Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Data privacy issues back in the spotlight

An e-Book publication sponsored by exterro

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

exterro

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today as we deliver a fully integrated Legal GRC platform that enables our clients to address their regulatory, compliance and litigation risks more effectively and at lower costs. With software solutions that span privacy, legal operations, compliance, cybersecurity and information governance, Exterro helps some of the world's largest organizations work smarter and more efficiently. For more information, visit exterro.com.

Inside this e-Book

GDPR defined by mixed signals, unbalanced enforcement

Two years into the GDPR, we still don't know how lingering questions about compliance will be answered going forward. **Neil Hodge** has more.

The world's most stringent privacy law, the European Union's General Data Protection Regulation (GDPR), turned 2 years old on May 25. In those 24 months, the rules have put data privacy compliance on every board's agenda and have given Big Tech notice that their activities—and revenue streams—are under review.

Yet while companies have made great efforts to comply with the regulation, many feel they still do not fully understand what it requires of them. Instead, many organizations are more acutely aware of the potential draconian punishments awaiting them if they mismanage data or fail to protect it properly.

Compliance Week takes a look at GDPR enforcement trends and efforts to standardize regulatory approaches so far and how lingering questions about compliance—as well as non-compliance—may be answered going forward.

1. Will enforcement even out across the European Union?
Certainly, regulatory activity in 2019 was higher than in 2018 as data protection authorities came to grips with complaint handling and ground on with their investigations. But, although fines and reported data breaches may have increased last year, commentators generally agree the penalties handed out under the GDPR have not been as harsh as they could have been—for instance, no company has been hit with the headline 4 percent of global turnover fine yet and few expect that to change in 2020. Furthermore, according to data from Privacy Affairs, while there has been a total of 273 GDPR fines imposed through the end of May 2020, totaling €153,525,487 (U.S. $169 million) in penalties, the levels have varied wildly: The single highest fine is still France's €50 million (U.S. $55 million) penalty against Google from January 2019. The lowest fine, however, is just €90, or U.S. $99 (made against a Hungarian hospital). Many fines across the European Union are in the low hundreds of euros—hardly the scary prospect that many companies feared.

According to Privacy Tracker, which monitors GDPR enforcement actions, there have been 347 fines under the regulation, totalling €175,944,866 (U.S. $206,776,565), as of the end of July 2020.

José Luis Piñar, counsel in the Madrid, Spain, office of law firm CMS and a former director of the Spanish Data Protection Agency, says an examination of EU enforcement records shows how varied regulatory approaches can be. For example, while Spain holds the record for the highest number of fines by far as of the end of May, the total amount charged for those penalties is lower than elsewhere in Europe. Similarly, notes information from GDPR Enforcement Tracker, while the Czech Republic and Italy had issued a similar number of fines each by the time the GDPR turned 2 years old (13 and 11, respectively), the total sum is drastically different—some €32,175 (U.S. $35,387) compared to €39.4 million (U.S. $43.3 million). Three countries—Liechtenstein, Luxembourg, and Slovenia—have still not issued any GDPR fines yet, while Estonia, Finland, and Ireland only issued their first GDPR penalties on the eve of the regulation's second anniversary.

At the start of the year there was hope there would be greater harmonization and standardization in the monitoring and enforcement approaches of Europe's data regulators so that companies had greater clarity about data rules and regulators' appetites to police them.

Lawyers and IT experts, however, generally agree that differences in approaches and interpretation among regulators will likely persist for the time being. "I fear that in the medium-term we will continue to see different approaches, even disagreements between EU data protection regulators," says Bojana Bellamy, president of the Centre for Information Policy Leadership, a global data privacy and cyber-security think tank. "Also, national courts will take different views, too, and we will end up with the Court of Justice of the EU [which interprets EU law to make sure it is applied in the same way in all EU countries] deliberating on many more data protection cases. The ambition of having one single GDPR law for the whole of EU is long way ahead," she says.

Experts also agree the COVID-19 pandemic may have slowed progress toward harmonization, too, and that fines could be delayed while key investigations are stalled. For example, the ICO indicated in April it has delayed finalizing British Airways and Marriott's fines and is prepared to give companies more leeway in the way they report and rectify any data breaches while the current worldwide health emergency continues. It also hinted at possible fine reductions given the poor financial state of some companies. Other EU data protection authorities have made similar measures. On May 7, the ICO went further and issued a statement that it would also pause its investigation into real-time bidding and the AdTech industry, saying it was not its intention to "put undue pressure on any industry at this time."

In short, the ICO—one of the biggest and best-resourced data protection authorities in the European Union—tacitly admitted it cannot pursue investigations into what many IT experts and privacy campaigners say are major areas of personal data abuse.

"COVID-19 has changed the world," says Robert Lands, partner and head of IP & commercial at law firm Howard Kennedy. "Regulators have not gone soft. The factor that is most likely to delay big fines is simply that the virus will make it difficult for supervisory authorities to complete their investigations."

According to a report published at the beginning of May by Brave, a tech company that promotes a private browser to protect users' data, half of the EU's data protection authorities have annual budgets of under €5 million (U.S. $5.5 million). Three—Estonia, Malta, and Cyprus—have budgets of less than €1 million (U.S. $1.1 million). It also found that only six of Europe's 28 national data protection authorities have more than 10 tech specialists (Germany, Spain, France, United Kingdom, Ireland, and Greece), while seven authorities have just two tech specialists (or less).

The report says the level of available funding impacts the quality of enforcement. As such, it calls for the European Commission to intervene by launching an infringement procedure against EU member states for failing to provide data protection authorities with adequate budgets—even referring them to the European Court of Justice, if necessary. It also said the European Data Protection Board (EDPB), the EU body charged with overseeing how member states oversee and en-

force the GDPR, should develop an EU unit to assist national data protection authorities in tech investigations.

Some experts believe any relaxation in regulatory scrutiny could inadvertently act as a signal for companies to either ride roughshod over the rules or downgrade the importance of compliance.

"There is always a risk that delays in investigations and outcomes will cause complacency," warns Jane Sarginson, a barrister at St Philips Chambers, while Camilla Winlo, director of data privacy consultancy DQM GRC, says, "There is clearly a danger that organizations facing tough times will interpret any sign that the regulator is relaxing their stance as a signal to reduce their focus on data protection."

2. Will Ireland toughen up? Ever since the GDPR came into force, all eyes have been on what early actions Ireland's Data Protection Commission (IDPC) would take given that it is the EU regulator of choice for the world's biggest technology firms, including Google, Apple, Twitter, Microsoft, and Facebook. And up until May, the regulator seemingly had little to boast about.

But with impeccable timing, on May 22—just ahead of the regulation's second anniversary—the IDPC handed Tusla, the country's child and family agency, its second (as yet unspecified) GDPR fine just days after handing it Ireland's first.

The IDPC also used the announcement to trumpet its progress in its efforts to take on Big Tech—a thorny issue with other EU data authorities (most notably Germany's) and privacy campaigners, who have bemoaned its slow progress.

The regulator has submitted a draft decision to other EU data protection authorities regarding a self-reported GDPR breach by Twitter, as well as a preliminary draft decision concerning WhatsApp and the information it shares with Facebook. The IDPC also announced it has completed an investigation into Facebook over how it processes personal data, adding it is deciding what—if any—penalty it will recommend, and that it has sent draft inquiry reports following separate investigations into Instagram and WhatsApp. Additionally, it noted that an EU court judgment on the IDPC's decision regarding privacy campaigner Max Schrems' complaint against Facebook was due for release on July 16 (and which has seen the EU-US Privacy Shield, the mechanism used by companies to ensure that trans-Atlantic data transfers are safe, ruled invalid).

For Schrems, however, the IDPC announcement was too little, too late. On May 24 he sent an open letter to every EU data protection authority, the EDPB, the European Commission, and European Parliament criticizing Ireland's slow progress, pointing out France's CNIL was able to single-handedly issue a €50 million (U.S. $55 million) fine against Google within seven months, while after two years, the IDPC has completed only the first of six steps in the cases against Instagram and WhatsApp. He also questioned the IDPC's appropriateness as a regulator. "The GDPR is only as strong as its weakest [data protection authority]," he said.

Ireland, with an annual budget of just €16.9 million (U.S. $19 million), is responsible for leading 127 GDPR-related investigations—more than any other country in Europe. Some 23 of these are investigations into Big Tech firms, with 11 relating to Facebook alone (seven relating to Facebook's Irish subsidiary and one to the parent company, two to WhatsApp, and one to Instagram). None of these investigations have been completed yet; nor are they likely to be before autumn at the earliest, the IDPC admits.

Under the GDPR, multinational companies are meant to select the data protection authority they believe is the most pertinent regulator for them: For most companies, it is the regulator based in the same country where they have their European headquarters. Big Tech has overwhelmingly chosen Ireland. Under the GDPR—as part of its "one-stop shop" mechanism—the designated data regulator is meant to field all complaints against that company, even if they come from other member states: For example, a Spanish complaint against Twitter should be dealt with by the IDPC.

While Google has its European headquarters in Ireland, however, all three of its GDPR fines have been handed down by other EU data protection authorities: France's CNIL fined Google €50 million (U.S. $55 million) in January 2019, while the Swedish data protection authority fined it 75 million Swedish Kroner (U.S. $7.6 million) in March this year. In July, the Belgian Data Protection Authority fined the search engine €600,000.

In the French case, EU data protection authorities decided that the case could be handled by the French data regulator since the Irish watchdog did not have "decision-making power" over Google's Android operating system and its services. In the Swedish case, the regulator said it was enforcing corrective actions regarding delisting user data the company had failed to implement in 2017 before the GDPR had come into force. The Belgian fine was a result of Google's refusal to delete search results linked to a Belgian public official, thereby violating the GDPR's "right to be forgotten" provision. Precedents have therefore been set showing Big Tech (and other companies) can be hit by multiple regulators, and for possibly the same infringements, irrespective of where they might be based.

Expectations about the likelihood of Ireland hitting a Big Tech company with a fine equal to 4 percent of global turnover, which would produce the first billion-euro penalty, remain low. The country has a reputation for taking a "light

touch" toward monitoring conduct or enforcing regulations, and of cozying up to big companies.

Critics (and cynics) point out Ireland's position as a major EU technology base has helped rescue its economy following the 2008 financial crisis and continues to do so now during the coronavirus pandemic. "A maximum turnover-based fine would be a bold move from the Irish regulator, especially when its government sought to create a welcoming European base for Big Tech," says Daniel Milnes, a partner and information lawyer at Forbes Solicitors.

3. How will GDPR enforcement develop in the future? Much of the focus of the GDPR's first two years has been about the level of fines and the speed at which they are issued. But there is more to the regulation than just its punitive powers.

Data lawyers, privacy campaigners, and compliance professionals had hoped a slew of GDPR decisions that have been in the works for months would have produced much-sought-after clarity about what data practices are unacceptable and what internal measures may help to stave off the dreaded maximum penalty if an organization suffers a breach. The complexity of many of the cases, the sparse resources and staff numbers of many of the data protection authorities, and the impact of COVID-19, however, have held up progress. As such, experts hope that by the GDPR's third anniversary there will be a clearer picture.

Tanguy Van Overstraeten, a partner and global head of law firm Linklaters' privacy and data protection practice, believes that in the future "businesses need certainty and a more unified approach" regarding sanctions, enforcement, and interpretation of the GDPR across the European Union. He points out that while there is growing harmonization within the European Union (as well as in third countries with similar data rules), he says "there are still significant differences" between member states on issues as wide-ranging as the age of children requiring parental consent, guidelines on the use of "cookies" on Websites, and criminal records.

Many lawyers agree there needs to be greater standardization, but they concede this is currently difficult to achieve: European regulators now apply different rules for the calculation of fines, for instance, which means there is little consistency in penalties from one EU member state to another.

Some believe, however, there will be greater alignment in the way EU data protection authorities interpret and enforce the GDPR in the coming year due to the number of decisions coming down the pipeline, as well as decisions around appeals likely to be published (even if delayed).

"Enforcement approaches between EU [data protection authorities] are likely to become more aligned as more decisions are appealed, and appeal rulings are released, which will provide greater clarity about how penalties are arrived at," says Annabel Gillham, a partner in the data protection team at law firm Morrison & Foerster.

"It takes time under new laws for cases to be investigated and for enforcement action, if appropriate, to follow," says Helen Davenport, data privacy partner at law firm Gowling WLG. "The GDPR is no different."

For some, however, the focus on fines is "irrelevant," particularly regarding the actions of Big Tech.

Tech company Brave Chief Policy Officer Dr. Johnny Ryan says the only effective way to tackle data abuses is to prohibit abusive practices. As such, he has a negative view of the effectiveness of many of Europe's data protection authorities so far.

"The U.K.'s ICO has not managed to make its larger fines stick and has backed off Big Tech problems," says Dr. Ryan. "Over two years since I blew the whistle about what our industry was doing to target ads, the ICO has yet to use any of its statutory powers to investigate the issue or to protect people in the U.K. from it."

"The only true way to measure a regulator's effectiveness is to ask: 'Have we stopped the harm? Have we stopped the business models that allow the harms to take place? Have we prevented these abusive practices from happening again?' The answer to all of these questions is 'no.' A fine may not necessarily change how a company operates. Forcing firms to change the way they process and handle data is the only way forward." ■

TOP 5 BIGGEST GDPR FINES

*Only includes final & binding fines

Google Inc.	€50,000,000
TIM - Telecom Provider	€27,800,000
Austrian Post	€18,000,000
Wind Tre S.p.A.	€16,700,000
Deutsche Wohnen SE	€14,500,000

Source: Privacy Affairs

Ireland GDPR report shows it's yet to hold Big Tech accountable

Neil Hodge explores the Irish Data Protection Commission review of its GDPR investigations, which has come under fire for ignoring Big Tech.

In June, Ireland's Data Protection Commission (IDPC) released its review of the work it has carried out investigating potential breaches and privacy complaints under the General Data Protection Regulation (GDPR) since the new rules came into effect in 2018.

Reactions to its publication have been muted, namely because of the conspicuous absence of detail surrounding its investigations into Big Tech. One data expert, who declined to be named, dismissed the 72-page document as a "lengthy press release."

The IDPC is the lead GDPR regulator in Europe for some of the world's biggest tech firms—notably Apple, Facebook, Google, Microsoft, LinkedIn, and Twitter—and has 24 open cross-border inquiries into their conduct. The report, however, features just seven pages on its investigations into Big Tech, four of which are simply a list of the cases.

Facebook is the subject of 11 statutory inquiries by the IDPC (eight into Facebook, two into WhatsApp, and one into Instagram). Of the other 13 cases, three each relate to Apple and Twitter; two to Google; and one each to Verizon, Quantcast, Microsoft (relating to LinkedIn), dating app Tinder owner Match Group, and online business review app Yelp.

The investigations into Facebook include breach notifications, how the company uses personal data to drive advertising, how it stores user passwords, and whether the company's terms of service and data policy are GDPR compatible.

But the report provides little detail on their progress other than that the inquiries are ongoing with draft reports sent to the relevant parties in some cases or the investigations are at a "decision-making" process (whatever that means). No timelines are given or explained. The same is true of the other inquiries into tech firms. The IDPC submitted a draft decision on Twitter to other EU data protection authorities on May 22—the most advanced stage it has reached out of all of its cross-border inquiries—but it is unclear what happens next, or when. It is also unclear if the draft decision will be a final decision.

Instead, the report devotes more space to the "quick wins" the IDPC has achieved against some of these firms in a "case study" section. In particular, the data authority discusses how it forced Facebook to pull its rollout of a dating app ahead of Valentine's Day this year over privacy concerns (which are unspecified in this report) and a failure by the company to give the regulator a data protection impact assessment, as well as dump its Election Day Reminder feature—not just for the Irish general election in February, but for all future elections in the European Union.

The report also talks about the regulator's "supervisory interactions" with Google (ongoing since late 2018), which have prompted changes to the search engine's location history and Web and app activity, but which are still not sufficient enough to assuage its concerns. Google again comes up (alongside Microsoft and Apple) over concerns about how users' voice data is processed. The IDPC says that it is developing pan-European guidelines to make the technology GDPR-compliant, despite tweaks by tech companies.

Another victory involved the IDPC persuading LinkedIn to cease displaying the member-to-guest connection invitation screen on its platform, which was generated by syncing the address books of its European members. The IDPC views the move as "a positive step taken by LinkedIn Ireland in meeting its GDPR requirements, particularly for the processing of non-user data." LinkedIn was more sanguine, saying that it removed the feature because it no longer provided significant value to EU users.

More space in the report is devoted to how the regulator has reprimanded and engaged with public-sector organizations that have breached GDPR compliance (or think they have, as every single inquiry is a result of self-reporting rather than from a complaint). In fact, the IDPC has launched over twice as many inquiries (53) against national entities—including the police service and the Catholic church—as it has against Big Tech. Local authorities alone account for 31 of the probes.

Of these investigations, two cases have resulted in Ire-

"The DPC has clearly been working hard, but a large number of these cases look like they could have been resolved by data controllers, data protection officers, and at the corporate level without getting the regulator involved. The DPC has published a significant amount of guidance for data controllers, but perhaps it should have more efficient mechanisms for weeding out these cases before they escalate and take up its time."

Ryan Dunleavy, Partner, Stewarts

land's first GDPR fines—both against the country's child and family agency, Tusla, and both small (€75,000 [U.S. $84,203] and €40,000 [U.S. $44,908], respectively).

Some of the key takeaways of the report show that organizations have either failed to understand the GDPR or are worried about non-compliance with it (or both). In the two years since the GDPR came into effect, the IDPC received some 12,437 breach notifications—93 percent (11,567 notifications) of which relate to GDPR.

The regulator says that "despite the high volumes, the cases that have been assessed give no indication that organisations are over reporting."

Rather, it says, "they suggest that many of the breaches that the IDPC examines could have been prevented by more stringent technical and organisational measures at source"—meaning that an organization's in-house data protection officer should have reviewed and remedied the issues themselves.

By far the most frequent cause of breaches reported to the IDPC—and which accounts for 80 percent of the total—is "unauthorised disclosure." The report says manual processing—and consequently an inferred lack of robust processing procedures—is at the root of far more reported breaches than phishing, hacking, or lost devices (which amount to just 5.6 percent of breach notifications collectively).

David Kennefick, product architect at cyber-security software vendor Edgescan, says the worryingly high level of human error points to organizations' "general low-level of maturity in how to handle people's data." Kennefick adds there is also a danger organizations may be downplaying the significance of breaches caused by human error—writing them off as silly errors rather than properly investigating why such breaches occurred, whether the controls put in place to prevent such breaches are working or are being ignored, and whether steps to remediate previous exposures are sufficient.

Some experts believe the data regulator's priorities may have been skewed toward dealing with routine queries it could turn around quickly, rather than face the more daunting challenge of bringing Big Tech to account, and that the absence of hard detail is "telling."

"The regulator has gone for 'low hanging fruit' instead of trying to tackle the bigger problem," says one data privacy expert. "The Commission seems to have spent more resources dealing with self-reported incidents that probably affect a relatively small number of people than address the massive privacy concerns that people have with Big Tech that affect millions across the European Union."

Ryan Dunleavy, partner and head of the media disputes department at law firm Stewarts, says the report shows the IDPC has been dealing with a high-volume of cases that were potentially resolvable at the data protection officer level rather than focusing more on significant data and privacy issues—especially those around Big Tech.

"This report shows how inundated the DPC has been over the two years since the GDPR was introduced across Europe," says Dunleavy. "The DPC has clearly been working hard, but a large number of these cases look like they could have been resolved by data controllers, data protection officers, and at the corporate level without getting the regulator involved. The DPC has published a significant amount of guidance for data controllers, but perhaps it should have more efficient mechanisms for weeding out these cases before they escalate and take up its time."

For Dunleavy, "the report skirts around the key questions that everyone wants to know more about: When are we going to see more progress from the regulator on data and privacy issues related to Big Tech?"

"Given its role as lead supervisory authority to the various multinational Big Tech organisations that often have their EU headquarters in Ireland, it is disappointing to see that the DPC's action against them over the last two years appears to have been limited and that fines against Big Tech by the Irish regulator still seem to be hovering on the horizon," he adds.

The Irish Data Protection Commission was approached for comment but did not respond. ■

Market forces, not regulations, lead the charge for data privacy

Data privacy is about to become a more tangible concept to Americans not due to regulation like the CCPA, but because the most influential brand in the nation is making it a pillar of how it does business. **Dave Lefort** has more.

Data privacy is about to be a much more tangible concept for U.S. consumers, and it's not because the first state law regulating it (the California Consumer Privacy Act) became enforceable for thousands of businesses in July.

Yes, the CCPA has been on the minds of compliance practitioners for a couple of years now, but most of the public knows nothing about it or its European predecessor, the General Data Protection Regulation (GDPR). A survey conducted in late 2019 by data solutions provider Tealium revealed that while more than 90 percent of U.S. consumers want the state or federal government to adopt regulations to protect their data, nearly 70 percent had never heard of either the CCPA or the GDPR.

Data privacy is getting its moment not because of anything the government is doing to protect what many believe is a civil right, but rather because the most influential brand in the nation is making it a pillar of how it does business going forward. In early June at its annual developers conference, Apple revealed it was about to take a big step toward making it more clear to its nearly 100 million iPhone users in the United States just how much data companies collect about us, who they're sharing it with, and whether they're using it to track us.

According to Apple, the following will be among the features baked into its next iPhone operating system update, scheduled for the fall:

» The user interface will feature prompts that lets users know what types of data each app collects about them and which data types are used to track them. Each will be displayed as an itemized list. (Examples below.)
» Users will have to "opt in" for apps to access their data. Previously, opting in was the default, and you had to take action to "opt out" if you didn't want to share certain data with an app provider.
» For apps that track location, users will have the option to share their approximate location rather than their exact whereabouts.
» iPhones will also display an orange dot in the corner whenever a user's microphone or camera is activated.

Apple compared these new features to labels on food products that display ingredients and nutritional information. While food labeling became widespread only after a federal law mandated it, there's no legislation requiring the degree to which Apple is prioritizing privacy labeling.

Is Apple making this move because it's the right thing to do ethically? Perhaps. More likely, the company is reading the tea leaves and sees that consumers are increasingly placing a premium on privacy.

There's data to back that up: 71 percent of consumers polled by management consulting firm McKinsey earlier this year said they would stop doing business with a company if it gave away sensitive data without permission. And about half of respondents said they are more likely to trust a company that limits the amount of personal information it requests.

For Apple, a company that doesn't rely on customer data nearly as much as its Silicon Valley competitors, making the personal data each app collects more transparent for users is also a smart business play.

The same can't be said for Google, whose Android smartphone operating system is the largest platform in the United States with about 120 million users. Google makes most of its money through advertising and internet search, both of which rely heavily on user data.

Shortly after Apple's announcement, Google unveiled a privacy improvement of its own: It will automatically delete a user's location history and Web activity after 18 months.

Not 18 hours. Not 18 days. Eighteen months. Not much of a concession, but would you expect one from a company whose business model is based on monetizing the data of its users?

That's sort of the point here: While the CCPA represents a step in the right direction for protecting consumers, businesses proactively prioritizing privacy is more likely to make a lasting impact. You can argue whether Apple's motivations were based more in principles or profits, but the impact on consumers' awareness of the data being collected will be unmistakable.

Future of privacy legislation in the U.S.

That's not to say legislation and regulation can't help. Nearly a dozen states are considering data privacy legislation of their own, and there are several bills floating around Congress that would address privacy at the federal level.

The problem is the coronavirus pandemic has hamstrung state legislatures and, at the federal level, it's going to be next to impossible to get privacy legislation on the docket in an election year with a divided Congress.

That being said, there are some good ideas on the table should public support force privacy onto Congress' agenda. The most recent bill is the Data Accountability and Transparency Act of 2020, which would create a new federal agency to regulate privacy and would also ban the use of facial recognition technology, which has shown recently to have issues of racial bias.

In an op-ed published on Wired.com, the bill's sponsor, Sen. Sherrod Brown (D-Ohio) writes that the overly verbose user agreements we all opt into without reading are "simply the price of admission" for using technology that's become irreplaceable to the 21st-century consumer.

"So most of us click Yes and agree to sign away our information, because our credit cards, mortgages, car loans, bank accounts, health apps, smart phones, and email accounts all require us to," he writes.

Unfortunately, neither Brown's bill nor three other bills that focus more on privacy issues related to COVID-19 contact tracing technology are likely to see the light of day in this session of Congress.

Looking beyond the election, data privacy isn't a pillar of President Trump's long-term agenda, and there's nothing related to the topic listed among Democratic presidential candidate Joe Biden's list of 37 "bold ideas."

So that brings us back to Apple and to the forces of the free market advancing the cause of privacy, along with state legislation like the CCPA and international regs like the maturing GDPR. People care about their data, and they'll care even more if they get privacy alerts on their iPhones whenever they download a new app.

If your company doesn't have an airtight policy around the data it collects, where it's stored, how it's used and protected, and whether it's shared with any third parties, your risk is only going to increase as momentum builds for more accountability and transparency around privacy. ■

WHY IS DATA RETENTION IMPORTANT?

Upfront, it is cheap to store data. However, when the organization is involved in litigation or, worse yet, a regulatory agency investigation, all of that ESI is now subject to attorney review for responsive documents—an expensive proposition.

Put simply, data you don't have can't be breached, and you don't have to produce it during litigation. When considering whether there's an organizational need to pursue data Retention, ask two questions:

1. Could a demand for all documents pertaining to a specific person expose your organization's over-retention of personal data?
2. Can your organization delete excess data that would help minimize exposure to judicial and regulatory sanctions, as well as civil liability?

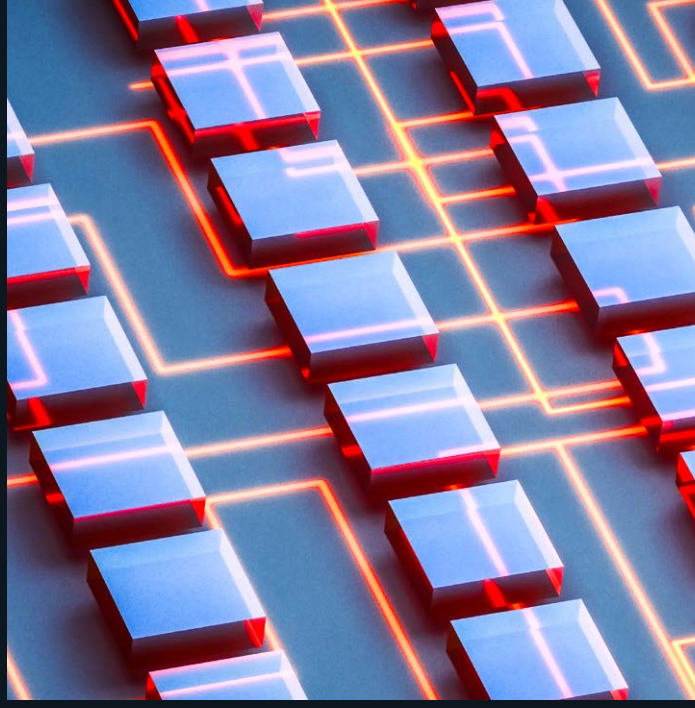
Leveraging proven retention methods and enforcement models is the most effective way to dispose of unnecessary records and data, while meeting regulatory obligations to avoid unnecessary risks.

YOU CAN'T AFFORD TO OVER-RETAIN DATA

The most egregious GDPR violations will hit companies that have over-retained data, which means that having an enforced data retention and deletion program is no longer optional. Most companies vastly over-retain records and information, and an average of 75% of that information contains some form of personal or sensitive data.

GDPR Articles 5, 13 17, and 25 require companies that are subject to the law to dispose of any personal data once it has fulfilled its purpose unless there is a legal or regulatory obligation to retain the data longer. Penalties and fines for breaches so far have been severe, with British Airways facing a $230 million fine, and Marriott facing a $123 million fine.

60 DAYS TO DEFENSIBLE DATA RETENTION



Failure to identify, address, and minimize risks related to data Retention will be the driver of fines, oversight burdens, litigation and settlement expenses. This makes the processes of developing an effective Retention process even more critical. The basic steps breakdown as follows:

1

DEVELOP & MAINTAIN A COMPREHENSIVE DATA INVENTORY

IDENTIFY WHAT PERSONAL DATA EXISTS, MEDIA TYPES USED, PROCESSING ACTIVITIES, DATA SUBJECTS, STORAGE LOCATIONS, AND RETENTION OBLIGATIONS.

2

LEVERAGE PROVEN RETENTION & DISPOSAL STANDARDS

ADOPT RETENTION STANDARDS THAT ARE INDUSTRY-SPECIFIC AND PROCESSES THAT ARE EFFECTIVE AND DEFENSIBLE.

3

COMMUNICATE PROGRAM EXPECTATIONS

AUTOMATE THE PROCESS OF DISTRIBUTING, TRACKING, AND ASSESSING EMPLOYEE COMPLIANCE LEVELS WITH VERIFIED AND TRACKED RESPONSES.

4

DISPOSE OF OVER-RETAINED DATA

APPROPRIATELY DELETE VAST AMOUNTS OF UNNECESSARY AND REDUNDANTLY-RETAINED DATA ACROSS ALL MEDIA TYPES AND STORAGE LOCATIONS INCLUDING EMAIL, UNSTRUCTURED SHARED DRIVES, AND PAPER.

5

ESTABLISH ONGOING CONTROLS

LEVERAGE PROVEN EXPERIENCE, STANDARDS, AND TECHNOLOGY TO STREAMLINE YOUR DATA RETENTION AND RETENTION EFFORTS TO ENSURE DEFENSIBILITY.

3-PHASE APPROACH FOR DATA RETENTION IN PRACTICE

Applying data Retention principles in practice requires a three-phase approach: conducting a preliminary analysis, further data classification, and remediation of legacy data. Each step below is a closer, in-depth look at how to classify data and apply Retention practices.

1. Preliminary Analysis

The first phrase is designed to give business unit leaders an idea of the data they have and the risks associated with it. Data analysts obtain the organization's metadata and analyze the file path directory structure, then apply preliminary classifications for the data. The end result is a baseline report that is used to compare future changes. Success in this phase is particularly important, given that subsequent phases will rely on the report's findings.

2. Further Data Classification

This phase has an emphasis on additional data owner identification through business unit mappings, incorporating four tasks:

- Business Unit Mapping. Ideally, you have an inventory of all of your enterprise data set up before you're attempting to minimize it. Not only is it an important component of the CCPA and GDPR to know what data you have (and on whom), but you have to know where to find that data. When breaking the data down by business unit, the question "Who has the most data?" is answered. A legal team member usually leads this effort, engaging the business unit (who know what data they need) and adding another level of classification.
- Retention Analysis. Here, records and information management professionals identify the maximum retention period for each business unit in order to identify data that is outside of that range. They then update the retention mappings onto a master table. In doing so, they follow existing retention policy or, if conflicts develop, create a new policy. Often, their biggest challenge is getting executive buy-in.
- Hold Analysis. For this task, attorneys (inside or outside counsel) identify all business units currently subject to legal holds, then map those holds to the business units in a master hold table. Once a given hold is released, the ESI involved is now able to be deleted under the company's retention policy.
- Implementation. This involves developing an implementation plan, rather than "pushing the button." The updated mappings for business units, retentions, and holds are analyzed and any needed adjustments are made. Disposition rules regarding inactive user accounts and data outside of retention/holds mapping are also finalized.

3. Remediating Legacy Data

This phase involves remediating legacy data identified in the prior phrases and developing a "go-forward" approach. Three tasks are implicated:

- Validation. The goal of this task is to obtain consensus between business owners and counsel as to the proposed disposition of the legacy data—the sign-offs—and then record the particulars of the consensus for future reference.
- Disposition. This is the point where someone in IT "pushes the button." Typically, "deleted" data is quarantined for a certain period (24 hours to 6 months) before it is truly destroyed, as a backup.
- Go-Forward Approach. Developing a "go-forward" approach translates into minimizing future problems with data proliferation. It involves documenting such processes in a disposition "playbook," developing management metrics and data integrity standards and then monitoring the organization's information ecosystem for activities that put data out of compliance.

BEST PRACTICES FOR IMPLEMENTING DATA RETENTION

Implementing a data Retention strategy means the process will be ongoing and organizations must be persistent in creating a data Retention strategy that is comprehensive and effective. *There are two main best practices to follow:*

1. CREATE INFORMATION RETENTION POLICIES

This usually involves three main things:

- **Gaining organizational buy-in.**
  In order to have organizational buy-in, starting from the top on down, requires having the right people at the table—representatives from IT, legal records and information management, and the respective business units.

- **Create the retention policies.**
  Counsel crafts the policies in conjunction with upper management using the business judgement rule to determine what data must: 1. be kept permanently, 2. Has strategic value to the organization, or 3. Is subject to a legal hold. Considerations include multinational aspects (is data subject to the Foreign Corrupt Practices Act or GDPR), ephemeral data (text messages and apps like Snapchat), and social media. Organizations that are highly-regulated in other areas can expect elevated regulations here.

- **Communicate and enforce policies.**
  This is the area where retention failures most often occur. The key to communicating and enforcing retention policies is to keep them simple and easy to understand by outside parties. Retention policies are part of the overall information governance plan.

2. HARMONIZE YOUR, LEGAL HOLD, AND DATA RETENTION POLICIES

The biggest challenge with any legal hold process is that, as more custodians are added, the efforts to administer the hold multiply. This is because a small percentage of the custodian base consumes a disproportionate amount of time and effort; they may be difficult to reach, not respond to hold notices, or ask numerous questions about the hold.

There are four steps in harmonizing all of the processes discussed:

- **Automate legal hold notifications.**
  An automated system, as the name implies, tracks who's acknowledged the hold and escalates the notice to a non-compliant custodian's manager without intervention from the hold administrator. That system also tracks which custodians have been interviewed and has an interactive method for asking interview questions so administrators can identify other candidate custodians and where responsive ESI is located. That system should also offer a consolidated means to limit custodian notices to those who are on multiple holds, so as to avoid "notice fatigue."

- **Link to the existing data infrastructure.**
  Linking a legal hold system to existing infrastructure means linking to HR, asset management and matter management systems so that when an administrator creates or updates a hold, he/she has access to the most current information.

- **Minimize irrelevant ESI.**
  After it's been verified that the data is no longer under a legal hold and doesn't serve a relevant business purpose, it's time to delete it. If there's a serious concern that the data might be relevant later, either don't delete it or review the data that is "quarantined" prior to full deletion.

- **Document the process.**
  Documentation is arguably the most important part of the process because if there's no proof of the process, it's more difficult to say why an individual did or did not do something. Courts look for a reasonable process, rather than a perfect one, and documentation goes a long way to demonstrating reasonableness.

A DATA RETENTION CASE STUDY

The Client

A $15 billion distributor with 20,000 employees in more than 1,000 locations nationwide. The company serves customers in all 50 states and locations around the world.

The Challenge

The CISO's challenge was twofold: cut down 53 TB of steadily growing data, and understand the relationship between their data and the data owners. At the same time, the GC desired the implementation of a data Retention policy to reduce litigation and cybersecurity risks. One of the greatest challenges the CISO and GC faced was knowing where to begin.

The Solution

Technology and tightly-structured processes with ongoing controls to meet obligations and reduce risks. Exterro provided deletion strategies for all media types, including email, unstructured data, and paper records to defensibly delete unnecessary records and information. We also provided all the necessary documentation to memorialize the data Retention logic and initial cleanup efforts.

ROI

After implementing the data Retention policy, the strategies significantly reduced volumes of data across the organization.

- **File Share:** Eliminated 20 TB of the file share data immediately. The cost avoidance of containing the growth in their file share environment is $60,000 annually.
- **Email:** Applying an email policy and auto-delete resulted in email storage volume decreasing 4% annually. Originally, the volume growth was increasing at 8% annually.
- **Paper:** By applying retention rules to offsite paper, they immediately reduced off-site storage by 50%.
- **Backup Procedures:** Reduced tape archive from 30,000 tapes to zero, and reduced backup retention from 90 days to 28 days. As a result, 300 TB of savings eliminated the need to acquire additional backup storage. The annualized cost reduction from these changes is $1.2 million.

SEE EXTERRO DATA RETENTION IN ACTION

Manually performing these Retention processes can be labor-intensive. But with a combination of structured processes and technology, risks and costs can both be reduced. The world's most trusted and defensible data retention and disposal software solution for meeting GDPR and CCPA regulatory obligations is Exterro's Data Retention platform.

LEARN MORE WITH AN EXCLUSIVE

FREE DEMO

Experts: CCPA enforcement to prioritize children's privacy

Aaron Nicodemus queries experts on what enforcement will look like under the California Consumer Privacy Act.

What will enforcement of the California Consumer Privacy Act (CCPA) now that the deadline has arrived?

For one, companies can expect aggressive enforcement from California Attorney General Xavier Becerra. That contrasts with the enforcement environment for the last major personal data privacy legislation, the European Union's General Data Protection Regulation (GDPR), which took effect in May 2018.

Becerra has said publicly he disagrees with GDPR regulators' initial practice of issuing warnings, rather than fines and enforcement actions, said Dominique Shelton Leipzig, a Los Angeles-based attorney who co-chairs law firm Perkins Coie's AdTech Privacy and Data Management practice.

"He's made it clear that he wants to learn from the GDPR's experience, that it did not have enough teeth at the beginning, that there were not enough enforcement actions," she said. "He's been very cognizant of the criticisms of (privacy) regulators in Europe."

Becerra remained committed to the July 1 enforcement date, despite the coronavirus pandemic and a request by more than 60 business groups to push the enforcement date back to Jan. 1, 2021.

The first wave of enforcement actions, Shelton Leipzig said, will be on issues on which Becerra's office can make a statement.

Children's privacy a top priority

A coronavirus-related alert Becerra issued in April advised the public that children's privacy rights would continue to be protected under the CCPA during the pandemic.

"Whether it's our children's schooling, socializing with family and friends, or working remotely – we are turning to mobile phones and computers as a lifeline. With such a dependency on online connectivity, it is more important than ever for Californians to know their privacy rights," he wrote.

Consumer CCPA-related complaints to the AG's office will also likely spur enforcement actions, but those complaints have not yet been made public.

Companies that are flouting the law will be the first in line for enforcement actions, Shelton Leipzig said, particularly if they cannot show they attempted to comply with the law.

"Starting someplace is better than starting nowhere," she said.

"I'd be especially concerned if I was a company that collects sensitive data" but had done little to comply with the law, predicted Philippus von Nerée, head of operations at Semasio, a German-based marketing insight and targeting company that grew up under strict, local privacy regulations and the GDPR. "The better you prepare, the better you document, the easier it will be to show you made a good faith effort (to comply)."

"The safest thing to be is a zebra in a herd of zebras," added Dan Clarke, president of IntraEdge, which has developed Truyo, an Intel-backed GDPR and CCPA compliant data privacy platform. "You've got to show your company has made an effort to comply. The last thing they want to see is that you've done nothing."

A CCPA-related lawsuit against TikTok, filed on behalf of a minor, alleged the Chinese company mishandled the data of the minor.

Digital marketers, data analysts beware

One industry that might be in the AG's crosshairs with the CCPA is digital marketing. Digital marketing companies are called data brokers as defined under a different California state law, and they have to register with the AG's office every year. Registered data brokers are more likely to be compliant with the CCPA than those that are not, but the industry's business model of collecting and selling data to third parties will likely put their data collection practices under the AG's microscope.

Already, a lawsuit in which data broker Bombora alleged CCPA violations by its competitor ZoomInfo could provide some clues to potential enforcement actions by the California attorney general.

"The safest thing to be is a zebra in a herd of zebras. You've got to show your company has made an effort to comply. The last thing they want to see is that you've done nothing."

Dan Clarke, President, IntraEdge

Big Data users are another likely target, Shelton Leipzig said. Any organization or any industry that sorts and analyzes large data subsets could be asked to prove how they protect consumers' privacy. Areas of interest within Big Data include predictive analysis, business intelligence, Software as a Service (SaaS), and facial recognition, among others.

The AG's office has also posted consumer-facing CCPA notices and made public statements on CCPA priorities for industries as varied as technology platforms, social media companies, financial institutions, utilities, telecommunications, and connected cars.

There are already several CCPA-related lawsuits filed in California courts that the AG's office will likely be monitoring. California-based consumers filed lawsuits against Zoom and Houseparty alleging the companies mishandled their personal information.

According to the CCPA, the law applies to any company doing business in the state of California "that earns $25 million in revenue per year, sells 50,000 consumer records per year, or derives 50% of its annual revenue from selling personal information." Only California-based consumers can request to opt out of a business' data collection practices, request that their personal information be deleted, or file a lawsuit alleging mishandling of their personal data. If asked by the AG's office, companies will have to prove they were responsive to such requests. Companies must disclose to the AG's office the value of the data collected to the business.

That still covers an awful lot of companies, and many are still trying to figure out how to respond to the CCPA's numerous requirements—despite the law taking effect Jan. 1.

Good news for companies that have complied with the GDPR—90 percent of their preparations will help them comply with the CCPA, said Nerée.

"The tracking of user requests in the CCPA is new," he said, and even GDPR-compliant companies for whom the CCPA applies will have to build a system to respond to and track opt-out and data delete requests from California-based consumers. The CCPA also has a requirement that companies assign a value to the data they collect, which is also missing from GDPR regulations.

For other corporate leaders attempting to comply with the CCPA, the first thing to do is to understand how your organization collects, stores, monitors, and uses the data it collects.

"The challenge that we are seeing more and more is a fundamental awareness of data," said Stephen Cavey, co-founder of Ground Labs, a vendor that develops data management and regulatory compliance technology. Businesses should ask themselves: What data are we collecting? How are we storing it? Are we prepared to handle opt-out requests?

There are two ways to figure that out, Cavey said. One is the manual or assumption-based model, where all department heads are asked about their data collection practices. That model is based on the assumption the department heads know exactly where all of the data their organization collects is stored and how it can be accessed.

This model often overlooks many kinds of data that is collected, Cavey said. A more thorough approach involves hiring a consultant to complete a data security survey. "The findings can be absolutely breathtaking," he said.

As an example, a telecommunications client of Ground Labs had a secure link to its bank, which it used to send a daily reconciliation of its finances. The company had excluded the reconciliation from its data security survey, guessing (incorrectly) that there was no personal data transmitted in the reconciliation reports. Turns out the company sent more than 100 million pieces of personal information on its customers to the bank, which the bank then uploaded into its system. All of that data had to be accounted for in a revised survey.

Then there is the issue of distributed data, exacerbated by the work-from-home phenomenon sparked by the coronavirus pandemic. Employees with a weak WiFi signal might download a document to work on it, rather than remaining linked to their company's secure network. There's personal data that is shared with third parties, consultants, and vendors that needs to be tracked. Contracts with those third parties should include clauses that address how personal data should be handled.

"Not unless you do a proper assessment of your data will you truly understand the scope of the problem," he said. ■

Europe's top court strikes down EU-U.S. data transfer rule

Neil Hodge examines Europe's top court ruling that a mechanism used by thousands of companies to send data to the United States is unlawful.

In a surprise decision that will have a major impact on trans-Atlantic data transfers, Europe's top court ruled in July that a mechanism used by thousands of companies to send data to the United States is unlawful, citing concerns raised by privacy activist Max Schrems in his ongoing legal battle with Facebook over whether EU citizens' data can be shared with U.S. authorities under the country's surveillance laws.

The EU-U.S. Privacy Shield—scrapped in July—was set up in 2016 to protect the personal data of Europeans when it is transferred across the Atlantic for commercial use. More than 5,300 companies had signed up to the program, which allowed (on paper, at least) validated companies safe access to EU citizens' data without fear of legal reprisals under EU privacy law.

Its predecessor, known as Safe Harbor, was also scrapped by the same court in 2015 after Schrems raised similar concerns then following revelations made by former U.S. intelligence contractor Edward Snowden in 2013 about mass surveillance.

In a statement, Schrems said: "The court clarified for a second time now that there is a clash between EU privacy law and U.S. surveillance law," adding that "this judgment is not the cause of a limit to data transfers, but the consequence of U.S. surveillance laws."

While the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. agreement, it did uphold the validity of another data transfer mechanism known as standard contractual clauses (SCCs)—template contracts that are prepared by the European Commission and have been relied upon by businesses to facilitate transfers for nearly 20 years.

"Large companies have complex webs of data transfers to hundreds, if not thousands, of overseas recipients. The CJEU has made it clear companies cannot justify them using a 'tick box' exercise of putting SCCs in place. Instead, the risks associated with those transfers need to be properly assessed."

Tanguy Van Overstraeten, Partner and Global Head of Privacy and Data Protection, Linklaters

The CJEU added that EU data protection authorities, however, should proactively suspend or prohibit a transfer of personal data to a third country where they take the view that the level of data protection afforded in the European Union cannot be matched by the country where the data is being exported to—a position put forward in a non-binding opinion last December.

As a result, SCCs may not provide the thousands of companies that use them the legal protection they need; while valid, they can only be used where the risks associated have been properly assessed.

How ruling will impact businesses

Lawyers say that large companies will make hundreds (if not thousands) of transfers, so the additional compliance checking may be burdensome. They also say the possibility of ceasing some existing types of data transfers altogether cannot be ruled out.

In addition, lawyers suggest the ruling means that data transfers to other jurisdictions, such as India or China, will need careful examination because they also have strong state surveillance powers.

"Failed schemes like this have significant impacts for individuals and for businesses," says Stewart Room, global head of data protection and cyber-security at law firm DWF. "Businesses will be asking themselves 'what's next?' There are other countries that pose challenges to privacy rights and data protection and they raise obvious questions about the potential for other legal action."

Tanguy Van Overstraeten, a partner and global head of privacy and data protection at law firm Linklaters, says that "large companies have complex webs of data transfers to hundreds, if not thousands, of overseas recipients. The CJEU has made it clear companies cannot justify them using a 'tick box' exercise of putting SCCs in place. Instead, the risks associated with those transfers need to be properly assessed."

"Similarly, this may encourage data protection regulators to clamp down on international transfers more aggressively, with the possibility of transfers to jurisdictions with strong state surveillance powers becoming increasingly difficult. The judgment leaves a huge question mark over data transfers to the U.S.," says Van Overstraeten.

Emma Erskine-Fox, an associate at U.K. law firm TLT, says that data regulators now need to provide guidance on the safe use of SCCs. "SCCs are widely regarded as being out-of-date, clunky and unfit for modern data processing practices, but organizations will need to continue to rely on them for some time to come. Additional guidance is urgently needed on how and where the SCCs can be relied upon," she says.

Lawyers say that businesses will now look to European Union regulators to propose some form of transition to allow them to move away from the Privacy Shield without the threat of significant sanctions and civil compensation claims.

Some experts also suggest that the CJEU's judgment could have implications for the United Kingdom's prospects of gaining adequacy at the end of the Brexit transition period to ensure that data flows between the United Kingdom and the European Union continue as they do now.

Under the EU's General Data Protection Regulation (GDPR), it is incumbent upon those exporting the data to a recipient in a third country to check that it will be handled with the same level of protection as in the European Union. If not, they could face hefty fines of up to 4 percent of global annual revenues.

"The judgment makes it clear that companies cannot just sign the SCCs, but also have to check if they can be complied with in practice," said Schrems.

The case—C-311/18 Facebook Ireland and Schrems—went to the CJEU in Luxembourg after the privacy campaigner challenged Facebook's use of SCCs, saying they lacked sufficient data protection safeguards. It is now highly anticipated that the Irish Data Protection Commission, the lead regulator for Big Tech firms in Europe (including Facebook), will follow the CJEU's lead and demand changes in the way that the social media company stores personal data for EU citizens. ■

Companies paying price for EU-U.S. Privacy Shield removal

The legal and financial burden for those complying with the invalidation of the EU-U.S. Privacy Shield might be worse than first thought, writes **Neil Hodge**.

When Europe's top court scrapped the European Commission's second attempt at establishing a cast-iron mechanism to ensure secure data transfers across the Atlantic, businesses knew there would be a price to pay.

Following a list of "frequently asked questions" issued on July 24 by the European Data Protection Board (EDPB), the EU body in charge of regulating Europe's compliance with data privacy and the General Data Protection Regulation (GDPR), however, it became apparent the legal and financial burden for companies might actually be worse than first thought.

On July 16, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield, which allowed (on paper, at least) some 5,300-plus validated firms safe access to EU citizens' data without fear of legal reprisals under EU privacy law.

Like its predecessor—known as Safe Harbor, which was scrapped in 2015—the Privacy Shield was axed over concerns raised by Austrian privacy campaigner Max Schrems that U.S. surveillance laws allowed the government access to EU citizens data, thereby violating EU regulations.

Yet—while the Privacy Shield was immediately dropped as a legal option—two other principal mechanisms remain open. While valid, however, neither are legally bulletproof any longer.

Standard contractual clauses (SCCs)—"off the shelf" template contracts prepared by the European Commission that have been relied on by businesses to facilitate transfers for nearly 20 years—were ruled to still be valid, but with caveats: The level of data protection in the third country has to be equivalent to that in the European Union and, if not, companies and EU data protection authorities will have to proactively suspend or prohibit transfers of personal data.

The other mechanism available to EU companies—and not mentioned in the CJEU judgment—are binding corporate rules (BCRs), which follow EDPB guidelines, have stringent accreditation requirements, and can take a long time to implement. As a result, they are not a popular option (only 135 companies have signed up to them).

Because the United States is not believed to be a safe country in terms of data privacy, and because of the country's Foreign Intelligence Surveillance Act, however, BCRs may also give limited protection if companies continue to transfer data between the European Union and United States.

Lawyers had hoped the accreditation process around BCRs would be simplified and companies would be given a "grace period" to continue using SCCs as before the ruling without the threat of regulatory sanctions while the European Commission agrees to a third mechanism to ensure the safe transfer of data between the European Union and United States.

The EDPB, however, has ruled out both possibilities. Instead, say lawyers, the onus is firmly on companies—and poorly resourced data protection regulators—to ensure strict adherence to the GDPR when personal data is transferred to a third country. And if there is any doubt about the strength of a third country's snooping laws (and not just the United States, but countries such as China, Russia, and India), data transfers to entities within it are out. Failure to prevent could result in a hefty fine of up to 4 percent of a company's global revenues under the GDPR.

The EDPB says "supplementary legal, technical or organisational measures" may need to be used by companies to ensure compliance and provide safeguards, but it does not elaborate as to what these measures might be. Privacy experts say data encryption might be one possibility, but that this is neither a simple, nor cheap, remedy. The EDPB has said it will issue further guidance but has not specified when.

The GDPR actually envisages the development of codes of conduct and certification mechanisms that allow the lawful transfer of personal data from the EU/U.K. to countries such as the United States. According to Pulina Whitaker, a partner at law firm Morgan Lewis, however, none have yet been approved. As such, she says, "these options should now be prioritized for approval to fill the gap in allowing data transfers," adding: "We would expect these to be approved within

the next year."

Tanguy Van Overstraeten, a partner and global head of privacy and data protection at law firm Linklaters, says "the onus on companies having to check the circumstances surrounding a data transfer to third countries to ensure an equivalent protection to that afforded in the EU may become quite expensive and burdensome."

Van Overstraeten adds that while the CJEU ruling has immediate effect, he hopes there will be no active enforcement action from data protection authorities. "The EDPB has been fast in publishing its preliminary assessment in the form of FAQ. It has announced further guidance will be forthcoming, which I hope will be pragmatic and solution-driven. It is important not to enforce against companies that are looking for appropriate solutions while also awaiting guidance from supervisory authorities."

Alex van der Wolk, partner and co-chair of law firm Morrison & Foerster's global privacy and data security practice, thinks making companies and data protection authorities responsible for evaluating a destination country's laws "is a huge burden to bear, and one can wonder whether it is at all appropriate to put this burden on the market and (generally) under-funded DPAs."

"It took the Irish DPA millions of Euros to litigate the Schrems case, and it took the CJEU years to reach a conclusion on the adequacy of the Privacy Shield framework. It is unimaginable that companies or DPAs are able to do this for each and every transfer," he adds.

Van der Wolk says "it's unlikely there will be a political solution soon," despite the pressing need. He believes the major question currently is whether SCCs can still be used for transfers to the United States and, if so, under what circumstances. While the CJEU gave guiding principles on how the SCCs are to be used, the practical implementation will have to come from lawmakers, data protection authorities, and the market itself, he says.

"The EDPB's FAQs in that respect are not yet helpful as they say they are still evaluating what 'additional measures' may look like," says van der Wolk. "It is very much hoped that the EDPB will come with further specifics on this."

In the meantime, lawyers believe companies will perform risk assessments about where they are sending data to, what kind of protections they have in place, and what kind of data is being transferred.

Andy Serwin, U.S. chair and global co-chair of DLA Piper's data protection, privacy, and security practice, says "for data importers, we expect that EU companies will drill in more to these issues and U.S. companies will have to have additional information ready for the inevitable questions. For EU companies (or U.S. companies that have EU operations) that are data exporters, they will have to conduct an analysis under GDPR to determine whether there is adequacy around the particular transfer in question."

Experts are hopeful a practical, interim solution can be worked out quickly, but many admit the lack of a "grace period" is a cause for concern. Some expect increased regulatory scrutiny going forward, but several also expect an increase in consumer complaints about the safety of their personal data being transferred to countries with stringent cyber-security laws.

"It took the Irish DPA millions of Euros to litigate the Schrems case, and it took the CJEU years to reach a conclusion on the adequacy of the Privacy Shield framework. It is unimaginable that companies or DPAs are able to do this for each and every transfer."

Alex van der Wolk, Partner, Morrison & Foerster

The lack of coordination among national data protection authorities about what enforcement approach they should take is another issue that needs to be resolved quickly. Privacy experts want guidance at EU level, indicating the circumstances per country under which SCCs can be used to transfer data. But already EU data regulators have signaled different approaches and tolerances to non-compliance.

For example, German data regulators have taken a hard line on adherence to the CJEU's ruling and the inherent dangers of EU citizens' data being sent to the United States, while the Irish Data Protection Commissioner has said data transfers to the United States are not invalid, just "questionable."

U.K. companies, on the other hand, have been advised by the U.K. Information Commissioner's Office to "conduct a risk assessment as to whether SCCs provide enough protection within the local legal framework" and "take stock of the international transfers ... and react promptly as guidance and advice becomes available." The ICO added it would take a "pragmatic" approach.

One privacy expert, who declined to be named, said: "The GDPR was supposed to bring a more consistent approach to enforcing data protection across the EU—not make it more fragmented. Guidance that is endorsed by all 27 EU data protection authorities (as well as the United Kingdom) is essential to ensure harmonization of rules and approach." ■

Walmart the latest hit with CCPA-related lawsuit

Consumers are using the CCPA to sue firms they say mishandled their data. Walmart is the latest to be slapped with a lawsuit. **Aaron Nicodeumus** explores.

A San Francisco man alleges in a class-action lawsuit filed with the U.S. Northern District of California on July 10 that Walmart was hacked and the personal information—including his credit card—that he gave to the company is being sold on the dark web. The man, Lavarious Gardiner, says hundreds of other Walmart customers have similarly seen their Walmart data appear on the dark web, where criminals and fraudsters sell and trade it. Gardiner says he has been forced "to purchase a credit and personal identity monitoring service to alert him to potential misappropriation of his identity and to combat risk of further identity theft."

Under the California Consumer Privacy Act (CCPA) companies can be hit with a penalty of up to $750 "per consumer per incident" in regard to data breaches. Walmart says it was not hacked and that it is not the source of the data on the dark web.

"Protecting our customers' data is a top priority and something we take very seriously. We dispute the plaintiff's allegations that the failure of our systems played any role in the public disclosure of his personally identifiable information (PII)," said a Walmart spokesman in an e-mail. "We intend to defend the company against the claims and will respond as appropriate with the court."

The CCPA has been in effect since Jan. 1, with a look-back provision to Jan. 1, 2019. Enforcement, however, began July 1, with no public actions yet taken under the law. With the CCPA, California is the only state that allows consumers to file such lawsuits against companies. Most consumers have to depend on their state attorney general's office to pursue action against companies when an alleged data breach occurs.

Several other companies have been sued for alleged violations of the CCPA, under similar circumstances.

Minted, an online stationery and craft retailer, was sued by two customers in June in the U.S. Northern District of California. The customers alleged their personal information was stolen and sold on the dark web. Minted says the data breach occurred in May 2020 and that it notified its customers a week later. The lawsuit contends the credit card information of five million Minted customers was exposed in the breach.

"The Walmart suit is certainly the most high-profile in what is almost certain to be a wave of privacy right action suits to come," said Dan Clarke, president of IntraEdge, a compliance software vendor. "If what [the plaintiffs] have alleged is accurate, Walmart and Minted would be at the forefront of suits clearly in the scope of CCPA's private right of action and associated potential statutory damages."

Another CCPA-related lawsuit was filed in March against Sunshine Behavioral Health Group, a chain of drug and alcohol addiction clinics in San Juan Capistrano, Calif. The lawsuit, filed in the U.S. Central District of California in March, alleged Sunshine Behavioral Health suffered a data breach that exposed 3,500 client records. The lawsuit contends one of those client records belong to a Pennsylvanian who says he has spent hours working to protect his PII after someone tried to open a fraudulent credit card with the stolen information.

"This is a defining time for the CCPA, when precedents will be set and case law will start to be established," said Stephen Cavey, co-founder of Ground Labs, a vendor that develops data management and regulatory compliance technology. "Many businesses won't act to be compliant for something like this until absolutely pushed. The wait-and-see approach is a dangerous strategy to follow."

Based on public statements by California Attorney General Xavier Becerra, some experts have guessed the AG's office will prioritize protecting children's privacy as it enforces the CCPA, as well as shining a light on the way digital marketers and data analysts store, use, and sell the data they collect.

Several other CCPA-related lawsuits have also been filed, including against TikTok, filed on behalf of a minor, that alleged the Chinese company mishandled the data of the minor; and Zoom and Houseparty, in which consumers alleged the companies mishandled their personal information.

A lawsuit filed by data broker Bombora alleged its competitor, ZoomInfo, violated the CCPA by how it collected and sold its customer data. And a lawsuit against online retailer Hanna Andersson and Salesforce that cited potential violations of the CCPA in a data breach moved toward settlement in July. ■

Google fined for violating GDPR 'right to be forgotten'

Belgium's Data Protection Authority has fined Google Belgium for refusing to delete search results linked to a Belgian public official, a provision of the GDPR known as the "right to be forgotten." **Aaron Nicodemus** reports.

Belgium's Data Protection Authority (APD) fined Google Belgium €600,000 (U.S. $670,000) for refusing to delete search results linked to a Belgian public official, a provision of the EU's General Data Protection Regulation (GDPR) known as the "right to be forgotten."

The APD announced the fine as punishment for Google Belgium's "serious breach" of the GDPR for refusing to delete search results, known as dereferencing. The fine is the largest ever levied by the APD; the previous high was a fine of €50,000 (U.S. $56,000).

The public official had appealed to the APD to force Google Belgium to delete two search results after the internet giant's subsidiary refused to do so. In response, the APD issued the fine regarding Google Belgium's refusal to delete one search result but agreed with its stance on the other.

The search result that drew the fine involved "a complaint of harassment against" the public official, who said the harassment claim had been "declared unfounded many years ago," according to the APD.

"The APD considers that the request for dereference is well founded and that Google has expressed a serious breach by refusing it," the APD wrote in its translated press release. "Since the facts have not been established, are old, and are likely to have serious repercussions for the complainant, the rights and interests of the person concerned must prevail." The APD called Google's decision "particularly negligent, given that the company had evidence of irrelevance and out-of-date facts."

The APD fined Google "for not having dereferenced the pages reporting the obsolete complaint against the complainant, for the lack of information provided to the complainant to justify the refusal of dereference," and the lack of transparency in the dereference form.

A second search result related to "a possible political labeling" of the public official, a label which the official refuted. The APD agreed Google had the right to refuse to delete the search results, "considered that, given the role of the complainant in public life, maintaining their referencing was necessary in the public interest."

The APD ordered Google to "stop referencing the pages concerned in the European Economic Area and to adapt its dereference request forms in order to provide more clarity in relation to which entity (ies) are responsible for this data processing."

"In the right to be forgotten, a balance must be struck between, on the one hand, the right of the public to access information, and, on the other, any interests of the data subject," said Hielke Hijmans, president of the APD's litigation chamber. "If some of the articles cited by the complainant can be considered necessary for the right to information, the others, which relate to unproven harassment and are about 10 years old, must be able to be forgotten. By now providing links through its widely used search engine that can cause serious damage to the complainant's reputation, Google has shown clear negligence."

A spokesperson for Google and its parent company Alphabet said: "Since 2014, we've worked hard to implement the right to be forgotten in Europe and to strike a sensible, principled balance between people's rights of access to information and privacy. We didn't believe this case met the European Court of Justice's criteria for delisting published journalism from search—we thought it was in the public's interest that this reporting remain searchable. The DPA disagreed. We're going to ask the Courts to decide."

Google's EU headquarters is based in Ireland, but it has been other EU countries—first France, then Sweden, and now Belgium—to issue fines against Google for GDPR violations.

France fined Google €50 million (U.S. $57 million) in 2019; then a French court shot down Google's appeal in June. Sweden's Data Protection Authority fined Google 75 million Swedish Kroner (U.S. $7.6 million) in March for its failure to comply with the GDPR, also related to the "right to be forgotten." ■

FUTURE-PROOF YOUR COMPLIANCE APPROACH

Get ahead of the coming regulatory onslaught by preparing your organization now with automated processes and technology that facilitates easy compliance with the CCPA, GDPR, and other data privacy regulations. Request a demo of Exterro's Legal Software Suite, the industry's only Legal Governance, Risk, and Compliance (GRC) platform, and see how future-proofing your compliance approach can pay dividends in cost avoidance.

GET A DEMO

exterro
Legal GRC Software