GDPR and CCPA Start to Bare Teeth as Privacy Protection Goes Global

Matthew Newman, Mike Swift and Vesela Gladicheva*

In the past two years, US companies have been forced to comply with sweeping new requirements to safeguard individuals' personal data imposed by the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

In a digitally connected world, where data flows across continents in the blink of an eye, protecting citizens' data privacy has become integrated in most businesses' crucial operations. It wasn't long ago that United States companies saw privacy as a European obsession that should be better left to private companies to manage. Now tech giants are clamouring for more regulation – even on the US federal level – to ensure consistent application of stringent privacy rules.

'What has changed with GDPR is that privacy is finally taken more seriously', Bruno Gencarelli, a senior European Commission official, said during a recent conference.[1] 'Privacy has made it to the boardroom. Privacy, the role of courts; it's an increasingly litigated area. That says something about privacy. The GDPR is part of that.'

One way to think about the evolution Gencarelli describes is that US companies are becoming more mature about how they handle personal data.

---

* Matthew Newman, Chief Correspondent, MLex Market Insight, and Mike Swift, Chief Global Digital Risk Correspondent, MLex Market Insight, with reporting by Vesela Gladicheva, Senior Correspondent, MLex Market Insight. This article was finalised in late June 2020.

1 'The View from the Commission: The GDPR Turns Two', International Association of Privacy Professionals, 2 April 2020.

The GDPR and more recently the CCPA,[2] which was the first comprehensive data protection law in the US, are forcing them to acquire a much better sense of what personal data they collect, how they use that data, the systems to protect that data and when that data was destroyed.

Companies have also been obliged to follow the EU's strict rules on international data transfers. Multinational groups can rely on EU decisions that certain countries provide 'adequate' data protection, but they can also use other mechanisms, such as standard contractual clauses (SCCs), to ensure that EU principles are applied when data is transferred outside the bloc.

While SCCs are the most common method to transfer data legally, they have also been challenged following Edward Snowden's revelations about US intelligence agencies' demands for data from US tech companies. Following a complaint by a privacy activist who challenged Facebook Ireland's reliance on SCCs as a legal basis for transferring personal data to Facebook in the US, the Court of Justice of the European Union (CJEU) on 16 July annulled the EU US adequacy agreement known as the Privacy Shield and placed strict conditions on the use of SCCs.

The GDPR has also spawned organisational changes. More companies have a chief privacy officer or other privacy leaders who report directly to the chief executive officer or the board of directors, although those companies remain in the minority. And privacy – it might better be described as 'data management' – has been elevated to a more strategic role for many companies, even becoming a key way to differentiate a company from its competitors. Consider the gigantic advertisement Apple plastered over 12 vertical floors on the side of a Las Vegas hotel last year during the influential Consumer Electronics Show: 'What happens on your iPhone, stays on your iPhone.'

'I think the GDPR has presented a strategic opportunity for privacy protection to move from being more of a functional role to being part of the decision-making and strategic function of the business', said Eleanor Treharne-Jones, chief revenue officer for IntraEdge, an Arizona company that joined with Intel in a joint venture called Truyo, which provides software to help companies respond to privacy requests under the GDPR, CCPA and other privacy laws.

What has sparked this change in mindset? Events such as the 2018 Cambridge Analytica scandal, in which the data of up to 87 million users may have been improperly shared with a political consulting firm, have focused citizens' minds on protecting their data. Legislators reacted by pushing through a tough new privacy law in California that took effect in January 2020. Other states are likely to follow California's lead.

---

2 Text of the California Consumer Privacy Act of 2018: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

GDPR's second anniversary

The GDPR is now marking its second anniversary. The EU's landmark data protection law gives companies chills, makes some privacy advocates sigh in frustration and causes consumers to frown whenever they have to click on a meddlesome cookie consent pop-up.

The GDPR's first year was greeted with fanfare and self-congratulations by regulators in Europe, but privacy activists are now openly lamenting that national authorities lack funding for enforcement. They are also deeply concerned that the GDPR doesn't have much to show for itself. After two years, there has been only one significant fine against Big Tech – a €50m penalty against Google in France in January 2019. This decision was upheld in June by France's State Council, the country's highest administrative court.

Companies from Palo Alto to Paris still struggle to integrate changes, abide by new rules and change corporate cultures. They are also seeing a wave of new privacy laws around the world, most notably the CCPA in California, but also regulations in Brazil and Thailand, and proposals in India and Indonesia. These initiatives have been inspired to varying degrees by the GDPR and could be followed by even more ambitious efforts, such as a federal privacy law in the US.

Some regulators see the GDPR's international influence as its biggest success.

'GDPR has been a good example, even if it's difficult to be compliant. It has excellent principles to be complied with for other countries', said Tine Larsen, president of the Luxembourg National Commission for Data Protection. 'Countries must have a high level of data protection if they want their economies to be trustworthy. If companies comply with GDPR as one standard, a higher standard, then it would apply all over the world.'

This year marks the 50th anniversary of what is widely acknowledged as the world's first digital data privacy law, passed by the state of Hesse in central Germany in 1970. Following the abuses of civil liberties during the Nazi and communist eras, it's not surprising that Germany has been a strong advocate for strict data protection rules.

US companies are increasingly aware that what started as a unique curiosity in one German state has grown into a global movement, with about two-thirds of the world's countries and self-governing territories now having a privacy law, up from about half in 2015, a recent United Nations study

concluded.[3] Recent academic research concluded that from 2010 to 2019, 62 additional countries enacted data privacy laws, more than in any previous decade.[4] There are now 143 nations with data protection laws in place, and the number could top 200 during the coming decade.

Some US companies look at the GDPR as a heavy burden that has forced them to make costly changes to their organisations and saddled them with compliance headaches. Other companies see the regulation as a business opportunity allowing them to transform their approach to privacy and harness the true value of their data. Truyo, for example, is part of a growing list of new ventures providing compliance services or allowing consumers to exercise their new privacy rights. Apple has gone to great lengths to maintain the strong encryption built into its iPhones, sometimes to the ire of US law enforcement.

Mark Zuckerberg, founder and chief executive of social media giant Facebook, thinks the GDPR should be an inspiration for more regulatory certainty on data protection in the US and beyond.

'New privacy regulation in the United States and around the world should build on the protections GDPR provides. It should protect your right to choose how your information is used – while enabling companies to use information for safety purposes and to provide services', Zuckerberg said in a blog post on 30 March 2019.[5]

Whether they regard the GDPR as an opportunity or a bane, from the day the regulation took effect on 25 May 2018, companies have had to adapt to individuals' new rights, allowing access to data to fielding requests to erase personal information.

The GDPR has transformed the regulatory scene in Europe. Data protection authorities in the EU have been flooded with complaints about intrusive surveillance cameras, telemarketing, promotional emails and companies' failure to provide access to data. These complaints involve a wide range of companies and public authorities: banks, electric utilities, medical centres, municipalities and more. From the GDPR's first day, privacy activists turned their guns on the biggest technology companies, including Google, Facebook and Amazon.

---

3 'Data and privacy unprotected in one third of countries, despite progress', United Nations Conference on Trade and Development: https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2348&utm_source=UNCTAD+Media+Contacts&utm_campaign=e9f09e07c1-EMAIL_CAMPAIGN_2020_04_29_07_40&utm_medium=email&utm_term=0_1b47b7abd3-e9f09e07c1-70608677.

4 Graham Greenleaf and Bertil Cottier, '2020 Ends a Decade of 62 New Data Privacy Laws' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611.

5 'Four Ideas to Regulate the Internet', 30 March 2019, Mark Zuckerberg, Facebook CEO, https://about.fb.com/news/2019/03/four-ideas-regulate-internet.

But enforcement against US Big Tech has been limited to the French decision against Google and a smaller one against the search giant in Sweden. The remaining cases are still pending at Ireland's Data Protection Commission.

The focus is on Ireland because most tech companies – Apple, Facebook, Google, LinkedIn, Twitter, WhatsApp and others, but with the notable exception of Amazon's EU base in Luxembourg – have chosen Ireland as their country of 'main establishment'. Under GDPR rules, the data protection authority where a company has its main establishment is the lead supervisor in pan-European cases. This is crucial because complaints in other countries are funnelled to the country's data protection authority and global companies have to deal with only one authority.

Ireland's Data Protection Commission is investigating all of these companies for suspected GDPR breaches. The probes are exploring such issues as AdTech practices, data-breach notifications, the right of individuals to access data that companies hold about them, the lawful basis for processing information referred to in data policies and the obligation to inform users about how data is processed.

Helen Dixon, the Irish Data Protection Commissioner (DPC), has taken a cautious approach in her first decisions. The DPC has opened more than a dozen investigations into Big Tech companies, including Apple and Google.

GDPR fines are imposed for infringements of the law, rather than for harm done on the data subject; they do not therefore compensate any data loss caused to individuals. Data subjects can sue companies for damages either on an individual or group basis in the form of a class action.

On the eve of the GDPR's second anniversary, the DPC took its first step to resolving a cross-border probe into a US tech giant – Twitter. The Irish watchdog forwarded its provisional decision to peers in the European Data Protection Board, the umbrella body for the EU's national regulators. The move represents the most high-profile test yet of how the GDPR's 'one-stop shop' process works. That process specifies that when the lead regulator in a cross-border case makes a decision, any EU regulators with an interest in the case have four weeks to comment on it, object or propose changes.

The one-stop shop system will be further tested through disputes that have reached the European courts. One long-standing, high-profile case involves Facebook and how the US social media company uses tracking cookies, in a clash with the Belgian Data Protection Authority going back to 2015.

Facebook has argued that the Irish Data Protection Commission should be the only watchdog in the EU dealing with complaints over the company's processing of personal data, because its main European establishment is located in Ireland. The Belgian authority, on the other hand, has said that

the GDPR never intended to silence other regulators or courts in Europe by centralising complaints.

Last year, Belgian judges referred the case to the CJEU in Luxembourg to clarify whether the Belgian Data Protection Authority can continue its proceedings against Facebook and could be considered the lead authority to pursue the case.

Meanwhile, consumers lament how the GDPR has led to annoying pop-up boxes for websites' cookie consent. Privacy activists wonder why EU governments have not put their money where their mouth is and fully funded data protection agencies. Brave, a privacy-focused web browser, has complained to the European Commission that only six of Europe's 28 national GDPR enforcers have more than ten tech investigators. Brave called on the Commission to start lawsuits against EU governments for failing to comply with their obligations under GDPR to properly finance data protection authorities.

In the US, despite the CCPA having taken effect this year, uncertainty reigns because the California law could be replaced within a few years by tougher new state rules – anchored by the first stand-alone data protection authority in the US – or by a federal privacy law. The picture could become clearer in November 2020 when voters will decide whether to approve additional data-use restrictions in the proposed California Privacy Rights Act (CPRA), but some degree of uncertainty is likely to linger until 2022 or longer, depending on when Congress acts on a national privacy bill in the wake of the 2020 presidential election.

This article will first describe the main features of the GDPR, including its history and new rights for individuals and new requirements for companies. Secondly, it will compare the CCPA with the EU regulation, focusing on rights and potential penalties.

The third section will describe the impact of these privacy laws on US companies in terms of organisational changes and the legal uncertainty regarding the level of fines and the complex issue of compliance with rules on cookies and consent for processing data. There will also be a discussion of risks for companies of reputational harm from data breaches, investigations and lawsuits. Some of the major enforcement actions and current investigations will be reviewed.

Finally, the article will look at how data protection will evolve after more than two years of the GDPR and nine months of the CCPA. Will these landmark rules usher in a sea change in how personal data is treated in the US and the world?

Origins of the GDPR and CCPA

The GDPR is a vast law that took more than four years to negotiate before final approval in April 2016. The regulation is 261 pages long and is made up of 11 chapters with 99 articles.[6]

The legislation replaced the EU Data Protection Directive,[7] enacted in 1995 at the dawn of the internet era and before the rise of Google as the dominant search engine and the birth of social media giant Facebook and Twitter. The Directive regulated the processing of personal data and required the establishment of national data protection authorities.

Even though the Directive was meant to lead to full harmonisation of data protection rules, that was not the case as each government implemented the rules differently. As a result, there were a variety of interpretations of the definitions and rules, and the authorities' enforcement and the severity of penalties differed widely.[8]

The GDPR, in contrast, is a regulation and requires full adoption in national legislation by all countries, though there are some notable exceptions that will be discussed further in this article. The belief was that a 'strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation', said Viviane Reding, the European Justice Commissioner who proposed the regulation in January 2012.[9]

While the GDPR brought the EU firmly into the internet age, data privacy and data protection rights have been part of the EU's heritage as a reaction to the abuses suffered by millions during the Second World War. The right to privacy or private life was enshrined in the Universal Declaration of Human Rights (Article 12) in 1948.[10] and the European Convention of Human Rights (ECHR) (Article 8) in 1950.[11]

By the late 1970s, the Council of Europe, an international organisation to which all EU countries belong, concluded that Article 8 of the ECHR had a number of shortcomings, such as uncertainty over what was covered under 'private life'.[12]

---

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504.

7 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

8 *Handbook on European data protection law* (2018 edn, Council of Europe, European Union Agency for Fundamental Rights).

9 https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.

10 www.un.org/en/universal-declaration-human-rights.

11 www.echr.coe.int/Documents/Convention_ENG.pdf.

12 Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (European Data Protection Supervisor, September 2014), p 4.

There was also a recognition that the increasing use of computers and the automatic processing of personal information required new data protection rules. Legal experts for the Council of Europe found that there was a 'lack of general rules on the storage and use of personal information' as well as 'how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others'.[13]

These reflections led to a new instrument called the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108). This is a legally binding instrument, which was opened for signature on 28 January 1981 by the Council of Europe.[14]

While Convention 108 served as a template for national data rules, it failed to lead to a harmonisation of privacy rules in Europe. By the 1980s, with the growth of transborder data transfers, this lack of convergence was becoming a threat to the free flow of data between European countries. The possible impediment to the development of the EU's single market was seen when France's data protection authority, the Commission Nationale de l'Informatique et des Libertés, blocked the transfer of personal data between Fiat France and Fiat Italy, arguing that Italy did not have adequate rules. The impasse was only resolved after Italy agreed to abide by the French data protection standards.[15]

The push for a Europe-wide data protection directive gathered pace with the adoption of the Single European Act, which set a deadline for the establishment of the single market in goods by 1992. Officials at the European Commission realised that international data flows in the then 12-nation bloc were an essential part of the growth of the single market, and they published a draft directive in 1992. The directive was finally approved in 1995, becoming the most influential data protection instrument to date.

The other major advance for data protection law came with the Charter of Fundamental Rights of the European Union in 2000, which became legally binding in 2009. It contains an explicit right to the protection of personal data (Article 8).[16]

The Lisbon Treaty in 2009 gave the Charter of Fundamental Rights the same legal standing as the constitutional treaties of the EU. As a result, the EU institutions and bodies and the Member States are bound by it. Moreover,

---

13 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434.

14 https://rm.coe.int/16808ade9d.

15 Julia Schwanholz, Todd S Graham and Peter-Tobias Stoll (eds), *Managing Democracy in the Digital Age: Internet Regulation, Social Media Use, and Online Civic Engagement* (Springer 2017).

16 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

Article 16 of the Treaty on the Functioning of the European Union obliges the EU to lay down data protection rules for the processing of personal data.[17]

The GDPR took the EU to a higher level in personal data protection and became the gold standard for other nations' privacy rules. It locked in new rights for individuals – referred to prosaically as data subjects – and imposed new obligations on companies to become accountable to customers and citizens. It set up new systems for enforcement and harmonised privacy rules across the then 28-nation European Union (the UK left the EU on 31 January 2020, but the GDPR remains in force until the end of the Brexit transition period – currently set for 31 December 2020). While updating and modernising the existing 1995 Directive, the law was designed to withstand the test of time. It provides flexibility so that regulators can tackle emerging technologies and privacy challenges such as facial recognition, artificial intelligence and internet-connected cars.

Individuals' rights

The GDPR gave privacy advocates reason to celebrate and made life much more complicated for companies.

The GDPR made companies take a hard look at how they processed and stored personal data. This review, known as 'mapping', involved huge costs because companies had to conduct audits of all personal data, change internal procedures and hire additional staff, including a data protection officer. Companies that conduct a GDPR 'gap analysis' seek to understand if there are any gaps in their compliance and how to improve.

They examine data controller and data processor responsibilities, what personal data is held, where is it held and why and what categories of personal data are held. They examine data subject rights, privacy by design and by default, as well as general governance and risk management.

According to a study by accounting company PwC, 68 per cent of large US multinationals spent $1m to $10m on GDPR readiness and compliance.

A survey by the International Association of Privacy Professionals (IAPP) and accounting firm EY found that US multinational companies spent a combined $7.8bn on GDPR compliance.

For individuals, GDPR put them in control of their personal data. The regulation gave individuals the right to ask for the erasure of data (also known as the right to be forgotten, Article 17), the right to access personal data, the right to move data from one provider to another (known as data portability), the right to be informed about data processing and the right to

17 https://eur-lex.europa.eu/resource.html?uri=cellar:41f89a28-1fc6-4c92-b1c8-03327d1b1ecc.0007.02/DOC_1&format=PDF.

correct data. The GDPR put individuals in the driver's seat, allowing them to restrict and object to data processing. For example, they could stop their data from being used for direct marketing and prevent automated decision-making and profiling (processing personal data to predict someone's job performance, economic situation or health). The right to be forgotten became a feature of EU privacy law with a 2014 judgment of the CJEU on a Spanish case involving Google (C-131/12). The ruling recognised data subjects' right to seek the removal of links specifically by search engines.

A year after the GDPR took effect, the European Commission conducted a survey about individuals' awareness of these rights. The survey found that the highest levels of awareness for individuals was for the right to access their own data (65 per cent), the right to correct the data (61 per cent), the right to object to receiving direct marketing (59 per cent) and the right to have their own data deleted (57 per cent). The survey found that even if citizens are aware of their rights, they still feel that data protection is a major concern, with 62 per cent saying that they are concerned that they do not have complete control over the personal data provided online.

CCPA v GDPR

It is not a coincidence that California became the first US state to pass a comprehensive privacy law. Unlike the US Constitution, the California constitution contains an explicit right to privacy, which is provided in Article 1.[18]

The privacy laws of California and Europe have a common lineage. Alastair Mactaggart, the San Francisco Bay Area property developer, who is one of the founding parents of the CCPA, has said many times that the GDPR formed a template for the California law. But the laws are more cousins than sisters.

For one, the CCPA puts no limits on the collection of personal data and requires no consent from data subjects. The thrust of the law is to allow California residents – if they choose – to block the unimpeded trade in their personal data with companies with which they have no direct relationship.

The CCPA creates four basic new privacy rights:

1. Right to know – consumers have the right to know what personal information is collected about them and how it is used, shared or sold.
2. Right to delete – consumers can demand to have their personal data erased.
3. Right to opt out – consumers can block the sale of their personal information to a third party.
4. Right to non-discrimination – businesses cannot discriminate on price or service when a consumer exercises a CCPA privacy right.[19]

18 Text of the California Constitution: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

19 California Attorney General fact sheet on CCPA: https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.

There are a number of similarities between the GDPR and CCPA, including a broad definition of personal data and the reliance on existing regulators for enforcement. Penalties are another similarity, although the CCPA privacy sanctions are capped at $7,500 per violation, rather than being tied to a firm's annual global turnover. A CCPA fine could add up quickly, however, if a violation affects several million Californians.

But there are also many differences. Unlike the GDPR, there is no 'right to be forgotten' in the CCPA. The CCPA generally doesn't apply to small businesses with less than $25m in revenue, although there are exceptions if a firm gets most of its revenue from the sale of personal data. And the CCPA gives Californians the right to opt out of the sale of personal data to third parties, a right that is not contained in the GDPR.

In November, California voters will decide whether to approve an even tougher suite of privacy protections under the proposed CPRA. In some respects, the CPRA would carry tighter restrictions than the GDPR, including enhanced penalties for privacy violations involving children under age 16, and tighter rules involving location tracking for the purpose of targeting ads.

The CCPA (and CPRA for that matter) do not restrict the collection of data. But increasingly, US privacy lawyers and companies are focusing on whether the stream of data from consumers' smartphones might constitute a 'sale' under the California law, because of the financial value of that personal data. For example, smartphone apps or computers could share data through social media widgets – a Facebook 'like' button for example – analytics software, media players and service providers such as payment processors.

For now, several large tech companies, including Apple and Facebook, have taken the position that they do not have to offer users a link to opt out of the sale of data, because they do not sell data as defined by the CCPA. The majority of early CCPA litigation has been filed in federal court, mostly in Los Angeles, San Diego or the San Francisco Bay Area. However, because the private right of action in the CCPA is limited to data breaches and not privacy violations, it is unclear at best whether any of those suits will be the vehicle for a court to decide the definition of 'sale' under the new law. Ultimately, it will require a judge to define whether the transfer of a valuable asset such as personal data constitutes a 'sale' under the CCPA. Because actual enforcement of the privacy rules by the California Department of Justice did not begin until 1 July 2020, it may be many months – and perhaps even several years – before that definition is clearly drawn by trial and appeals courts.

Nevertheless, a consensus may be emerging that if those types of data streams are used as the basis to build a profile of a consumer and they target ads back to him or her, that might constitute a 'sale' under the CCPA.

'That seems to be where people are building a consensus that that is a sale', Will DeVries, senior privacy counsel at Google, said during a recent video webinar organised by the Berkeley Center for Law and Technology at the University of California at Berkeley.

Google has already begun developing new ways to serve ads that are less dependent on profiling because of the growing ability of consumers to use CCPA tools such as browser settings to opt out of the use of their data for profiling. But because the existing CCPA is so new that courts have not yet had time to decide questions such as the definition of sale, and the growing possibility that the CCPA could be replaced by the even stricter CPRA, there is a huge amount of uncertainty at the moment about how US privacy laws will be enforced in coming years. Enforcement questions about Europe's GDPR are an additional source of uncertainty for Google.

'We just have to accept that uncertainty is a way of operating right now', DeVries said. 'As a company that's going to be in the spotlight for compliance, we know that's our obligation.'

GDPR obligations on companies

US-based companies must first determine whether they have to comply with the GDPR. The GDPR applies to companies established outside the EU if they either offer goods or services to individuals within the EU or monitor their behaviour. If a company does not specifically target its services to individuals in the EU, it is not subject to the GDPR.

But since many Silicon Valley companies have reaped billions by hoovering up data from EU citizens for years, it's a fair bet that hundreds of US tech companies have decided to comply with the GDPR.

There is a good reason why companies are extra-vigilant about ensuring that the rights guaranteed in the GDPR for individuals are respected. Failure to safeguard these rights could lead to hefty fines: penalties for violating GDPR obligations – such as getting consent before using personal data, appointing a data protection officer and reporting data breaches within 72 hours – are up to four per cent of global turnover or €20m.

The GDPR mandates the appointment of a Data Protection Officer (DPO), but not based on the size of the company. Rather, the important criteria are whether a company's core activities consist of processing sensitive personal data 'on a large scale', and whether the company regularly or systematically monitors individuals or processes special categories of data (Article 37(1) of GDPR).[20]

20 www.privacy-regulation.eu/en/article-37-designation-of-the-data-protection-officer-GDPR.htm.

Companies are required to perform a thorough Data Protection Impact Assessment (DPIA) before any data processing that is 'likely to result in a high risk to the rights and freedoms of natural persons' (Article 35(1) of GDPR).[21] The DPIA is a central feature of the GDPR's shift towards a 'risk-based approach' in which companies are accountable for data processing. This approach is regarded by EU officials as an improvement over a one-size-fits-all obligation because it tailors obligations to companies' particular risks.

Data breach notification

Perhaps the most well-known obligation (for both data controllers and processors) is the data breach notification. A breach occurs when personal data is disclosed, either accidentally or unlawfully, such as in hacking attacks.

Data breaches have attracted massive media attention in recent years. Internet platform Yahoo! initially reported that 500 million users had their personal accounts hacked in 2013. That number mushroomed to three billion after a review in 2017. Other high-profile data breaches, such as by hotel chain Marriott International and British Airways, are the subject of investigations and possible fines running into millions of dollars. (The possible fine against Marriott by the UK's Information Commissioner's Office (ICO) is still pending and is now due in September 2020. The regulatory process in another major data breach probe, involving British Airways, is ongoing, the ICO has said.)

When a data breach poses a risk to an individual's rights and freedoms, companies have a duty to notify the supervisory authority without undue delay, and at the latest within 72 hours of having become aware of the breach. Individuals must be informed without delay if the breach is likely to result in a 'high risk' to their rights and freedoms. Companies need to describe the nature of the data breach and tell people how to avoid adverse effects. Failure to notify could result in penalties.

When the GDPR first went into effect, companies took a pragmatic approach and issued notifications on all data breaches, data protection lawyers say. But that put a huge burden on companies. Only 25 per cent of the companies surveyed by McKinsey Research said that they can meet the requirement to report any data breach to regulators no later than 72 hours after management becomes aware of it. For large and decentralised organisations, reporting appropriately and quickly can be difficult.

21 www.privacy-regulation.eu/en/article-35-data-protection-impact-assessment-GDPR.htm.

Compliance costs

Getting a company's data management in order is costly, but the failure to have a well-ordered system could be catastrophic for companies, both in terms of penalties and reputation. After the initial flurry of spending to prepare for GDPR ahead of May 2018, companies have had to deal with ongoing compliance costs, which include operational changes and the introduction of new regulations, notably the CCPA, and other regimes around the world. While businesses may regard these requirements as burdensome, the European Commission has promoted the GDPR as a way for companies to improve consumer trust through risk-based personal data management.

Anecdotal evidence, and a growing number of real empirical studies, suggest a cultural shift is washing across many companies as a result of the two seminal laws. The GDPR and CCPA are driving organisational change and reprioritising budgets as executives increasingly fret over the regulatory risk and loss of consumer trust that a big privacy breach could bring.

The GDPR is 'forcing a level of maturity for organisations', Harvey Jang, the global data protection and privacy counsel for Cisco Systems, said at a data security conference in San Francisco last year. 'It's forcing engineers to go in and trace what data is being collected and what is being done with it.'

Governance data collected over several years by the IAPP show that around the world, a growing share of chief privacy officers or other top privacy leaders now report directly to the chief executive officer or the board of directors. From 2018 to 2019, the share of privacy leaders reporting to the board of directors jumped from five per cent to 22 per cent, as shown by IAPP data.

The trend is more marked in companies that are headquartered in Europe than in the US, which could be due to the GDPR's requirement that companies designate a DPO to be responsible for that function internally. In the EU, the chief privacy officer or other privacy leader reports to either the CEO or the board in 60 per cent of companies as of 2019. In the US, just 26 per cent of privacy leaders report directly to the CEO or the board, with the chief privacy officer more likely to report to a company's general counsel, the IAPP data shows. In the EU, however, a company's top privacy leader is most likely to report to the board.

On both sides of the Atlantic, the GDPR and the CCPA appear to be driving organisational change, giving privacy and data security a more strategic role within companies. From 2016, the year the GDPR was passed, to 2019, the percentage of privacy leaders reporting to the CEO increased from 16 per cent to 23 per cent, previously unreleased IAPP data shows.

That is still a minority of companies, of course. But the IAPP data shows that more companies are recognising the importance of data protection and

are rapidly elevating privacy professionals to higher positions. It is likely that the GDPR and CCPA are causing more companies to see privacy protection as a key element of the decision-making and strategic function of the business, rather than a functional, regulatory compliance role.

Disentangling the impacts of the GDPR and the CCPA – in Europe or the US – is difficult, if not impossible. In fact, there is evidence that both laws are having a crossover effect on both sides of the Atlantic. A 2019 study[22] found that 46 per cent of US respondents said that compliance with the GDPR helped define the strategy for CCPA compliance and other US state privacy laws, while a third of European companies said that CCPA compliance would cause their organisation to re-evaluate their compliance position under the GDPR. In the US, consumers are actively asserting new rights to transparency and to block the sale of their personal data to third parties that were granted to California's 40 million residents by the CCPA. That is likely to reinforce those cultural shifts within companies.

A survey last month of 221 companies with at least 1,000 employees found that about half were receiving at least ten consumer requests from consumers each week to exercise their new CCPA privacy rights. About 20 per cent of companies reported receiving more than 100 CCPA requests a week, with nine per cent receiving more than 500 requests a week, according to the survey by Truyo, the joint venture of IntraEdge with Intel that makes software for automated privacy rights management for the CCPA, GDPR and other privacy laws. The biggest companies, not surprisingly, are getting the most CCPA requests. Nearly eight in ten respondents said they believe the Covid-19 pandemic will only bolster the trend of consumers aggressively asserting their privacy rights under the CCPA in the near future.

About two-thirds of the companies surveyed by Truyo expect to spend at least $100,000 on CCPA compliance in 2020, with ten per cent expecting to spend more than $1m. The survey found that 59 per cent of companies had invested in new technology to respond to CCPA requirements.

With the CCPA, the risks that worry executives the most are its fines, followed by the risk to 'brand reputation' in case of a privacy breach, the survey found.

---

22 'Keeping Pace in the GDPR Race: A Global View of GDPR Progress in the United States, Europe, China and Japan', McDermott Will & Emery LLP and the Ponemon Institute.

Enforcement uncertainty

Much of the frustration directed at the GDPR comes from the failure of EU authorities to land a significant fine against a big US tech company in the past two years. The one exception is the French Data Protection Authority's €50m fine against Google on 21 January 2019 for a lack of transparency, inadequate information and the lack of valid consent regarding personalised ads.

The French decision exposed some serious defects in the 'one-stop shop' mechanism under the GDPR.

In the two years after it came in, the one-stop shop mechanism – designed to handle privacy probes into companies that straddle multiple EU countries – has processed few decisions and seen a lack of transparency from enforcers. The exchange of vital information on probes has been incomplete, and crucial parts of the system remain untested.

Two probes into Google last year highlighted some of the problems with the one-stop shop.

First, the French authority's decision to fine the US tech giant brought about a wider discussion at the European Data Protection Board (EDPB) about the one-stop shop concept of lead and concerned supervisory authorities. The French probe came about because it was launched before Google had confirmed its EU headquarters for data processing. The fine landed a day before the company announced it would be Ireland.

In the other case, EU regulators took more than a year to decide who should handle complaints in multiple countries over how Google processes users' location data and handles transparency around that processing. Google initially came under investigation by Sweden's privacy watchdog, Datainspektionen, which, eight months later, handed the case over to its Irish counterpart, which in turn opened its own investigation in February.

EU legislators' intention was to eliminate red tape for multinational businesses and reduce the risk of them facing separate investigations in multiple countries over the same infringement. But that has failed, and businesses do not seem any better off than under the old data protection regime. The one-stop shop has proven highly complex to navigate for businesses and regulators alike.

Dispute resolution mechanism

Another weak point is the one-stop shop's dispute resolution element, which has yet to be tested. This additional process of cooperation among regulators will no doubt entail further problems and delays to probes.

In cross-border cases, the lead supervisor must cooperate with other concerned authorities to reach a consensus. Here, disagreements between these authorities that prove impossible to resolve would activate the EDPB's role as a mediator and see it issue a binding decision – something that has yet to happen in the 130 cases already decided.

Larsen, the president of the Luxembourg Data Protection Authority, said her authority has forwarded eight cross-border cases to the EDPB, but none has resulted in the mechanism being used.

'So far there have been no decisions that have triggered the consistency mechanism', she said. 'That's the magic moment we are waiting for.'

The first test for the one-stop shop will now arrive after the Irish DPC has sent its draft decision on Twitter to the EDPB on 22 May 2020 for review and possible amending by other national data protection authorities. It means that businesses trying to navigate the EU's legal landscape for data protection are experiencing increased regulatory uncertainty, ultimately affecting investor decisions.

Lawyers advising companies to think about designating a 'main establishment' in the EU and benefiting from the promised gifts of the one-stop shop are meeting with indifference. Companies see the system as complex and opaque, rather than a blessing. Some want it to be scrapped.

'To be efficient, it has to be simple and applied in a simple manner. It doesn't achieve that. It was made quite complicated. It won't stand the test of time', said Olivier Proust, a data protection partner at Fieldfisher in Brussels.

While this one-stop shop has increased information sharing among authorities, companies say the real solution is to bolster the powers of the EDBP and create a single European data protection authority.

'If the EU is serious about privacy enforcement, then the only way it will have teeth is to have a pan-European enforcement body', Proust said.

However, the GDPR was the result of compromises by EU governments, which are wary of giving up more sovereignty. In any case, EU countries are not interested in reopening GDPR negotiations to amend the legislation.

Derogations, inconsistency

Another big source of frustration with the GDPR is that it allowed EU governments to derogate from the regulation and apply national rules. Normally an EU regulation would apply across the EU, and Member States would not have any choice in applying the law. In fact, that was one of the main selling points of the GDPR. But the regulation includes about 50 clauses that allow derogations, leading to the creation of differing rules, for example, on the age of consent, facial recognition for law enforcement purposes, the

processing of sensitive data or the use of data for scientific research. There are also more than 20 separate DPIA frameworks adopted at a national level.

Access Now, a privacy advocacy group, said in a report last year that these divergences risked leading to fragmentation and a lack of consistency in applying the GDPR. 'In the worst cases, a small number of Member States have adopted national measures that contradict the spirit, objectives, and text of the GDPR', the group said.[23]

For companies, these divergences create legal uncertainties. A good example is how EU governments have interpreted EU rules on obtaining data subjects' explicit consent for cookies on websites. This is a crucial question that should have been resolved with a revamp of the EU's e-Privacy Directive. But more than three years of EU government talks have led to a stalemate, and some national authorities are forging ahead by releasing their own guidelines. The EDPB has recently stepped in by issuing its own guidelines based on a recent ruling by the CJEU in the Planet 49 case (C-673/17),[24] which found that users must now give explicit and active consent before a website may place cookies on a user's device.

In its May 2020 guidelines, the EDPB has come out against websites that use 'cookie walls'. In this practice, a website makes access to the site's content conditional on a visitor accepting all cookies. The EDPB said that this practice is not valid consent because users are not presented with a genuine choice.[25] Guidelines from France's CNIL take a similar line to cookie walls.

A more relaxed approach to cookies that moves away from a strict conformity with GDPR-level consent is a key goal for marketers and publishers in the e-privacy talks. In France, professional associations of media, advertising and online commerce contested the French data protection authorities' total prohibition of cookie walls. For websites that rely on advertising, a prohibition of cookies would have been hugely detrimental to their business model.

On 19 June 2020, the French State Council agreed with the complainants, ruling that the CNIL cannot infer a prohibition of cookie walls from the GDPR's requirement that websites must obtain users' freely given consent for cookies. The CNIL has thus exceeded what it can do under 'flexible law'. Without ruling on the substance of the question, the State Council considered that the CNIL could not, under the cover of an act of flexible law, enact such a general and absolute prohibition. This ruling shows that the debate over cookies and freely given consent is far from over in Europe.

---

23 www.accessnow.org/cms/assets/uploads/2019/07/One-Year-Under-GDPR-report.pdf.

24 http://curia.europa.eu/juris/document/document.jsf?docid=218462&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=1486059.

25 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

Conclusion

The GDPR was ushered in with great promises that it would bring legal certainty and lower costs for companies. In a data-driven world where personal data must move with ease from country to country, the GDPR was meant to ease burdens on companies and provide consistency over rules and their enforcement. In many ways, that has happened in the past two years.

But some promises and expectations have fallen flat, particularly the one-stop shop. Another major concern at the two-year anniversary is the outlook for international data transfers. Many companies are worried that a key mechanism used for international data transfers will be declared invalid by the CJEU.

Global companies – including tech companies such as Facebook and manufacturers such as Caterpillar – have been stuck in legal limbo after an Austrian privacy advocate, Max Schrems, challenged the validity of Facebook's use of 'standard contractual clauses' to move data across the Atlantic (C-311/18).[26] Now that the EU's highest court has annulled the Privacy Shield, companies must find another way to legally transfer data outside of the 27-nation bloc to the US and other countries. The problem is that if they turn to SCCs, they must judge whether the national laws where the data is exported are in conflict with the data protection obligations in the SCCs.

This landmark ruling will lead to more legal uncertainty for thousands of companies that use an EU data transfer mechanism, prompting some to call for a grace period to adjust to the new environment.

The European Data Protection Board, which brings together EU privacy enforcers, has said it will provide more guidance on the use of data-transfer tools, including SCCs, as well as binding corporate rules, or BCRs, for intra-group transfers. It's looking into what kind of 'supplementary measures' – whether legal, technical or organisational – could be put in place so that companies could continue to rely on SCCs and BCRs.

Still, there are reasons to be optimistic. The GDPR prompted massive changes for EU regulators, some of which had not had any ability to impose fines and were 'toothless paper tigers', as Tine Larsen of the Luxembourg DPA said. Making changes to administrative procedures, making sure the rights of defence are complied with and revamping organisations take time, according to Tanguy Van Overstraeten, a data protection lawyer at Linklaters in Brussels.

'In my practice, I can see that the authorities are doing their best. They are setting up the necessary exchange of briefs, spending time investigating the behaviour of the stakeholders. And we can intervene, following the inspections and them listening to our defence. All this takes time, however',

26 http://curia.europa.eu/juris/liste.jsf?num=C-311/18.

he said. As a result, it's not a big surprise that there have not been decisions against Big Tech, he added.

For companies, the GDPR and CCPA are works in progress. Companies need to move beyond local compliance and think about global privacy accountability. They need to change cultures, imbed privacy frameworks and evolve with the new challenges imposed by law-makers.

The GDPR can be regarded as a template for countries to craft their privacy laws. It represents a major step towards a global system of data protection. Companies that focus their energy on implementing practices that can be applied globally will be in a strong position to tackle the changes ahead.