Osterman Research

WHITE PAPER

White Paper by Osterman Research
Sponsored by AccessData
Published November 2018

Best Practices for GDPR and CCPA Compliance

Executive Summary

The European Union's (EU) General Data Protection Regulation (GDPR) came into force in late May 2018 and has implications for organizations everywhere who collect or process personal data on people in Europe. The extra-territorial scope of GDPR is much more applicable to the new global digital markets of the 21st century, and many other countries, regions, and states are following the core principles of GDPR and introducing new data protection and data privacy requirements, such as The California Consumer Privacy Act of 2018 (CCPA). The first fines under GDPR are expected by the end of 2018.

It is important to note that while the focus of this paper is on the GDPR and CCPA, there are other, similar regional mandates that are emerging across the world, including in Colorado, Japan, Canada, Australia, Brazil and elsewhere. This makes it essential that decision makers understand their need to have a common approach to dealing with privacy regulations instead of addressing them individually.

KEY TAKEAWAYS

- The regulatory climate around the world for data protection is heating up, with the GDPR leading the way and other countries and regional areas starting to enact their own frameworks. While some share many similarities with GDPR, others are more focused on data breach notification. It is essential for decision makers to understand that the GDPR and CCPA should not be treated as singular pieces of legislation, but more as the leading edge

- GDPR is now in place, and many organizations that should be compliant are still not compliant.

- New data protection and data privacy legislation, such as the CCPA, introduce several of the core principles of data protection from GDPR to the United States. While CCPA is focused only on Californian consumers, it signals a shifting wind.

- There is growing concern among regulators about the misuse of personal data, in light of high profile data breaches, inappropriate and unintended use of personal data for micro-targeting of advertising to sway elections, and other areas of concern.

- All organizations that collect, control, and/or process personal data need to step up their data protection measures, including organizational approaches and technologies to safeguard, protect, and assure the authenticity and integrity of personal data.

- Organizations that do not take appropriate steps will find themselves subject to punitive administrative fines, loss of reputation, loss of brand value, and lost business opportunities.

The regulatory climate around the world for data protection is heating up.

ABOUT THIS WHITE PAERc

This white paper includes data from an in-depth survey of North American organizations with regard to their plans for GDPR and CCPA compliance. The paper was sponsored by AccessData; information about the company is provided at the end of the paper.

The GDPR and the CCPA

New data protection regulations, such as the GDPR and CCPA, lay out the legal rights held by consumers over their personal and sensitive personal data. Entities that collect and/or process this type of data must extend these rights to consumers (in GDPR terms, natural persons known as "data subjects"), or face harsh penalties.

Specific rights vary by regulation and region, although GDPR is the most far-reaching of any current data protection regulation.

KEY DRIVERS FOR THE GDPR AND CCPA

The current push around the world on data protection is the result of several fundamental trends:

- **Aligning freedoms and responsibilities for data collection and processing of personal data**
  Vast new global digital markets have been created, leveraging new technologies that enable personal data to be collected, processed, analyzed, interpreted and used for revenue-generating activities – often without the knowledge, awareness, consent or understanding of data subjects themselves. Data protection regulations mandate the need for appropriate processing security, including organizational and technical measures.

- **Equal rules for all**
  The nature of commerce has changed drastically over the past two decades, and organizations that collect and process data on people are now unlikely to be jurisdictionally co-located. The main trend in data protection legislation is to protect the data subject based on their location, thereby applying equal rules for all organizations that collect and process data regardless of their legal location. This creates a level playing field, imposing the same rules on all players.

- **Very public bad behavior with personal data by some companies**
  Undisclosed data breaches (Uber and Google), unintended data profiling usage (Facebook and Cambridge Analytica), unintended usage of personal data (Facebook and phone numbers supplied for security), and unbridled personal data collection (Google) has set the stage for imposing strong controls on new economy companies who cannot control themselves. Making clear what is expected with regard to protection of personal data prevents any organization – new or old – from both reaping obscene profits and damaging individuals and nations by doing whatever they want with personal data behind a techno-induced haze of secrecy. Among others, the EU is deeply concerned with how micro-targeting of advertising and content based on personal profiles is corrupting freedom of choice and undermining democracy.

- **The extra-territorial scope of GDPR**
  The worldwide focus of the GDPR demands that countries and regions outside of the EU develop similar legal protections if they want streamlined access to Europe's population. While governments around the world face a legislative challenge, all organizations wanting to continue (or start) collecting or processing data on European data subjects must ensure that their current data protection approaches meet the demands of GDPR. At the same time, what the GDPR has mandated for Europe, other countries and regions are seeking to replicate for the data subjects in their jurisdictions. GDPR has shown what is possible, and other countries are following Europe's lead.

- **Forming new cultural norms where data protection and good business are not mutually-exclusive**
  While GDPR clearly imposes significant penalties for failing to meet data protection mandates (not to mention the reputational damage that goes along with this), organizations that do embrace GDPR and similar regulations have much to gain. For example, clarity of intent from data subjects on data that has been collected enables operational efficiency (i.e., legacy data can be deleted), improved revenue opportunities (i.e., by developing a trust-based relationship with customers who want to hear about new products and services), and safe data exposure and usage more broadly across the organization (i.e., marketing can use data with appropriate consent for new initiatives, rather than locking it away for only anonymized usage by data scientists for customer loyalty programs).

The worldwide focus of the GDPR demands that countries and regions outside of the EU develop similar legal protections.

WHY THE GDPR?

The GDPR introduced a modernized and harmonized legal framework for data protection across all 28 member states of the European Union. GDPR is also extra-territorially applicable to organizations collecting and processing data on natural persons in Europe. In short, GDPR is:

- Modernized for the new world of global data flows, digital marketing, advertising-based business models, global social networks, and pervasive data tracking capabilities (including those in every smartphone). The world is a different place than it was in 1995 when the European Commission published a directive on data protection; at that time, the Internet wasn't a mainstream reality.

- Harmonized in its applicability across the 28 member states. The earlier Directive had to be incorporated into local laws in each state, which created a patchwork complex of state-specific regulations that made compliance more difficult than it needed to be (for example, data breach notifications, the definition of personal data, and whether data could be transferred out-of-state). The new regulation applies across the board, with only a few allowances for state-level tailoring; this was a key principle of creating a Digital Single Market across Europe.

- Modernized and harmonized in its definition of applicability for the current world. The location of entities collecting and processing data is largely irrelevant; the key is who the collected data is about. If it is about natural persons in Europe – and this is not limited merely to the citizens of Europe – then GDPR applies.

WHY IS PRIVACY SUCH A CONCERN IN EUROPE?

One interesting questions is why Europe? Or, more fully, why is data protection such a significant matter for this part of the world? The answer has to do largely with the historical abuse of personal data on European citizens before, during and after World War II. Personal data was used against citizens, frequently with devastating results. Consequently, the right to privacy has been a foundational aspect of the new Europe from the late 1940s.

The extra-territorial scope of GDPR means that every organization in the world should review what data it collects or processes on natural persons in Europe. Specifically:

- Data controllers and data processors based in Europe have an expanded set of responsibilities, and should benefit from the greater clarity and harmonization of the GDPR compared to the early Directive.

- Data controllers not in the Union that collect data on natural persons in Europe or explicitly provide goods and services to people in Europe – whether or not a payment is involved – must also comply with its provisions.

- Data controllers must ensure that any organization that processes or stores such data act only under their instructions, and that such processors have adequate data protection policies, standards, and safeguards in place. This is an issue, for example, for multi-nationals that have regional data centers or use public cloud services; clarity on where data is being processed is a vital issue to understand, along with conditions under which a government agency can gain access.

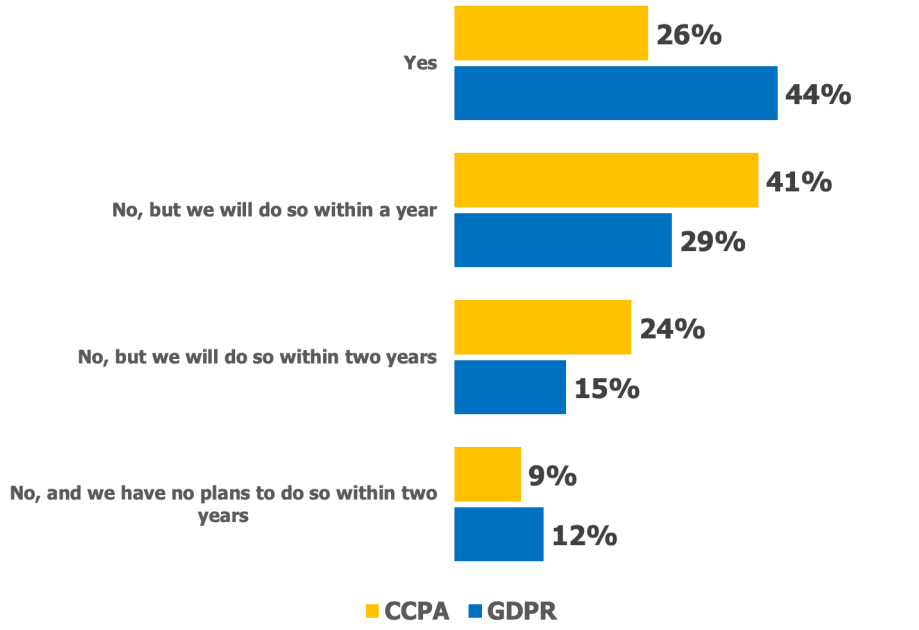
- Organizations that process data on natural persons in Europe on behalf of other organizations must also meet their requirements under GDPR, including developing and enforcing organizational and technical measures and safeguards.

The extra-territorial scope of GDPR means that every organization in the world should review what data it collects or processes on natural persons in Europe.

ORGANIZATIONS ARE NOT YET THERE

The research we conducted for this program found that with regard to the privacy of data throughout its lifecycle and in all the forms it make take, organizations still have a long way to go. We found that most organizations have not yet considered all forms of data privacy for either the GDPR or CCPA, as shown in Figure 1.

Figure 1
"For purposes of GDPR and CCPA compliance, has your organization considered all forms of data privacy throughout its full lifecycle and in all of the forms it may take?"



Source: Osterman Research, Inc.

ON PERSONAL DATA

GDPR defines personal data in two ways. First, it specifies the data elements about a natural person, that individually or in combination can be used to identify a natural person (Article 4[1]). Direct identifiers include name, ID number, and unique online identifiers like an email address. It also includes indirect identifiers such as location data and various types of identity. Finally, there are "special categories" of personal data that require additional protections, safeguards, and constraints, such as data on racial and ethnic origin, political leanings, religious and philosophical beliefs, genetic and biometric data, health data, and data about a natural person's sexual orientation and sex life (Article 9). This is one way of defining "personal data" – the data about a person.

The set of rights given to each data subject in the GDPR gives him or her ownership of their personal data – which is the ownership definition of "personal data". For example, the right of access (Article 15), the right to be forgotten (Article 17), and the right to data portability (Article 20) in combination clearly show that ownership of personal data lies with the individual, and the organizations that control or process this data have stewardship over the data, not ownership.

The set of rights given to each data subject in the GDPR gives him or her ownership of their personal data.

The GDPR and the earlier Directive have many content similarities (and the GDPR extends and updates what was in the Directive), but the fundamental difference between the two is that whereas the Directive was a recommendation to the 28 member states that required adoption into national legislation, the GDPR is EU-wide law in and of itself. As harmonized legislation – albeit with some minor opportunities for EU member states to introduce national variations – it provides consistency for data controllers and processors, certainty on applicability, and a collaboration framework for how the national data protection authorities work together.

[1] An overview of some of the key Articles in the GDPR is provided in the Appendix.

ENTER THE CCPA

As a response to the GDPR, the government of the State of California implemented the CCPA – Assembly Bill 375[i] – with urgency in late June 2018. The example of the CCPA, which is being implemented in the world's fifth largest economy, is a good example of the type of patchwork of legislation with which organizations worldwide will have to contend. It serves as a call for organizations to develop a common approach to dealing with growing body of privacy legislation around the world.

The Act was passed, in part, to preempt a ballot initiative that was to be voted on in November 2018 and that, if passed, would have imposed stricter data privacy requirements. The new Act introduces several of the principles of the GDPR to state law in California and, like the GDPR, applies to the personal data of people in a defined geography even by organizations outside of that geography.

Like the GDPR, the CCPA provides:

- The right of access by a data subject to know whether his or her data is being collected and processed, for what reasons, and with whom it is shared.
- The right to know what personal data is being collected on a data subject, and in the case of CCPA, to whom the data was or is being sold.
- The right to deletion, so that an organization must delete the personal data held about a data subject.
- The requirement that an organization implements appropriate data protection measures over personal information, including both organizational and technical measures.
- Special protections for personal data on children under the age of 16.

While the above list of rights share some commonalities with GDPR, they suffer from several weaknesses and exclude the other fundamental rights in the GDPR. For example:

- Data subjects don't have the right to rectification or correction of their personal data that is held by an organization.
- Businesses subject to CCPA don't have the data minimization mandate of GDPR.
- Businesses subject to CCPA are not required to maintain documentation on where personal data is processed and for what purposes, nor to appoint a Data Protection Officer. Both of these requirements are key elements in the GDPR.

Finally, while California is a populous state, the law applies only to Californian residents and not to the broader United States or North America. CCPA is a local initiative, not a coordinated multi-state one like GDPR.

As a response to the GDPR, the govern-ment of the State of California implemented the CCPA.

KEY ELEMENTS OF THE CCPA

An organization has to comply with the provisions of the CCPA if it passes four threshold tests—that it operates for a profit, that it collects personal information on Californian consumers, and that it controls what happens with the processing of that information. The fourth threshold test requires at least one of three criteria to be met:

1. Annual gross revenues are more than US$25 million.
2. The business buys, receives, sells or shares the personal data of 50,000 or more Californian consumers, households or devices per year.

3. More than 50 percent of its annual revenue comes from selling the personal information of Californian consumers.

In the age of online gaming, smartphone apps, and online services in general, these thresholds will be crossed by many US and non-US organizations.

The implications include:

- The need for clear provenance of personal data collected or acquired on individuals, including geographical identifiers that will signal applicability of the CCPA.
- The need to develop processes to respond to access and deletion requests, as well as safeguards to apply appropriate data security for personal data.
- Processes for ensuring the authenticity of an access or deletion request. Identity theft is one of the key outcomes of past data breaches, and it is plausible that a malicious actor could use a stolen identity to gain further personal data and inflict even more financial and material damage on an individual.
- As with the GDPR, the CCPA raises the question of policy scope. One option is to follow the letter of the individual laws in each of the legal jurisdictions in which an organization operates, affording only the personal data rights enshrined in each jurisdiction to those affected. The second option is to take a higher-level view of data protection requirements, affording a universal set of rights to all people everywhere the organization operates. The first creates a fragmented, complex and ever-changing patchwork of policy, while the second creates a simpler and consistent policy framework.

As with the GDPR, the CCPA raises the question of policy scope.

PRIVACY REGULATIONS ARE SPREADING

The GDPR has applicability for data subjects in Europe, but given the extra-territorial scope of this applicability, we have previously called it the "Global" Data Protection Regulation instead of the "General" Data Protection Regulation. GDPR is indeed having global effects, with more than 100 countries around the world implementing laws that draw on the principles of GDPR. Few are as extensive as GDPR, but many share similarities. For example:

- **India**
  India's Personal Data Protection Bill of 2018 is very closely aligned with the GDPR, including rights for individuals, the tiers and scope of administrative fines, and the need for a legal basis for processing personal and sensitive personal data. Several differences also exist, such as the requirement for absolute data localization for "critical personal data," although interestingly this phrase is not specifically defined, and that the State gets its own legal basis.
- **Brazil**
  The new General Data Privacy Law 2018, or Lei Geral de Proteção de Dados Pessoais (LGPD), was signed into law in August 2018, and will go into effect in February 2020. LGPD contains many of the same privacy principles of the GDPR, requires a legal basis for collection and processing, applies in-country and extra-territorially, and adopts the two percent of global revenue fine level (but not the four-percent one). Data breach notifications are also required. Brazil is yet to create an independent data protection authority, since the President vetoed this section of the law, stating that the task of creating such an agency sat with his office and will be forthcoming.
- **Australia**
  Australia recently introduced a new data breach notification law (in February 2017) that extended its existing data privacy legislation. Australia lacks a GDPR-type law at present, although some murmurs are starting to be heard about

Australian's owning their online footprint and personal data, which could indicate a GDPR-type initiative will be forthcoming shortly.

Several other jurisdictions have strengthened their data breach notification requirements – such as Colorado – although most of these breach-oriented initiatives lack the breadth of GDPR and don't create the consumer rights of access, erasure, rectification, and limitation of processing, among others.

PENALTIES UNDER THE GDPR

The GDPR, CCPA and other data protection regulations introduce significant penalties for non-compliance, with GDPR in particular elevating the thresholds from previous levels. GDPR has two levels of fines for non-compliance, the lower of which is 10 million Euros or two percent of total worldwide annual turnover from the preceding financial year, whichever is the highest (Article 83). The higher level is twice this, and applies to situations such as not complying with the basic principles of processing (including conditions for consent), withholding data subjects' rights, and transfers outside of the EU that are unauthorized or inappropriate. Data subjects can also seek damages through the civil courts.

The new penalty levels in the GDPR will prove costly. For example:

- The fine of £500,000 levied by the Information Commissioners Office in the UK in September 2018 against Equifax Ltd, the UK branch of Equifax Inc., for its shortcomings as part of the Equifax breach would have been much higher under GDPR (and the new Data Protection Act of 2018 in the UK which brings GDPR to the UK). The timing of the breach meant the fine regime under the old Act had to be used; it would have been at least 20 million Euro if GDPR / DPA 2018 applied.

- The Facebook data breach disclosed in September 2018 opens Facebook to a potential maximum fine of US$1.63 billion, should the Irish data protection agency find negligence and shortcomings in its data protection measures.

- The privacy advocacy group None of Your Business lodged complaints for the violation of data protection rights against Google, Facebook, Instagram and WhatsApp on May 25, 2018. If upheld, the maximum fines would reach almost US$5 billion for Google, and US$1.63 billion each for Facebook, Instagram and WhatsApp.

The GDPR, CCPA and other data protection regulations introduce significant penalties for non-compliance.

Other regulations are similarly strident. For example:

- The CCPA provides two levels of fines – US$2,500 or US$7,500 per violation with no maximum – along with the provision for people to bring lawsuits for data breaches at a rate of US$100 to US$750 per incident, or at a higher level if actual damages can be demonstrated to be more significant. The higher fine of $7,500 applies to intentional violations, or for situations where a business has not taken the required and reasonable steps to protect personal data. At these rates, a data breach could be extremely costly, such as when 3.5 million records in Los Angeles County were left accessible on an unsecured Amazon hosting service.

- The new Personal Data Protection Bill of 2018 in India introduces both the two-percent and four-percent fine levels of the GDPR, along with a criminal liability route with jail terms and public disclosure. At the two-percent level, the other way of calculating the fine is set at 50 million Indian Rupee (about US$700,000). At the four-percent level, it's 150 million Indian Rupee (about US$2.1 million).

- The new General Data Privacy Law of 2018 in Brazil adopts the two-percent fine level from GDPR, but not the four-percent one. In the Brazilian law, the maximum penalty for non-compliance is two percent of gross sales (for the

company or a group of companies), or R $50 million per infringement (about US$12.9 million).

- Penalties are also increasing in jurisdictions that focus more on data breaches and notifications rather than wider data protection principles and approaches. Arizona's data breach notification law allows for a penalty of up to US$500,000 for willful violations, and Australia's data breach notification law allows for a penalty of up to A$1.8 million for organizations. As regions and countries take a wider data protection view, we expect to see these fines increase significantly.

REMEDIATION CAN BE COSTLY

While legislation introduces costly fines for violating the principles of data protection, there are other costs as well:

- The costs to investigate a data breach and pay associated legal costs
- Reputational damage
- Decreasing market valuation
- Lost consumer confidence
- Lost revenue

For example, the Pentagon disclosed a data breach in early October 2018 that occurred via a contractor, and has initiated proceedings to cancel its contract with the vendor in question. Likewise, the data breach at Target in 2013 resulted in a US$18.5 million fine for Target, but Target also paid US$202 million in costs for its internal investigation and legal fees.

Without a federal law on data protection in the United States, individual states will continue to push ahead with passing their own privacy legislation. Much like the complexity of compliance in Europe under the Directive, this patchwork of legislation will:

- Create a complex set of state-level variations and exclusions, with some states requiring one thing and other states the opposite.
- Undermine the ability of the United States to remain united in an age of digital markets that rapidly and seamlessly span across states.
- Stimulate a gold rush mindset among legal firms, and facilitate an environment where more time and money is spent on legal fees than actually implementing data protection to protect the rights of data subjects.

Note that even without a federal law in the United States on data protection and privacy, the recent US$148 million fine against Uber for its poor handling of its 2016 data breach sets a new benchmark and shows a new willingness to impose punitive fines. Many of the individual state Attorneys General worked together to investigate the Uber case, and the punitive fine reflects Uber's flagrant disregard for due process after a data breach. The fine is much higher, by comparison, than the US$18.5 million settlement in 2017 between Target and 47 states for its 2013 data breach.

While legislation introduces costly fines for violating the principles of data protection, there are other costs as well.

RULINGS SINCE THE GDPR CAME INTO FORCE

GDPR came into force on May 25 and regulators have been working on various matters since that date:

- The European Data Protection Board, the EU-level agency created by the GDPR to coordinate the efforts of member state data protection authorities, has held three plenary sessions and is gearing up for a conference in late October 2018. Topics in the second and third plenary sessions included consistency and cooperation on cross-border issues, reviewing the draft adequacy decision with Japan, and identifying common elements for Data Protection Impact Assessments, among others.

- Reviewing the complaints that have been lodged, and deciding which ones to pursue in the short term. It is expected that the first fines in line with GDPR will be issued before the end of 2018, along with reprimands for data controllers, preliminary and temporary processing bans, and ultimata for serious data protection failings. Few details are available on which data controllers are under investigation, although we know that the data protection agency in Ireland is investigating the data breach of 50-90 million accounts that Facebook disclosed in late September 2018.

- Several data protection agencies have noted an upswing in the number of data privacy complaints and data breach notification since May 2018. The French agency noted an upswing of 64 percent in the number of complaints compared to a year ago, Italy saw a 53 percent increase, and the Irish agency said it received 1,300 complaints or concerns in the first week after GDPR came into effect.

More information on the European Data Protection Board is available at https://edpb.europa.eu/edpb_en.

ADMINISTRATIVE FINES

It is still too early for any administrative fines to have been levied on the basis of GDPR. Fines that have been imposed since May 25, 2018 have been on the basis of earlier regulations, although several current investigations are likely to result in large fines under GDPR due to the post-May 25 timing of the incidents. Specifically:

- The Information Commissioners Office (ICO) in the United Kingdom issued an enforcement notice against AggregateIQ in July 2018, a data analytics firm in Canada. The notice requires the cessation of processing of personal data obtained before GDPR come into force, which it acquired from several pro-Brexit organizations in the UK. If AggregateIQ does not comply with the notice, it may be subject to an administrative fine of the higher of four percent or €20 million. ICO is proceeding against AggregateIQ based on the UK's new Data Protection Act of 2018, the update that incorporates the GDPR into UK law.

- In September 2018, the ICO fined Equifax Ltd, the UK arm of Equifax Inc., for its role in the 2017 data breach that affected 146 million customers worldwide. Since the data breach occurred before GDPR came into force, the maximum fine permissible for the ICO was £500,000 (under the Data Protection Act of 1998); if it had been after GDPR, the fine would have reached the four percent or €20 million level. The ICO contends that Equifax Ltd contravened multiple data protection principles, hence the higher penalty level would have applied.

- The ICO also levied the maximum fine under the Data Protection Act of 1998 of £500,000 against Facebook in July 2018, for its role in the Cambridge Analytica data breach. The ICO accused Facebook of failing to safeguard people's information, and for lacking transparency in how data was used by other organizations. If the breach had occurred after GDPR came into force, the administrative fine would have been much larger.

- Facebook, already embattled from fake news, Russian interference in politics, and the Cambridge Analytica privacy breach, announced a data breach in late September 2018. Facebook's initial disclosure said the breach directly affected something on the order of 50-90 million users, although the details released by Facebook on exactly what was and wasn't breached remain unclear. This was updated in early October with specific details on what was breached for the 30 million users that were actually affected. The Irish Data Protection Authority is investigating. Administrative fines for the provisions in GDPR covering data breaches are set at the two percent level (or €10 million, whichever is highest), which on US$40.6 billion of revenue for 2017, would stand at US$812 million. If Facebook is deemed to have broken multiple requirements under GDPR, the fine could range to a maximum of US$1.624 billion[ii].

Several data protection agencies have noted an upswing in the number of data privacy complaints and data breach notification since May 2018.

- Uber suffered a data breach of personal data on 57 million customers in 2016, and tried to cover it up through a payment to the hackers. The breach was disclosed in late 2017, and Uber has recently been handed a US$148 million fine by most of the US states and Washington DC. This is not a GDPR fine, but is the largest ever handed down for a data breach in the United States. If the data breach had occurred after GDPR come into force, it would face a maximum penalty under GDPR of US$400 million.

- Finally, while no fine or warning has been given yet, Google may be subject to one shortly for its abuse of location data, a sensitive data element under GDPR. The abuse entails continuing to collect individuals' location data from their iOS or Android smartphone, even after users have said they don't want their location tracked, and also the inclusion of this no-consent-given location data to form part of the profile made available to advertisers. The Irish data protection agency, for example, has asked Google for more information on its usage of location data[iii].

The Current State of Readiness for the CCPA

Exactly how the CCPA will come into force remains unclear, as there are continuing changes regarding CCPA and wider machinations to render it void. On the former, several technical amendments were put forward in August 2018, and the Attorney General for California – who has multiple responsibilities under CCPA – lodged his concerns with various matters in a letter also in August. Looking more broadly, several large companies are lobbying Congress to develop a federal approach to data privacy in the US that will supersede the CCPA and other state-level initiatives, although some of these recommendations fall far short of the principles in the GDPR. Google, for example, argues that it can best determine what data privacy means for individuals (Google wants the freedoms of ownership over personal data, not the limitations of stewardship), and is against the core GDPR principle that a data subject owns his or her own data. Google also argues for limits on the quantity of data that can be held about an individual, a provision and concept that is not in GDPR (data minimization in GDPR is different to data caps per Google). For organizations subject to GDPR, it provides the level high ground at this point that should be used for lowering risk until greater clarity is achieved on the situation in the United States.

The GDPR, CCPA and other data protection regulations address a common general theme, but there are overlapping requirements, regional variations, and multiple inconsistencies.

What Should Your Organization Be Doing to Prepare and Comply with the GDPR and CCPA?

The GDPR, CCPA and other data protection regulations address a common general theme, but there are overlapping requirements, regional variations, and multiple inconsistencies. Organizations operating in a single market under a single regulation will have a clearer regulatory pathway, but this is increasingly difficult with online commerce, digital markets, and globalization. While there will always be regional variations to account for – such as notification timeframes and contact details – organizations facing the need to comply with multiple data protection regulations will have to decide on one core guiding principle: to only offer specifically what is required per market, or to more broadly offer the same rights to all consumers anywhere in the world.

The choice of a guiding principle will dictate the complexity of an organization's compliance journey, and with either pathway the following principles will be necessary for compliance.

MANAGE DATA WELL

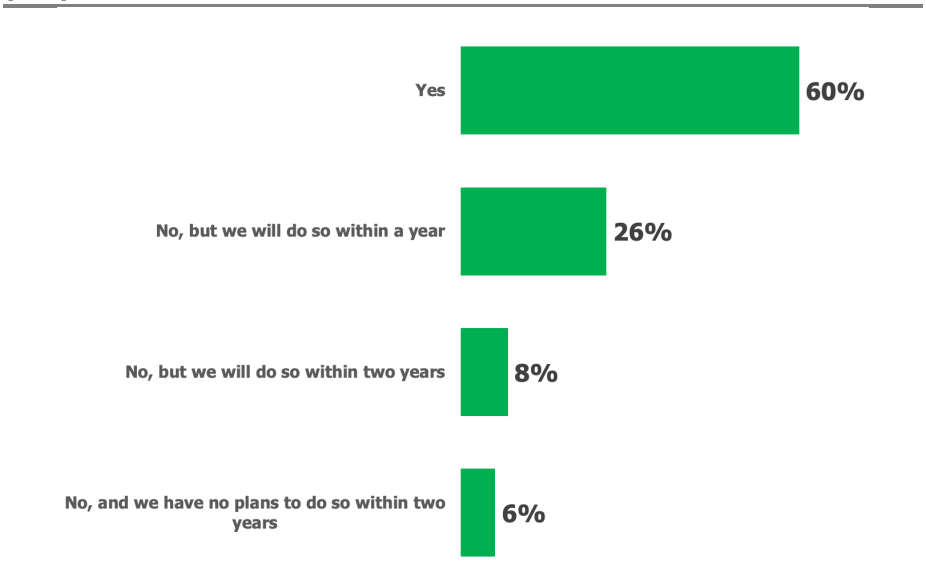
GDPR and CCPA, among others, impose a high duty of care on the management of personal and sensitive personal data. For example, while data must be protected in several ways, organizations must also have clear provenance on where personal data has come from and who it is about if they are to respond correctly to access, deletion, and if applicable, rectification requests. GDPR also requires that data is managed well in terms of transferring it outside of the European Union, and prescribes controls that need to be in place for cross-border transfers.

MANAGE GOOD RECORDS ON WHY DATA IS HELD

Under GDPR, data can be processed only under one of six legal bases, such as direct consent, contractual performance, and legal obligation (Article 6). The legal basis under which data is initially collected and processed has consequential implications, such as for erasure requests, because data does not have to be deleted under all legal bases. Good records are also required when a data controller is considering additional processing beyond the initial purpose, because this requires a contextual balancing of interests (the data subject and the data controller). The CCPA requires something similar, in a way, due to its requirement that data controllers advise consumers as to what data they are collecting or have acquired on them, and because consumers can request deletion of this data, the non-exercise of a deletion request is effectively the legal basis of consent.

Yet, many organizations are not managing their data well, particularly with regard to the consent of data subjects whose data is being managed. As shown in Figure 2, the research conducted for this white paper found that a significant proportion of organizations have not yet reviewed how they obtain consent from customers and others – a key element of privacy regulation, particularly the GDPR.

Figure 2
"Has your organization reviewed how you obtain consent from customers, prospects and others?"



Source: Osterman Research, Inc.

GDPR and CCPA, among others, impose a high duty of care on the management of personal and sensitive personal data.

MAINTAINING GOOD RECORDS ON DATA PROCESSING

Under GDPR, both data controllers and data processors must maintain an accounting of processing activities under their responsibility that include personal data. Controllers need records that show who is responsible, the intent of the processing activity, which categories of personal and sensitive personal data are being

processed, the types of people who see the output of the processing activity, time limits for retention, and which technical and organizational measures are in place to protect the personal data. Processors have a similar, albeit shorter, list of requirements. The records of processing activities must be provided to the supervisory authority on request. Some exclusions apply to smaller organizations with fewer than 250 employees.

Managing data well should also mean proactively deleting data that is no longer required for future processing activities, and in some cases using anonymization techniques to remove the personal data while maintaining aggregate records for business reporting and trend analysis.

ACT LIKE A STEWARD

Newer data protection regulations enforce the principle that personal data is owned by the data subject, not the organizations who collect or process it. Requirements for data controllers on giving notice to data subjects on what is being collected, providing access to what is held, and deleting data on request – albeit with provisios and exceptions for each requirement – clearly establishes the role of the data controller as a steward, not the owner. GDPR establishes several additional rights that the CCPA, for example, does not offer, including the right to rectification, the right to object to processing, and the right to human review of automated processing that results in a decision with legal effects for the data subject. While multi-national organizations face a patchwork of regulations on data protection, there is a growing body of legislation with enough common elements to tip the stewardship vs. ownership balance in favor of data subjects.

Newer data protection regulations enforce the principle that personal data is owned by the data subject, not the organizations who collect or process it.

DATA PROTECTION BY DESIGN AND DEFAULT

Both GDPR and CCPA impose elevated responsibilities on organizations handling personal data. GDPR requires that data protection is "by design and by default" (Article 25), and specifies the need for both technical and organizational measures to meet this requirement, with means such as pseudonymization, encryption, data minimization, data protection impact assessments, and the ability to demonstrate compliance. Although the CCPA doesn't explicitly require an elevated standard of data protection that is "by design and by default," many of its provisions create the need for such a standard. For example, businesses need to be able to verify the identity of a consumer requesting their own personal data, businesses must delete personal data when requested by a consumer (which requires explicit data modelling and tracking of where personal data is stored and used), and businesses must know whether a given consumer's personal data has or has not been sold or disclosed to a third party. Businesses must also have processes in place for discovering that a data breach which includes non-encrypted or non-redacted personal data has occurred. Since these capabilities are required under CCPA, their lack would indicate intentional violations of the law, it is incumbent on affected businesses to develop the necessary organizational and technical measures to protect personal data.

SECURITY OF PROCESSING

Assuring security of personal data means more than just preventing unauthorized access to personal data. In Article 32 of GDPR, additional security of processing measures include ongoing confidentiality, integrity, availability and resilience of the processing systems and services. It also calls out the need to restore availability and access to personal data after a physical or technical incident - such as a power outage or storage system failure - and requires a regular testing regime to check the veracity of both technical and organizational measures. All of these requirements are to be contextually balanced against the state of the art, costs of implementation, the nature, scope, context and purposes of processing, and the risks likely to be experienced.

MAINTAIN RECORDS ON CONSENT

The GDPR is much more explicit than CCPA on the requirements around consent. GDPR Article 6 (on legal bases) and Article 4 (definitions) together require that if

consent is used as the legal basis for collecting and processing personal data, the data subject must have provided it via a "freely given, specific, informed and unambiguous indication" of their wishes. Consent under GDPR cannot be implicit, opt-out, or the result of pre-ticked boxes (that is, the default consent option is set to yes). CCPA doesn't have the same concept of legal bases, only that Californians "know" what personal data is being collected, "know" if it is being sold or disclosed to others, and can opt-out of such sales and/or require the deletion of their personal data. Hence consent under CCPA is implicit – if the business has provided notice of activities pertaining to their personal data, and for as long as the data subject does not exercise his or her rights, there is effectively the legal basis of consent.

What is explicit under GDPR and implicit under CCPA, therefore, still requires the following minimum common record keeping:

- That data subjects have been fully and clearly advised on the types of personal data being collected on them.
- That consent has been gained explicitly, or in case of CCPA, has not been withdrawn.
- Dates when consent was gained explicitly or implicitly, and when it was withdrawn (if applicable). Specific dates are required to safeguard the validity of data processing activities between the two dates.

BE ABLE TO RESPOND TO ACCESS REQUESTS

Data subjects (under GDPR) and consumers (under CCPA) have the right of access to the personal data held and processed about them. Once a data access request is received, organizations need streamlined processes in place to identify where the individual's personal data is being used, why it is being stored or processed, and its provenance. Since notice must already have been given to data subjects/consumers on what data was being collected, there should be no surprises as a result of this process, unless additional unauthorized or unexpected processing activities have been performed. Organizations should also inform data subjects of their subsequent rights, such as erasure, and if applicable, limitation of processing and rectification. While each data subject individually can only request data access without fee infrequently, receiving data access requests from thousands of data subjects that require manual processes to satisfy will be costly and time consuming.

Data subjects (under GDPR) and consumers (under CCPA) have the right of access to the personal data held and processed about them.

DATA BREACH REPORTING

Reporting data breaches is a common requirement of new data protection legislation, in part because it enables affected data subjects to be extra wary of the misuse of their breached data for identity theft, financial harm, or other damaging outcomes. Data controllers and data processors must have the mechanisms in place to identify a data breach, the internal notification and escalation pathways established, and documented processes for providing notice within the timeframes required. If data subjects have to be advised, organizations should have systems in place to manage the notification process. It is important to note that a secure method of communications is a baseline requirement for protecting notifications that are sent under the requirements of the GDPR.

KNOW THE VALUE OF PERSONAL DATA

The CCPA entitles a business to charge a higher price to a consumer for a product or service if the consumer opts out of the sale of their personal data, as long as the higher price is reflective of the value that the business loses by not being able to sell their personal data (Section 1798.125). In order to exercise this right, businesses must have defensible documentation on the value they miss out on by not being able to sell personal data to third parties.

MAINTAIN THE PRIVACY OF DATA SUBJECTS

The intent of both GDPR and CCPA is to safeguard personal data and ensure appropriate protections are established to meet this requirement. Under GDPR, data controllers must not process sensitive data on people unless explicit consent has been gained, it is necessary to protect their vital interests, or one of the other exclusions apply. Data protection impact assessments are necessary to ensure that data processing activities are appropriately safeguarded, and where multiple data controllers are working together with personal data, they must jointly determine how to safeguard personal data in full knowledge that both are individually responsible for giving data subjects their rights. In selecting data processors, data controllers must ensure they are compliant with the requirements in GDPR, because while data processors have responsibilities under GDPR, the use of a data processor does not reduce the responsibilities and liabilities of a data controller.

OTHER REQUIREMENTS

The GDPR contains several requirements that the current CCPA does not. For example:

- With some exceptions, data controllers and data processors must appoint a Data Protection Officer (DPO), who will play a key role in matters related to protecting personal data. The DPO has a set of assigned tasks, must report to a high level in the organization, and must be accessible to data subjects for questions on processing their personal data and how to exercise their rights. He or she must have expertise in the field of data protection.

- With some exceptions, data controllers and data processors who are not based in the European Union must appoint a representative based in one of the Member States of the European Union. The appointment of a representative must be a formal activity, and he or she must be available for communication and interaction with both supervisory authorities and data subjects in regard to data protection under GDPR. The role of the representative is different to the role of the data protection officer.

The GDPR contains several requirements that the current CCPA does not.

Solutions to Consider for Compliance

Organizations subject to GDPR, CCPA and other data protection and data privacy legislation require a multi-faceted approach to compliance that includes a balanced set of organizational and technical measures. Technical measures should include:

- **Security from Threats**
  Endpoints, gateways, and cloud services must have sufficient safeguards to prevent unauthorized access, stop unauthorized changes, and protect personal data from malicious threats that attempt to compromise data integrity. Questionable and suspicious activities should at minimum generate alerts for further investigation, and in high risk situations, instantiate automated actions that safeguard personal data. Security tools should also continually assess endpoints, servers and other systems to new threat possibilities via out-of-date and unpatched operating systems and applications.

  There are a variety of security technologies and processes that are important to consider in the context of compliance with the GDPR, CCPA and other privacy regulations. These include threat intelligence and threat analytics that can help analysts to understand the source of potential data-breach focused threats and gain more information about them, user behavior analytics (UBA) and user and entity behavior analytics (UEBA) that can detect inappropriate actions by users or endpoints that could lead to privacy violations, Security Information and Event Management (SIEM) solutions that can help security analysts to collect and correlate log data as part of threat hunting activities, next-generation firewalls, web application firewalls and the like.

- **Security of Processing**
  Technical measures are likely to be required to ensure the confidentiality, integrity, availability and resiliency of processing systems and services, along with the ability to recover after a technical or physical incident. If the nature and scope of the data processing requires it, measures that deliver these capabilities are an essential part of the security mandate in GDPR.

- **Device and Data Encryption**
  Encryption solutions render personal data unintelligible and inaccessible to people who lack access authorization and rights, and encrypting all data storage on devices implements broader protections. Both GDPR and CCPA mention encryption as a data protection safeguard, and if personal data is encrypted to a sufficient level, it is much more difficult to pull off a successful data breach, and organizations are excused from breach notification requirements if strong encryption was in place for the breached data.

  Encryption isn't just a one-time action, however. It is essential to ensure that encryption remains operational – thereby preventing a breach through the removal of that encryption and subsequent access to personal data stored on a device or service. This requires continuous insight into encryption status across endpoints and other services. The Data Protection Commission in Ireland, for example, received a data breach notification in August 2018 related to the unintended removal of encryption from around 1500 laptops. And the breach at Heathrow could have been prevented by the use of an encrypted thumb drive, although other organizational failings were also cited by the ICO in the UK[iv].

- **Backup**
  Personal data that is copied to a backup solution to enable disaster recovery will still require safeguards and protections. This includes limitation of access to backup media, limitation of access to backup files, and in the case that a backup is put back into service as part of a recovery operation, the intelligence to enforce erasure requests that were initiated subsequent to the backup being created.

- **Archiving Solutions**
  Outdated and unnecessary data can be moved out of production systems into an archiving system, thereby reducing the quantity of personal data accessible through current systems, decreasing the potential data breach surface, and yet still providing access to authorized individuals as required. Archiving solutions still need to enforce data protection safeguards over personal data, however, and must have the ability to delete personal data if it matches the conditions of a valid deletion request, prevent data breaches, and enforce access controls.

- **Data Governance Solutions**
  Appropriate care is required to ensure data is retained for the right reasons, processed for as long as processing is valid, authorized, and not objected to, and deleted wherever it exists when a valid deletion request is received. This requires advanced data governance tools that can identify personal data, manage retention, and enforce deletion under the right conditions.

- **Geo-Ring Fencing**
  Transferring personal data outside of the European Union border requires a valid basis for doing so, along with the presence of controls to ensure ongoing protection over that data. Geo-ring fencing where data is stored in the world—either through local infrastructure or cloud services with explicit data residency options—provide a way of minimizing cross-border transfers.

- **File Analysis and Data Classification Solutions**
  Protecting personal data in structured databases and fit-for-purpose corporate systems is much easier than protecting personal data in unstructured systems and free-form repositories. File shares, SharePoint document libraries, email

Transferring personal data outside of the European Union border requires a valid basis for doing so.

messages, Excel spreadsheets, Word documents, local drives, backups, and non-sanctioned cloud apps all present great risks to personal data. Data classification tools reduce the risk of unauthorized access and data breaches by proactively seeking out personal data in unstructured systems and formats and automatically applying appropriate mitigations. Data classification tools should work both in real-time as data is being created, and periodically to ensure no new unprotected personal data has been introduced to the environment.

- **Pseudonymization and Anonymization**
  While encryption uses a random mathematical key to obfuscate data values, encryption can be circumvented if the encryption key is also breached. Pseudonymization and anonymization are two alternative ways of introducing obfuscation of personal data; the first involves substituting a personal data value with a lookup identifier to a separate system, and the second replaces personal data with a meaningless string. The risk of both is unauthorized reversal of the process, with pseudonymized data holding the greater risk of the two. If used, both approaches need to be done in light of this risk, and should apply to production systems, testing and development environments, and archived data.

- **Data Loss Prevention/Data Breach Identification and Adaptive Protection or Blocking Solutions**
  Data loss prevention (DLP) tools search for personal data in email messages, attachments, and other systems that send data between people, and depending on the specific DLP solution, can apply adaptive protection or block the message from being sent. For example, if a social security number is identified in an email message and the recipient is not authorized to receive the number, a DLP solution could block it from being sent. Alternatively, if the recipient was authorized to receive the number, the message could be automatically encrypted to introduce protection. DLP solutions require effective pattern-matching algorithms that identify and classify personal data, and a range of mitigations to protect it. DLP solutions help prevent against accidental data breaches by employees.

- **Data Infiltration**
  Just as technologies are required to identify and prevent data exfiltration, so to should there be checks in place to identify and prevent data infiltration. For example, if a new employee joins from a competitor and brings a spreadsheet containing customer details (name, contact details, products used, revenue levels), it incumbent on the new organization to block the new data from being added to their systems. A policy statement to this effect will also be necessary in the employee's code of conduct and onboarding process.

- **Identity, Access and Management Solutions**
  Limiting who has access to personal data – and especially to sensitive personal data – is a key tenet of data protection. Identity, access and management solutions enforce unique identifiers for each employee, with one or more authentication demands required before access is granted to personal data. Organizations that permit shared login credentials will fall afoul of the intent of data protection requirements; this practice should be stopped immediately. Strong systems and processes to enforce identity and control access limits the attack surface area for personal data, and means that departing employees can be rapidly prevented from accessing personal data once they have left.

- **Data Portability Solutions**
  Both GDPR and CCPA require data controllers to supply a data subject with his or her data in a format that enables easy transfer to another data controller. This is the right of data portability. Depending on what types of personal data a data controller collects and processes, and the scale of this processing, will indicate what specific capabilities are needed.

Both GDPR and CCPA require data controllers to supply a data subject with his or her data in a format that enables easy transfer to another data controller.

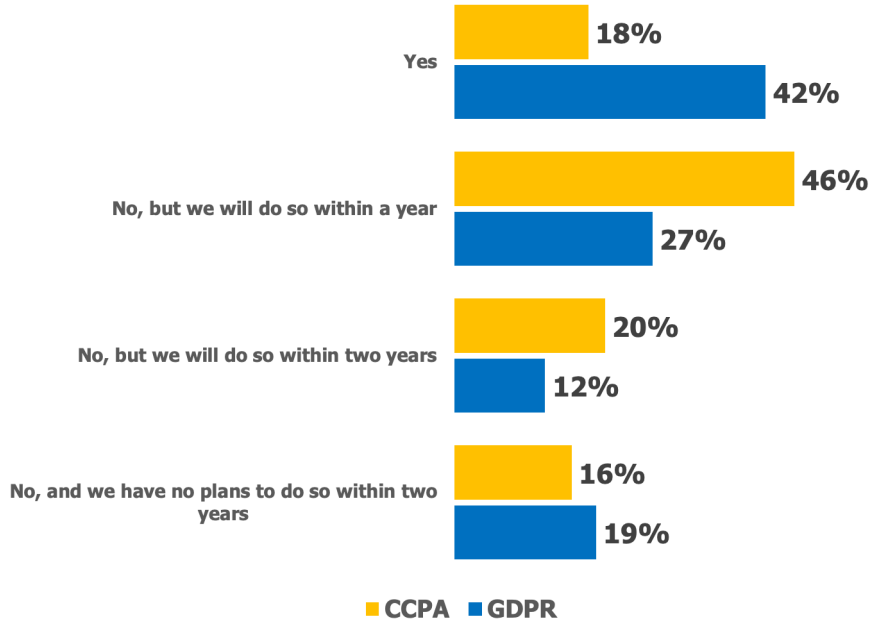
- **Application Security Testing**
  New applications that contain personal data must be tested for vulnerabilities. Application security testing tools provide automated testing methods to ensure silly mistakes are not made, vulnerabilities are identified, and mitigation pathways for weaknesses are identified before a breach takes place. The Conservative Party in the UK would have benefitted from such tools in September 2018, since its conference app exposed personal details on thousands of conference delegates, including members of parliament. It's a bad look when those responsible for data protection regulation in a country can't even get their own house in order.

- **Employee Training**
  Employee training is essential, because a solely technical approach to compliance is not enough – "organizational measures" are required in parallel in order to create a culture or atmosphere of data protection. When the UK's Information Commissioners Office fined Heathrow Airport Limited for the 2017 data breach via a lost unencrypted and non-password protected thumbdrive, it observed that only two percent of the 6,500 Heathrow employees had been trained in data protection, and that common working practices among employees were out of alignment with Heathrow's corporate policies on security. Employee training should cover such situations, along with specifying individual responsibilities to protect personal data, high-risk activities to avoid, and the dangers of using unsanctioned cloud apps to store and share personal data.

  Our research found that the majority of organizations have not yet undertaken training with regard to GDPR and CCPA compliance.

Employee training is essential, because a solely technical approach to compliance is not enough.

Figure 3
"Does your organization have a program in place to train your employees on their obligations and those of your organization under the GDPR and CCPA?"



Source: Osterman Research, Inc.

- **Other Technologies**
  There are several additional types of tools which elevate data protection measures for an organization, including incident response systems, mobile device management, privileged account management, and more. Organizations should take a wide view of the potential for undermining or compromising personal data, and put in place the best mitigations possible. While intentional actions to protect personal data may not be enough to prevent a data breach, for example, the fact that intentional actions have been taken will give strong evidence of the organizational intent to be compliant.

Data protection requires a balanced set of organizational and technical measures. The above technical measures, implemented in line with a clear view of the risks to personal data in an organization, in combination with complementary organizational measures, will help craft a strong data protection approach and culture.

Summary

Data privacy regulations like the GDPR and CCPA are becoming the norm and organizations must implement a variety of technologies and best practices to ensure compliance with them. A failure to comply with the growing patchwork of regulations will almost certainly result in significant and negative consequences, including direct financial costs through punitive fines, as well as loss of corporate reputation, lost business opportunities, brand damage and the like.

Sponsor of This White Paper

AccessData offers industry-leading solutions that leverage the power of forensics to help organizations more efficiently, effectively manage any digital investigation. For more than 30 years, AccessData has worked with more than 130,000 customers in law firms, corporations, law enforcement and government agencies around the world, to understand and focus on our customers' unique collection through analysis needs. AccessData solutions are provided both as stand-alone and enterprise-class tools that can synergistically work together.

The company is committed to helping its clients ensure the security and privacy of their data, and their customers' personal data. AccessData employees have contributed their time as volunteer members of the Electronic Discovery Reference Model (EDRM)'s GDPR Working group, tasked with helping to raise awareness about the importance of GDPR compliance and provide guidance on data privacy best practices. Furthermore, the company is focused on the development of new technologies that help organizations ensure compliance in the rapidly evolving world of privacy regulations.

www.accessdata.com

@AccessDataGroup

+1 800 574 5199

Appendix

This section provides an overview of some of the key requirements of the GDPR, but it is not meant to be an exhaustive compilation of all of the GDPR's requirements:. Organizations that are to remain in compliance with the GDPR must:

- Have a legal basis for controlling and processing personal data (**Article 6**). Legal grounds include direct consent from the data subject, for performance of a contract with the data subject, compliance with a legal obligation of the controller, protecting the vital interests of a data subject, and the legitimate interests of the controller. It is essential to be very clear on the specific legal basis for collecting and processing personal data, because some rights held by data subjects apply only to data held under one or two legal grounds, for example. While the "legitimate interests" basis appears to give wide sway to organizations, there are various provisions that limit its applicability, such as taking into account the context in which the data was collected and the relationship between the data subject and the controller.

- Collect and process personal data only for lawful purposes, and protect it at all times. Required protections include preventing accidental or unlawful destruction, loss, processing, disclosure, access, and alteration. Data subjects have significant rights and freedoms under GDPR, and these must be upheld through appropriate organizational and technological measures.

- Maintain documentation of all data processing activities (**Article 30**). Required details include the purposes of the processing, categories of data subjects and personal data involved, categories of recipients, safeguards on any data transfers, and if possible, time limits for erasure. A description of technical and organizational security measures is also required. These records are to be kept in writing or electronic form, and available for audit and review by the supervisory authority on request. Organizations with fewer than 250 employees are excluded from these documentation requirements, with some provisos.

- Perform an assessment on the risks to the rights and freedoms of controlling and processing personal data, and develop organizational and technological mitigations for the identified risks. The risk assessment has to include any third-party relationships for data held and processed on your behalf.

- Be able to demonstrate compliance with the GDPR, through organizational and technical measures, and the on-going assessment of the strength and suitability of these measures (**Article 25**). Demonstrating compliance includes having policies on how to protect data under your control, an up-to-date assessment of risks to personal data (e.g., unauthorized or overprivileged access), workable technical measures that enforce protection (such as encryption), rules on transferring data to other countries, a staff training and awareness program, the means to identify and investigate data breaches, and the means to respond promptly to data access requests by data subjects, among others. All of these measures are on-going: they need to work at all times, and having the means to verify the effectiveness of implemented measures is essential. Certification mechanisms are mentioned throughout the GDPR as well, highlighting the on-going nature of compliance. Overall, the clear intent of the GDPR is that personal data is actually protected, not merely that organizations implement data protection tools.

- Meet the elevated standard of consent, anytime consent is the legal basis for processing data (**Article 7**). Consent means "any freely given, specific, informed and unambiguous indication of the data subjects' wishes ... by a statement or by a clear affirmative action, [that] signifies agreement to the processing of personal data relating to him or her" (as defined in **Article 4(11)**). Consent cannot be implicit, the result of pre-ticked boxes, or silence. Consent must be documented (which means the data controller must be able to produce evidence

that consent was given). And among other stipulations, consent cannot be bundled (it must be given for each specific processing operation and purpose), and the data subject must be able to withdraw consent just as easily as they gave it. This elevated standard of consent applies to consent gained after GDPR comes into force in late May 2018, as well as to any pre-GDPR consent indications that will be used after GDPR goes live.

- Minimize the amount of personal data processed, a principle called data minimization (**Article 5(c)**). The intent of this requirement is that superfluous or extraneous personal data that is not required for a specific processing activity are not collected or processed. **Article 25** takes this requirement further, in addressing the requirement of "data protection by design and by default." Once personal data is no longer required for current data processing activities, it should be minimized through pseudonymization (a process of replacing direct and indirect identifiers with near-meaningless values, although these can be reidentified through specific means) or the data should be erased.

- Notify the supervisory authority of a data breach within 72 hours of becoming aware of the breach (**Article 33**), and under certain circumstances, notify every data subject whose data was breached as well (**Article 34**). A breach notification is not required to the supervisory authority if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons," nor to data subjects if the breach won't result in a "high risk" to their rights and freedoms. For example, if the breached data was encrypted with a sufficiently strong encryption mechanism, data breach notifications are not required.

- Appoint a data protection officer (**Article 37**), who can be an employee for one organization, a representative for a group of organizations, or an external consultant. This is mandatory for public authorities, and for organizations that meet one or both of two tests: core activities "consist of processing operations which ... require regular and systematic monitoring of data subjects on a large scale," or that special categories of data are processed on a large scale. The data protection officer (DPO) must have "professional qualities," "expert knowledge of data protection law and practices," and the ability to perform the tasks detailed in **Article 39**. Such obligations include informing and advising the controller and processor (and employees) of their obligations under GDPR, monitoring compliance, and being the liaison person with the supervisory authority. The DPO must "directly report to the highest management level" (**Article 38**), and is to be afforded independence in carrying out his or her tasks.

- Carry out a data protection impact assessment (DPIA) for envisaged processings that are "likely to result in a high risk to the rights and freedoms" of data subjects, and secure the participation of the designated data protection officer in the assessment (**Article 35**). High risks cover activities like automated processing and profiling, decisions that produce legal effects for people, large scale processing of "special categories of data," and the "systematic monitoring of a publicly accessible area on a large scale." The intent of such assessments is to force the pre-processing evaluation of what is actually necessary, how the processing activity could harm data subjects, and how to develop organizational and technical mitigations to reduce any foreseen harm. Under some circumstances, organizations must consult with the supervisory authority prior to undertaking the processing itself, and wait until the supervisory authority has ruled the processing activity to be lawful (**Article 36**).

- Ensure the protection of data during processing activities, through the implementation of "appropriate technical and organizational measures" (**Article 25**). These protection safeguards are to be implemented when determining how to carry out a processing, and at the actual time of carrying out the processing activity. The safeguards required are to be in proportion to the risks to the rights and freedoms of data subjects. **Article 32** lists technical and organizational security measures such as pseudonymization, encryption, processing system

confidentiality, integrity and resilience, and a regular testing process for ensuring the security measures actually work.

- Abide by specific conditions when processing special categories of data. **Article 9(1)** states the general prohibition: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." **Article 9(2)** then lists 10 exclusions to the general rule. Given the elevated harm that can accrue to individuals based on these special categories of data, greater protections are mandated. GDPR recognizes that the use of data may be sensitive, and hence seeks to limit such usage, which is why data protection impact assessments are generally necessary for processing special categories of data, the data protection officer must be across such processing, and consultation with the supervisory authority is required.

- Respond promptly to requests from data subjects about the personal data you control, process, or transfer about him or her (**Article 15**). The data subject has the right of access to know the purposes of the processing, categories of personal data processed, recipients or categories of recipients the data will or have been disclosed to, how long the data will be stored, their right to rectification or erasure, and more. If the personal data is subjected to automated decision-making and profiling, you have to provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." The first request from a data subject must be fulfilled free of charge, although "a reasonable fee based on administrative costs" can be levied for "further copies." **Article 63** adds that the data subject should be able to "exercise [this] right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing." **Article 63** goes on to suggest the use of a "secure system" that gives the data subject direct access to his or her personal data.

- Update and correct any inaccurate personal data held about a data subject, by various means including a supplementary disclosure from the data subject (**Article 16**). This is the flip side of the data subjects' right to rectification. Organizations will need tight integration across all data systems and processes to ensure data updated in one system is automatically and correctly updated across all other locations too.

- Permanently erase any personal data about a data subject under specified conditions (**Article 17**). These include the withdrawal of consent by the data subject (where consent was the original lawful basis for collection and processing), the data has been unlawfully processed, and the data subject objects to the processing of their personal data and there are no other legitimate grounds for continuing to process the data. If the data has been made public by the controller or processor, "reasonable steps" need to be taken to inform other controllers and processors of the erasure request.

- Be able to temporarily restrict the processing of personal data on request from the data subject under certain conditions (**Article 18**). These include contested accuracy, unlawful processing but erasure is not requested, and the data subject's need for the personal data for legal claims but where further processing is not necessary. **Article 67** outlines several methods for restricting processing, and requires that this fact "should be clearly indicated in the system."

- Supply personal data concerning a data subject in a "structured, commonly used and machine-readable format" in response to a request for data portability (**Article 20**). This requirement is limited to the personal data the data subject "has provided to a controller," and the data subject can request the controller to transmit the data to a new data controller "without hindrance" or in good faith.

There are various exclusions noted in **Article 20**, such as where other lawful grounds apply to future processing activities.

- Have alternative methods available for making decisions about people rather than just automated processing and profiling, such as human intervention (**Article 22**). There are several exceptions to this mandate, such as the necessity of processing related to contractual matters, exemptions under Union or Member State law, and where the data subject's explicit consent has been given (and not withdrawn). **Article 22** makes it clear, however, that whatever happens, the data subject's rights and freedoms must be safeguarded.

- Prevent data from being transferred outside of the EU to "a third country or to an international organization" unless specific protections are in place (**Article 44**). These protections can be either an adequacy decision by the European Commission (the target recipients have an adequate level of data protection; **Article 45**), or the controller or processor has appropriate safeguards in place and legal remedies available (**Article 46**), such as Binding Corporate Rules (**Article 47**), among others.

- Ensure additional restrictions are in place to safeguard the handling of personal data of children when services are offered directly to children (**Article 38**). Language aimed directly at children must be "in such a clear and plain language that the child can easily understand," (**Article 58**) and consent is required from "the holder of parental responsibility over the child" for children under the age of 16 (**Article 8**), although Member States can lower this to 13 years. One strong implication of this requirement is the ability to verify proof of age.

It should be clear from the above "brief review" that the GDPR demands many significant undertakings from all organizations controlling or processing personal data on natural persons in the European Union.

REFERENCES

[i] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[ii] https://investor.fb.com/investor-news/press-release-details/2018/facebook-reports-fourth-quarter-and-full-year-2017-results/default.aspx

[iii] https://www.dataprotection.ie/docs/EN/23-08-2018-Statement-from-the-Data-Protection-Commission-on-Google-and-the-use-of-location-data/m/1784.htm

[iv] https://www.dataprotection.ie/docs/EN/22-08-2018-Statement-by-Data-Protection-Commission-in-relation-to-Eir-breach-notification/m/1783.htm