000) to a healthcare organization that exposed sensitive personal data.

Latvia

The Latvian DPA did not impose many penalties during the first year of GDPR application. The biggest publicly announced fine was only €2,000, which is even smaller than the penalties imposed before the GDPR started to apply a year ago. However, there are a couple of reasons for this: firstly, the regulator said that it wanted to consult and help organizations comply, rather than punish them (an approach taken by several other EU data authorities, such as Belgium, Bulgaria, Croatia, Cyprus, and Greece), and secondly, it is overloaded with cases.

Lithuania

The Lithuanian DPA has been quite active. In January 2019 it made public a list of planned inspections announcing the names of 75 organizations that will face GDPR compliance inspections this year. After the investigations are completed, the DPA will provide its recommendations regarding the most common compliance failures.

Netherlands

The Dutch Data Protection Authority has not yet imposed GDPR fines as vigorously as many people feared: it started first and foremost by providing information, guidelines and tools about the GDPR on its website. So far, only one headline fine has been handed out: Uber was fined €600,000 (U.S. $673,000) for failing to comply with the obligation to report data breaches within 72 hours.

Sweden

In August Sweden imposed its first GDPR-related fine (around €20,000, or U.S. $22,000) against a local authority for using facial recognition technology to monitor the attendance of students in school. The school had processed sensitive biometric data unlawfully and failed to do an adequate impact assessment including seeking prior consultation with the Swedish DPA. Other ongoing cases of interest include an investigation into Google's access to the user location data by means of its so-called "Location History" and "Web & App Activity" and how payments services provider Klarna uses customers' personal data.

United Kingdom

The two biggest enforcement actions so far stemming from GDPR violations have come from the U.K.'s Information Commissioner's Office, which fined British Airways £183.4 million (U.S. $230 million) and Marriott £99.2 million (U.S. $124 million) on back-to-back days for data breach-related violations.

Source: Ius Laboris

GDPR showing results, but 'work needs to continue'

The EU's tough new data rules are "bearing fruit," but some member states have still not put the General Data Protection Regulation into action. **Neil Hodge** explores.

The European Commission published an assessment of how the General Data Protection Regulation has been implemented across the European Union. The report concludes most member states have set up the necessary legal framework, and the new system strengthening the enforcement of the data protection rules is falling into place.

It found businesses are developing a compliance culture while citizens are becoming more aware of

To improve General Data Protection Regulation awareness, compliance, and enforcement, the European Commission wants to strengthen the role of data protection authorities by encouraging member states to allocate sufficient resources to them, as well as step up cooperation between them.

their rights. At the same time, convergence toward high data-protection standards is progressing at international level.

The assessment, however, also highlights several areas of concern—namely, that Greece, Portugal, and Slovenia have still not updated their national data protection laws in line with EU rules. The Commission says they "must do so as a matter of urgency," warning that it will use "all the tools at its disposal, including infringement procedures" to ensure member states comply with GDPR and limit any fragmentation of the data protection framework.

To improve GDPR awareness, compliance, and enforcement, the European Commission wants to strengthen the role of data protection authorities by encouraging member states to allocate sufficient resources to them, as well as step up cooperation between them. The European Union's executive body also wants to ensure data regulators apply GDPR in the same manner so enforcement is applied evenly and consistently across the 28-country bloc.

The report has already uncovered some instances where the interpretation of rules around the GDPR are diverging. Some member states, for example, have introduced national requirements on top of the regulation, which the Commission says "leads to fragmentation and results in creating unnecessary burdens."

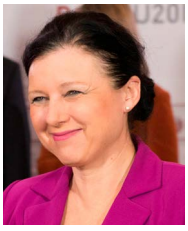
Germany, for example, requires companies with at least 20 employees to designate a data protection officer to be permanently involved in the automated processing of personal data.

The European Commission found privacy rights under the EU data privacy regulation are still misunderstood by both individuals and companies and data requests are dealt with too slowly and not thoroughly enough. It also found that while there have been several representative actions brought by privacy campaigners on behalf of data subjects, even more would have been brought if more member states had allowed such organizations to be able to do so without the need to get individuals to give them a mandate, as is possible under the regulation.

Measuring success

The European Commission has warned, however, that "the success of the regulation should not be measured by the number of fines imposed, but by changes in the culture and behaviour of all actors involved."

It points out that, rather than slapping companies like British Airways, Marriott, and Google with multi-million-Euro fines, data protection authorities have other tools at their disposal—such as imposing a temporary or definitive limitation on data processing, including a ban, or ordering the suspension of data flows to a recipient in a third country.



Jourová

Vera Jourová, European commissioner for justice, consumers, and gender equality, said that "work needs to continue for the new data protection regime to become fully operational and effective."

Companies can expect to learn more in 2020. The European Commission will once again report on the implementation progress of the regulation in the coming year. ■

CONDUENT

DSARs in a Post-GDPR World: The Changing Face of Compliance and Privacy

Joseph Pirrotta, Sr. Director, Legal Product Portfolio

The General Data Protection Regulation (GDPR) is changing the global data privacy landscape and increasing compliance complexities across every industry and sector.

GDPR has ushered in a new era of data rights and data privacy awareness. Data, which was once treated as a commodity, has now been put on a sacred pedestal with restricted access and usage controls. That's good news for consumer privacy — but GDPR compliance comes with its own set of challenges and complexities for today's businesses. Those complexities will continue to grow with other parts of the world adopting similar privacy regulations such as the California Consumer Privacy Act (CCPA) in the United States.

As other countries look to establish the same type of laws around data rights and privacy, there is much they can learn from the challenges and experiences businesses have already faced under GDPR — as well as the compliance hurdles they must continue to navigate and address.

One of the most critical focus areas for organizations in a post-GDPR and CCPA-compliant world is their ability to respond to Data Subject Access Requests (DSARs) more quickly than ever before. A DSAR gives individuals the right to discover what data an organization is holding about them, why the organization is holding that data and to whom their information is disclosed. Failure to respond in a timely manner to a DSAR can result in both negative perceptions about a company's regard for consumer privacy and business-crippling fines as well.

GDPR: A Look Back

The General Data Protection Regulation (GDPR) of 2016 was designed to strengthen and standardize EU residents' data privacy protections and rights over their personal information. The regulation applies to all organizations located in the EU and to any outside it that offer free or paid goods or services to EU residents and/or monitor their behavior.

Once the regulation passed, the EU gave organizations doing business across the EU's 28 member countries until May 25, 2018 to become compliant — but for many, it still felt like a race to the finish due to the complexity of compliance and the evolving nature of personal data.

Implementing a continent-wide data privacy regulation across multiple countries, each with its own sovereign data laws, is a unique task of its own. Even though GDPR is a European law, its ramifications have been felt across the world, with global organizations scrambling to make their websites and marketing GDPR-compliant — while putting in place the right processes and controls for managing how personal data is collected, held, used and "forgotten."

A Broader Definition of Personal Data

According to GDPR, personal data is any information relating to a living, identified or identifiable natural person (The CCPA definition is similar). GDPR broadened the definition of personal data beyond prior EU directives. For example, something that might be thought of as indirect data, such as a User ID, is considered personal data because it can be traced back to a person's name in a database. Similarly, location data and online identifiers such as IP address are types of personal data as well. Moreover, this personal data can reside across disparate systems — located on-premise or in the cloud. The complexity only adds to the variability of the nature of personal data and makes finding it quickly even harder. This challenge can have serious repercussions when it comes to responding to DSARs.

What is a DSAR?

Data Subject Access Requests are rights upheld by the GDPR. They grant a consumer access to the personal data a company is storing about them "on demand." This means an individual can make a request to access all personal information that a company has on them and organizations must comply. The right to a DSAR existed prior to the enforcement of GDPR, but the requirements and burden on organizations to fulfill them were less stringent and specific.

For this reason alone, most GDPR violations are related to non-compliance with DSAR requirements.

RESPONDING TO DSARS: BEFORE AND AFTER GDPR

BEFORE

1. Organization has up to 40 days to respond
2. Organization may charge a fee for the report
3. Organization could dictate how requests were made
4. Organization could generally avoid heavy fines for non-compliance – with max being €500,000 ($554K USD)
5. People could request any type of data

AFTER

1. Organization has up to 30 days to respond
2. Reports are free to the consumer in almost all cases
3. Requests can be made electronically or via physical mail
4. Max penalty for violations up to €20m ($22M USD) or 4% of global revenue
5. Organization now has the right to withhold data if it obstructs a legal inquiry or to protect the rights of others

With less time to respond to DSARs and the inability to charge the requester for their time and resources, businesses now have to organize and catalogue information much more efficiently for quick identification of personal information. This has resulted in additional costs such as new technology and staff training.

What's a data map?

A data map sources data fields to their related target data across multiple platforms and systems. Creating a good data map is essential to effectively navigate DSARs, especially those requiring multiple, disparate data systems and types of data (structured and unstructured, sensitive vs. non-sensitive). Knowing where each piece of data resides and the relationship between different data points is the first step to creating a good data map.

- **Faster access to data**
- **Ease of data segmentation**
- **Avoid delinquency fines or lawsuits**

The High Price of Non-Compliance

Recent high-profile cases on non-compliance with DSARs, resulting in fines up to $230M USD, demonstrate both the importance of complying with GDPR and the tremendous burden that compliance officers bear in this new regulatory environment.

Data privacy enforcement risk is now among the top risks a company must consider as part of its enterprise risk management framework. With fines as high as 4% of global revenue, compliance and data protection officers have taken on even more pressure since the launch of GDPR.

It's worth noting that, according to ICO data, the mishandling of DSARs is the #1 data protection issue complaint today at 42%. Complaints typically focus around one of two issues – either the report was not delivered on time or it provided incomplete information.

Responding to employee DSARs, in particular, can be one of the most challenging tasks for an organization because employee data is usually intermingled with highly sensitive information which requires surgical precision to extract. That's why it is critical for organizations of all kinds to create accurate and effective data maps — something Conduent has helped several companies do using our Analytics and Consulting capabilities.

Conduent is Helping Organizations Comply with DSAR Requirements

In the post-GDPR world, organizations and compliance leaders have quickly realized that compliance is often a full time job — particularly as it relates to DSARs. Conduent's Analytics Solutions have helped many of our clients stay on top of requirements including a major packaging company.

This packaging company approached Conduent with a challenge of reviewing and responding to a set of 25 DSARs. The project included approximately 6,000 documents that had to be reviewed and redacted separately for each request. By first applying our Analytics and Search capabilities to drastically reduce the overall document volume — and then scaling up our staffing from a team of 20 to 75 reviewers, Conduent successfully delivered the data for all 25 DSARs in a mere six days. This helped our client complete their reports well ahead of schedule with minimal disruption to daily operations.

Since that first engagement, the Conduent team has reviewed an additional 13 requests, again using our automated Analytics and Search tools to reduce the document volume from 5.5M to approximately 100K and then using our customized workflow developed with the client to deliver exactly what the client needed.

To avoid any accidental data disclosures, part of the Conduent team's workflow is to review the data set upfront for all details of the requestor such as designation, location, associated employee numbers, etc. and verify with the client that the details match with the requestor. Daily status reports and diligent tracking have allowed the Conduent team to stay in lockstep with the client, ensuring that all steps in the process continue along as planned — and any red flags are noted before they become compliance liabilities.

About Conduent

Conduent delivers mission-critical services and solutions on behalf of businesses and governments — creating exceptional outcomes for its clients and the millions of people who count on them. Through people, process and technology, Conduent solutions and services automate workflows, improve efficiencies, reduce costs and enable revenue growth. It's why most Fortune 100 companies and over 500 government entities depend on Conduent every day to manage their essential interactions and move their operations forward.

Conduent's differentiated services and solutions improve experiences for millions of people every day, including two-thirds of all insured patients in the U.S., 10 million employees who use its HR Services, and nearly nine million people who travel through toll systems daily. Conduent's solutions deliver exceptional outcomes for its clients including $16 billion in medical bill savings, up to 40% efficiency increase in HR operations, and up to 40% improvement in processing costs, while driving higher end-user satisfaction. Learn more at www.conduent.com.

Conclusion

The importance of responding to and complying with the requirements of DSARs cannot be overemphasized. As we've seen with some major companies since the implementation of GDPR, the impact on businesses can be enormous if part of the process is held up or mishandled — and the law takes no excuses. With CCPA now in effect, the pressure on compliance officers will only continue to grow.

It's critical for today's businesses to have an internal policy around DSARs, resources to support responses and an infrastructure in place to help handle spikes in volume. That infrastructure may draw from internal resources, but also having an outsourced partner to help with large requests and DSAR spikes is a wise choice. In this way, organizations can ensure compliance at every turn while employees have more time to focus on good data management and mapping practices. In doing so, they help protect their organization from risk and reinforce its reputation as a masterful steward of data — and a brand consumers and business partners can trust.

To learn more about how Conduent can help your business succeed, visit **conduent.com/legal-and-compliance**

CONDUENT

Ireland vs. Big Tech: The wait continues

Dave Lefort explores Ireland's reticence to enforce GDPR.

We live in an era in which instant updates and instant analysis are valued above all in what's become a 24-hour, nonstop news cycle.

Forgive me, then, for getting a bit antsy as we pass the 18-month mark since the European Union's General Data Protection Regulation (GDPR) went into force and we've seen very few precedent-setting actions taken by data protection authorities (DPAs). Of the 28 EU member states, at least 23 have issued fines for violations of the GDPR, but there's been one country notable in its absence from that list: Ireland.

Why is the world keeping such a close eye on the Emerald Isle? It is the European home (and data privacy regulator of record) to some of the United States' biggest technology companies: Google, Facebook, and Twitter, to name a few. It has historically been kind to Big Tech, which begs the question of how it will handle potential violations of the GDPR.

Major tech firms are the subject of at least 19 investigations into potential GDPR violations by the Irish Data Protection Commission, including at least 10 probes into the practices of Facebook alone. Both Google and Facebook have tangled with governments over their alleged abuse of the personal data of their users, but never has a regulator been in a position to make as big an impact on one of these company's bottom lines as Ireland is.

The maximum fine for a GDPR violation is 4 percent of a company's annual turnover, which means for a company like Facebook, for example, it could be up to $2.2 billion (4 percent of the company's annual revenue in 2018). That's far from the pocket-change $643,000 it was penalized by the U.K.'s DPA for the Cambridge Analytica data scandal, which predated the GDPR.

Why such a long wait, then? Could it be that a reluctant Ireland is dragging its feet? Sure … but there could also be another explanation.

"We have to aim first, not shoot."

That's a quote from Ventsislav Karadjov, deputy chair of the European Data Protection Board, speaking at the recently concluded Compliance Week Europe conference. He said it not about Ireland in particular but on the general importance of letting the investigative and enforcement processes play out at their own pace.

His point was that every enforcement action taken for General Data Protection Regulation violations is going to be heavily scrutinized not only by the business community but more importantly by the courts. And that means every case they make needs to be airtight.

"It's very important that everything is done by procedure under the law," he explained. "We have to prove each of the actions taken. If we don't, we are at risk that when companies go to court, we'll lose the case. And if that happens, we'll lose credibility as a regulator and credibility in the eyes of data subjects."

Sounds logical, even if we're still wary about Ireland's appetite to pick a fight with Big Tech. ■

German telecom fined for GDPR abuses; fights back

A German federal privacy watchdog fined 1 & 1 Telecom €9.55 million (U.S. $10.6 million) for GDPR violations, but the company won't accept the penalty. **Jaclyn Jaeger** reports.

A German federal privacy watchdog announced it has fined telecommunications service provider 1 & 1 Telecom €9.55 million (U.S. $10.6 million) for violations of the EU's General Data Protection Regulation. The organization argues that it won't accept the penalty and will file a lawsuit.

The fine against 1 & 1 Telecom is one of the largest to date under the GDPR, put into effect in May 2018. In July 2019, British Airways was hit with the largest penalty thus far, a £183.39 million (U.S. $230 million) fine stemming from the compromised data of nearly 500,000 customers. That same month, Marriott International's faced a £99.2 million (roughly U.S. $124 million) fine for a data breach that exposed the data of 339 million guest records globally.

The 1 & 1 Telecom fine is the second largest brought by a German data regulator, behind a €14.5 million (U.S. $16.1 million) penalty assessed upon property company Deutsche Wohnen SE in October by the Data Protection Authority of Berlin regarding privacy violations in the archiving of tenant data.

In the 1 & 1 Telecom case, according to the Fed-

"The security of millions of customers' data is our top priority. Therefore, 1 & 1 adheres strictly to the applicable data protection regulations. The fine is absolutely disproportionate." *(English translation)*

Julia Zirfas, Data Protection Officer, 1 & 1 Telecom

eral Commissioner for Data Protection and Freedom of Information (BfDI), 1 & 1 Telecom had not taken "sufficient technical and organizational measures" to prevent unauthorized persons from obtaining information on customer data. The BfDI said it became aware callers to 1 & 1 Telecom's call center could obtain extensive information on personal customer data simply by getting the customer's name and date of birth. Such an authentication procedure violates Article 32 of the GDPR, which requires taking appropriate technical and organizational measures to systematically protect the processing of personal data.

1 & 1 Telecom has cooperated in the investigation. For example, the company introduced a new authentication procedure, which the BfDI said has been significantly improved in terms of technology and data protection, in consultation with the regulator.

Despite these measures, the BfDI said the imposition of a fine was necessary. In assessing the amount of the fine, the BfDI credited 1 & 1 Telecom's cooperative behavior throughout the proceedings.

More to come?

In a separate case, the BfDI said it has fined Internet service provider Rapidata €10,000 (U.S. $11,100) for failing to designate a data protection officer in violation of Article 37 of the GDPR. Regulators said the amount of the fine reflected Rapidata's failure to comply with repeated requests but also took into consideration that it's a small business.

"Data protection is a fundamental right," said Federal Commissioner Ulrich Kelber in a translated release. "The fines are a clear sign that we will enforce this protection of fundamental rights."

On an industry-wide level, more fines may be forthcoming. Based on its own findings, information, and customer complaints, the BfDI said it is also investigating the authentication processes of other providers of telecommunications services.

1&1 Telecom's response

In a translated response statement, the company said it "will not accept the fines" and plans to file a lawsuit. "This procedure was not about the general protection of data stored in 1 & 1, but about how customers can access their contract information," the company said.

The case in question occurred in 2018 and concerned a telephone query of the mobile number of a former partner. "The responsible employee fulfilled all the requirements of the then-valid 1 & 1 security guidelines," the company stated. "At that time, two-factor authentication was common, and there was no single market standard for higher security requirements."

Since then, 1 & 1 has continued to enhance its security requirements. For example, a three-level authentication has been introduced, and 1 & 1 says it will soon provide each customer with a personal service PIN. "The security of millions of customers' data is our top priority," said Julia Zirfas, an attorney and the company's data protection officer. "Therefore, 1 & 1 adheres strictly to the applicable data protection regulations."

"The fine is absolutely disproportionate," Zirfas added. ■

British Airways faces record-setting GDPR fine

British Airways was hit with the biggest GDPR fine ever from the ICO for a September 2018 fraud. **Joe Mont** reports.

British Airways was hit in July with the largest penalty to date under the European Union's General Data Protection Regulation, a £183.39m (U.S. $230 million) fine stemming from the compromised data of nearly 500,000 customers. The nearly quarter-billion-dollar penalty, announced by the U.K.'s Information Commissioner's Office (ICO), amounts to nearly 1.5 percent of British Airways' annual revenue for the financial year that ended Dec. 31, 2017.

The fine relates to a cyber-incident notified to the (ICO) by British Airways in September 2018. This incident in part involved user traffic to the British Airways Website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers was compromised in this incident, which is believed to have begun in June 2018.

The ICO, in a statement, said its investigation "found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information."

"People's personal data is just that: personal. When an organization fails to protect it from loss, damage or theft it is more than an inconvenience," said Information Commissioner Elizabeth Denham. "That's why the law is clear. When you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."

British Airways has cooperated with the ICO investigation and has made improvements to its security arrangements since these events came to light, the ICO statement adds.

The ICO investigated this case as lead supervisory authority on behalf of other EU member state data protection authorities and in consultation with other regulators. Under the GDPR "one stop shop" provisions, the data protection authorities in the EU whose residents have been affected will also have the chance to comment on the ICO's findings.

"We are surprised and disappointed in this initial finding from the ICO that it intends to issue the airline with a penalty notice," responded Alex Cruz, British Airways' chairman and chief executive. "[We] responded quickly to a criminal act to steal customers' data. We have found no evidence of fraud/fraudulent activity on accounts linked to the theft. We apologize to our customers for any inconvenience this event caused."

"British Airways will be making representations to the ICO in relation to the proposed fine. We intend to take all appropriate steps to defend the airline's position vigorously, including making any necessary appeals," added Willie Walsh, chief executive of parent company International Airlines Group.

According to an ICO spokesperson, the process is ongoing. ■

Marriott reveals $124M GDPR fine for data breach

The U.K. Information Commissioner's Office intends to fine Marriott about £99 million (U.S. $124M) for GDPR abuses. **Joe Mont** has more.

Following what the agency termed "an extensive investigation," the Information Commissioner's Office (ICO), the U.K.'s independent regulator for data protection and information rights law, has issued a notice of its intention to fine Marriott £99,200,396 (roughly U.S. $124 million) for infringements of the General Data Protection Regulation.

The ICO was notified by Marriott in 2018 of a cyber-incident that led to the proposed fine. A variety of personal data contained in approximately 339 million guest records globally was exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area. Seven million of the affected files were related to U.K. residents.

The vulnerability is believed to have begun when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott "failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems."

"The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected," U.K. Information Commissioner Elizabeth Denham said in a statement. "Personal data has a real value so organizations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."

Marriott has cooperated with the probe and made improvements to its security arrangements since these events came to light, the ICO said. The company will have an opportunity to make representations to the ICO as to the proposed findings and related fine.

"We are disappointed with this notice of intent from the ICO, whi ===ch we will contest," said Marriott International President and CEO Arne Sorenson in a statement. "We deeply regret this incident happened. We take the privacy and security of guest information very seriously and continue to work hard to meet the standard of excellence that our guests expect."

The Marriott announcement came one day after British Airways was hit with the largest penalty to date under the GDPR, a £183.39m (U.S. $230 million) fine stemming from the compromised data of nearly 500,000 customers.

Also, the ICO published an annual report that cites an "unprecedented year" for the regulator. In the report, the ICO notes that the number of data protection complaints it received nearly doubled, increasing from 21,019 in 2017-2018 to 41,661 in 2018-2019 (covering 12-month span that ended March 31).

According to an ICO spokesperson, the process is ongoing. ■

French real estate firm slammed with GDPR fine

France's data watchdog CNIL levied a notable fine on real estate services provider Sergic. **Jaclyn Jaeger** reports.

French data protection authority CNIL on June 6 levied a €400,000 (U.S. $453,000) fine on Sergic, a French real estate services provider, for failing to adequately protect the data of users of its Website and for implementing inappropriate procedures for storing data in violation of the EU's General Data Protection Regulation.

Sergic operates a Website where users can create a file to apply for a rental and upload supporting documents. In August 2018, the CNIL received a complaint from a user of the site who was able to access, from his personal space on the Website, documents saved by other users by slightly modifying the URL displayed in the browser.

In 2018, the CNIL conducted an online check, which found that documents sent by the applicants for rentals were freely accessible without prior authentication. These documents included copies of identity cards, vital cards, tax notices, certificates issued by the family allowance fund, divorce decrees, and account statements and bank account details, the CNIL said.

The CNIL said it alerted Sergic to the existence of this lack of security and subsequent violation of personal data. A few days later, the CNIL said it carried out an on-site inspection at Sergic and discovered the company had been aware of the issue since March 2018 but did not resolve it until September 2018.

GDPR violations

Based on these findings, the CNIL found two breaches of the GDPR. First, the CNIL found that Sergic failed in its obligation to preserve the security of the personal data of the users of its Website in violation of Article 32 of the GDPR.

The company had not put in place a procedure to authenticate users of its Website to ensure that the persons accessing the documents were the ones who had uploaded them, a basic measure. This failure was further aggravated by the nature of the data made available and by the company's lack of diligence in correcting it. Specifically, the company did not resolve the security issue until six months later and did not take any emergency measures to limit the impact of the issue in the meantime, the CNIL said.

Secondly, Sergic kept all the documents that were uploaded by candidates for a duration that was longer than necessary for the purposes of the processing. The CNIL noted that, once the purpose for processing is achieved—for example, the management of the applications—the data must be deleted or, at least, archived in a separate database if it needs to be retained for compliance with legal obligations or for dispute management purposes. Here, again, the duration of this archiving must be limited to what is strictly necessary, the CNIL said.

In imposing the €400,000 fine on Sergic, the CNIL said it took into consideration the seriousness of the breach, the lack of diligence by the company in addressing this vulnerability, and the fact that the accessible documents revealed private aspects of the applicants' lives. It also took into consideration the size of the company and its financial strength. ■

Conduent Legal & Compliance Solutions

Let's move insights forward

Legal, risk and compliance departments are challenged to become more proactive, efficient, and data-driven. We deliver mission-critical legal and privacy solutions that enable better outcomes, deliver smarter insights and can help you achieve a 50-90% ROI.

Learn more at conduent.com

CONDUENT