jahia

Data Privacy In A Post-GDPR World

Because the way you manage your customer data defines you as a company

By Elie Auvray and Kristina Podnar

About the authors

Elie Auvray

Elie is the Head of Business Development and a board member of Jahia Solutions Group SA, a group he co-founded and led as CEO through 2017. Jahia aims to “Make Digital Simpler” with an open-source Digital Experience Platform that brings together content management, data-driven marketing, and great integrations to help its customers deliver true one-to-one digital experiences - all without sacrificing customer data privacly

Being a passionate software entrepreneur with more than 20 years of experience, Elie founded his first company - Voice, a software company - at age 22 in 1996 pioneering easy-to-use web application development. In 1999, Voice merged with the company of the former President EMEA of Cisco in order to create a global software provider, Reef Internetware that successfully raised 85 million euros in 2001 from international venture capitalist (Goldman Sachs, 3i, Viventures). Reef Internetware IP was acquired by Mediasurface in 2002.

Elie has a bachelor’s degree in Business & Tax Law from the University of Paris 2 (Panthéon - Assas) and a master’s degree in Contract Law. He also has a bachelor’s degree from the Business Law Institute (IDA) of the University of Paris 2 ((Panthéon – Assas).

eauvray@jahia.com

Kristina Podnar

Kristina Podnar is a digital policy innovator. For over two decades, she has worked with some of the most high-profile companies in the world and has helped them see policies as opportunities to free the organization from uncertainty, risk, and internal uncertainty.

As a principal at NativeTrust Consulting, LLC, a McLean, VA-based company founded in 2006, Kristina works with clients to bring clarity across the global organization and its regulatory environment to rapidly customize a policy framework that frees the organization to fully leverage digital in service of its larger mission.

Kristina has a BA in international studies and an MBA in international business from the Dominican University of California and is certified as both a Change Management Practitioner (APMG International) and a Project Management Professional (Project Management Institute). Her book, *The Power of Digital Policy* was published in March 2019.

me@kpodnar.com

Introduction: The way you manage your customer data defines you as a company

When the world opened for business on May 25, 2018, the European Union's General Data Privacy Regulation (GDPR) came into effect, permanently changing the way businesses around the world collect, process, and store data on EU prospects and customers. Indications suggest that many organizations didn't - and still don't - fully grasp the magnitude of the new legislation or the extent of its requirements:

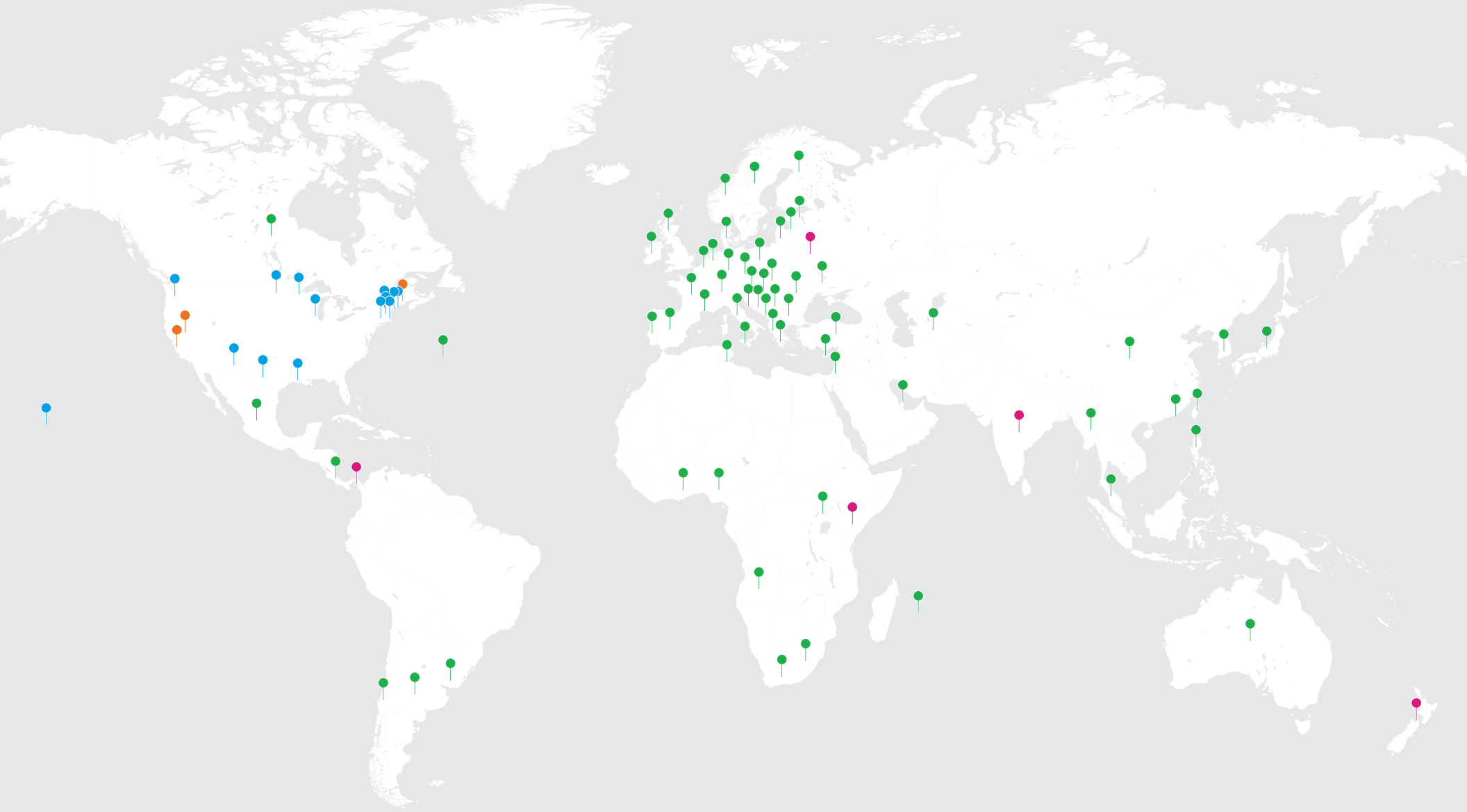
- According to research released by the International Association of Privacy Professionals (IAPP), only nine percent of privacy professionals in the U.S. and EU report their firms as fully compliant with GDPR requirements more than a year after its implementation.
- A survey carried out by the Ponemon Institute indicated that only 18 percent of respondents are highly confident in their organizations' ability to communicate a reportable data breach to the relevant regulators within 72 hours of becoming aware of the event…which is seen by 70 percent of respondents as the main GDPR security requirements they should principally address.
- Beyond GDPR, organizations are struggling with a patchwork of data privacy regulations popping up around the globe. In the U.S., executives of Amazon, AT&T, Dell, IBM, Qualcomm, SAP, Salesforce, Visa, Mastercard, JP Morgan Chase, State Farm, Walmart and others have called for a federal law around the subject, as their organizations have had to prepare not just for GDPR, but the California Consumer Privacy Act (CCPA) effective January 2020.

Organizations seeking compliance with the growing number of data privacy regulations will need to remain vigilant, especially those that rely heavily on personal data. And for those that have placed data privacy at the heart of their digital operations, the path to GDPR and subsequent compliance will be a smoother one.

This white paper mainly addresses the fundamental reasons for GDPR compliance, and the approach that organizations should consider. However, notice should be taken of rolling data privacy laws and regulations such as the California Consumer Protection Act (CPPA), the Protection of Personal Information Act (POPIA), and the Brazil General Data Protection Law (LGPD) which have similar goals and legal obligations:

- Recognition by the organization of users' personal data and the implied social contract of protecting that data,
- Consideration of the data privacy laws and regulations, and how they affect their organization and its digital operations, and
- Understanding of the data privacy requirements, which extend to integrating privacy into core business processes and, eventually, at the core of the business itself.

Changes to data privacy laws, and introductions of new laws, are being fueled globally by growing public concerns surrounding record-shattering data breaches and inadequate data-protection practices. It can be challenging to keep up on the latest regulations, some of which you may not have heard about before.



- Approved data privacy regulation
- Data Privacy regulation under construction
- U.S. Approved data privacy regulation
- U.S. Data privacy regulation under construction

Today, customer digital data privacy is not just a single country or regional concern, but rather it is a global expectation of prospects and consumers. This new norm is penetrating all aspects of online efforts, as summarized by the Internet Advertising Bureau (IAB) Lab 2019 San Francisco event: "Data Responsibility, The New Normal in a Consumer-Centric World"
https://www.iab.com/events/data-responsibility-innovation-day/

1 - What GDPR means for your organization

Overview

- What is it?
- Who is covered by the law? What's different about this legislation?

What is it?

The GDPR is the **European Union's General Data Protection Regulation**, which went into effect on May 25, 2018. Its purpose is to "harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy for EU citizens wherever they work in the world."

Who is covered by the law? What's different about this legislation?

The GDPR replaces the Data Protection Initiative of 95/46/EC.

Key changes include:

Increased scope: The GDPR greatly extends the jurisdiction of the previous law. Whereas the Data Protection Initiative was somewhat ambiguous as to whether it applied outside of the EU, the GDPR makes it clear that geographic location is not a factor. The law applies to data belonging to any EU resident, regardless of whether the related activity takes place within the EU. The law applied in both B2C and B2B context

Increased penalties: Non-compliant organizations can be fined up to 4% of their global annual sales or €20 million, whichever is greater. As we've seen, fines are being levied on a tiered approach in accordance with the seriousness of the violation.

Explicit consent: Organizations must obtain explicit permission to collect, process, or store personal data using language that clearly describes how the data will be used. Organizations cannot cloak the terms of consent in hard-to-understand, technical language or to rely on consumers to opt-out of unwanted communications. Moreover, consent must be use-specific, meaning that data collected for one reason (like downloading a white paper) can't be used for another purpose (such as targeted marketing emails) and that organizations cannot collect more data than is necessary for the stated purpose.

In addition, organizations must make it easy for EU residents to withdraw their consent at any time.

The law applies to any organization conducting business in the EU as well as to organizations outside the EU that collect, process, or store information on EU residents, regardless of citizenship. This includes:

Non-EU companies that employ EU residents (regardless of location)

Non-EU companies that collect, process, or store data on EU residents (even, for example, an IP address for a single individual)

It is a mistake for organizations to simply assume that they're not affected because they have no physical presence in the EU. As we've seen, the UK's ICO took enforcement action with Canadian firm Aggregatel Q, despite the company having no apparent presence in the EU.

Breach notification

Organizations must issue all required notifications within 72 hours of the time they become aware of a breach. Required notifications vary by jurisdiction but typically include regulatory authorities, consumers, credit reporting agencies, law enforcement, etc. Organizations must also provide credit monitoring to consumers whose data was compromised.

Right to access

Citizens and current EU residents have the right to know what data is being collected, how it's being used, where it's being processed, and who has access to it. In a significant shift toward empowering consumers, organizations (upon request) must provide an electronic copy, in machine-readable format, of the collected data free of charge. Users have the right to request that any incorrect information about them be corrected.

Right to be forgotten

In addition to the right to withdraw consent, consumers have the right to demand that their data be erased and that, in some situations, third parties cease any processing of their data.

Data portability

This provision of the GDPR introduces the concept of portability, which means that consumers have the right to request their data in an electronic format and then transfer that data to another processor.

Privacy by design

The concept of privacy by design isn't new, but the GDPR was the first piece of legislation to make it a requirement. It means that, instead of being a retroactive "patch," privacy should be an integral, ground-up part of digital business processes. One example would be collecting as much data as is truly necessary rather than collecting as much as possible.

Data Protection Offers

This is one of the few areas in which the GDPR makes things somewhat easier. Under the older legislation, the requirements for logging data processing activities were cumbersome and varied by jurisdiction. Under the GDPR, those notifications have been replaced with internal record-keeping requirements, and some organizations — those whose core activities involve the handling of certain amounts or types of sensitive personal data — must appoint qualified Data Protection Officers (DPOs) to oversee all related activities. And, because it's necessary for DPOs to be objective, they must be granted special employment protections.

What GDPR means for your organization ctd.

GDPR consequences for your organization

- How does the GDPR define “personal data”?
- How can organizations determine whether the law applies to them from a geographical standpoint?
- How can organizations determine whether the law applies to them from a functional standpoint?
- Is user consent always mandatory or is there an exception?
- Does the law affect B2B companies differently than B2C companies?
- Are there any categories of personal data that are exempt from the law’s requirements?

How does the GDPR define “personal data?”

The GDPR defines personal data as any information that can be used to directly or indirectly identify an individual. That includes things like name(s), photos, email addresses, banking information, social media activity, medical information, and IP addresses.

How can organizations determine whether the law applies to them from a geographical standpoint?

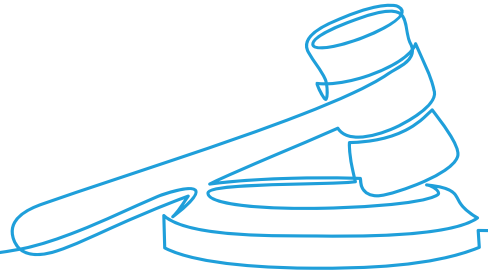
All organizations operating inside the EU are required to comply with the law. Organizations with no physical presence in the EU must comply if they:

- Sell or market goods or services to EU residents
- Employ EU residents
- Monitor the behavior of EU residents
- Collect, process, or hold the personal data of EU residents

The number of EU residents affected is not a factor. In other words, there is no minimum threshold. If even a single individual’s data is involved, the law applies.

In addition, third-party processors and controllers who work with the personal data of EU residents may have additional GDPR obligations, regardless of physical location. And outsourcing to a third-party processor outside of the EU doesn’t absolve a company of its own GDPR obligations.

As a consequence, there are few cases where GDPR does not apply. The fact that a company subcontracts the personal data processing to another company (even outside the EU) is irrelevant as soon as this company delivers products or services to European residents.



How can organizations determine whether the law applies to them from a functional standpoint?

The technical answer is that you need to know whether you're a processor and/or a controller as defined by the GDPR.

Controllers store personal data. A payment platform like PayPal is a good example.

Processors use that data for a specific purpose but don't store it once that purpose has been achieved. One example would be people who sell things online and use PayPal to process payments. They use a buyer's information for shipping and payment purposes but don't store that data after the transaction has been completed.

Organizations who process payments in-house rather than outsourcing them to a third-party provider may play the role of both processor and controller.

Keep in mind that, even when organizations outsource one or both of those roles, that doesn't absolve them of their responsibility to be compliant. Moreover, the company in charge of the personal data processing (defined as a "processor" by the GDPR) has additional obligations with regard to its customers:

- Provide guarantees that the way they process personal data meets GDPR requirements
- Provide guarantees that the way they protect the related personal data is aligned with current security standards
- Provide assistance and advice to customers that may be non-compliant
- Alert customers in case of a data breach

On a practical level, it's difficult to imagine a business that, in today's digital economy, wouldn't be covered by the GDPR from a functional perspective. Even public institutions, agencies, and associations are part of the GDPR scope of application.

Of particular note here is the need to alert customers in cases of a data breach. Data leaks are one of the worst thing that can happen to any brand. But the way they deal with leaks could do even more harm if the company can't show the security processes and infrastructure put in place to protect their customers. This is the reason why marketers, since they are the ones who deploy and use customer data tools, have to partner with their IT department at the very beginning of their initiatives. Data must not be managed in silos, especially since multiple teams - marketing, business and IT - are in charge of the deployment and usage of customer data-driven applications.

The recent Marriott and British Airways fines decided by the U.K.'s Information Commissioner's Office (ICO) are a wake-up call to how important this requirement really is.

Is user consent always mandatory or is there an exception?

Under GDPR, companies are able to collect prospect or customer data in any of these three scenarios:

- By getting the explicit consent from the prospect or customer
- If the data collection is required in order to fulfill a contract established with the individual
- As long as the organization has legitimate interest

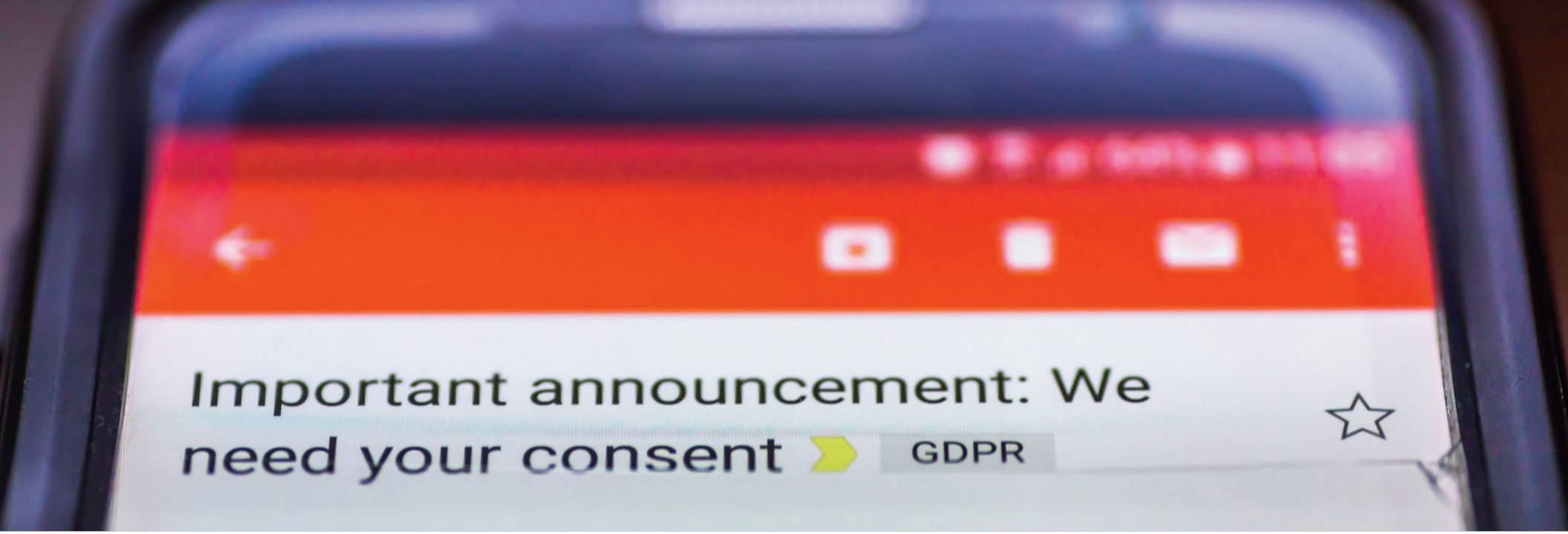
The first two scenarios are well understood but the third one - legitimate interest - is far more complex. A company can collect and use data without the consent of the individual if the purpose is based on legitimate interest.

But what does that really mean?

The GDPR indicates that any one of the following three instances allow a company to collect and process data without consent or contract.

- The company would be placing itself at risk if it did not collect or process the personal data for its own business purposes. For example, the data is transferred within the organization for internal administrative purposes. Or, the organization collects and uses the data for cyber security purposes. The GDPR also indicates that an organization may use the data if it is proof of a crime, breaking of a legal obligation, or in the interest of greater or national security. Of course, none of these reasons are justified if they limit or take away people's basic rights or freedoms.The company has collected data from an individual for reasons where that individual could reasonably expect the data will continue to be used or is processed.
- The company has an already existing relationship with the individual, such as that of a customer or an employee, and therefore is continuing to direct market or contact the individual because of that pre-existing relationship. In fact, the GDPR explicitly says that "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." This should be interpreted as consent to receive marketing or commercial offers from existing customers for similar goods or services and that consent is not required to do so. But the company still must provide a way for an individual to refuse the marketing or offers, or to opt out. It is easy to look at the legitimate purpose rule and continue existing marketing or communications activities. However, keep in mind that some existing European countries have laws in place that supersede this specific rule. For example, France has its own data protection law known as the Commission nationale de l'informatique et des libertés (CNIL), and an organization would be out of compliance with the law if it were to follow this "existing relationship" legitimate use scenario.

Should you have any doubt how to proceed, the answer is simple: Consent is king.



Does the law affect B2B companies differently than B2C companies?

There is a difference in the level of consent required to collect, store, and use personal data. The GDPR requires that B2C companies get specific consent to store a person's data or to communicate with them beyond the initial transaction (such as to send them marketing emails). B2B organizations, on the other hand, don't have to obtain explicit consent from other businesses. They merely need to make it easy to opt out of receiving further communications.

They do, however, have the same obligations as B2C organizations when it comes to the personal data of an individual employee of that company. For example, if the purpose of your business is to manage personal data on behalf of your customer, or if you are delegating that processing to another company, even though that contract could be considered as a B2B one, the substance of the relationship involves processing personal data. Therefore; each company will have to respect B2C obligations mentioned in the GDPR.

Are there any categories of personal data that are exempt from the law's requirements?

Yes. The GDPR does not apply to personal data that you're legally required to retain for specific purposes. This includes things like select employment records, tax records, records pertaining to legal actions, records of loans and mortgages, etc. Basically, personal data in records that you are legally required to maintain is exempt from GDPR regulations as long as it's used for those purposes only. For example, you can't extract personal information from mortgage applications and use it to communicate with applicants for unrelated purposes.

2 - What the LGDP, POPIA, and CCPA mean for your organization

What are the LGDP, POPIA and the CCPA?

While the industry has been focusing heavily on GDPR, there are a slew of other data privacy regulations that need to be noted. For example, the Brazilian General Law of Protection of Personal Data (LGDP), was published on August 15, 2018, the Protection of Personal Information (POPIA) Act was enacted in 2013, and the California Consumer Privacy Act (CCPA) was signed on June 29, 2018.

The common foundational goal of all of these regulations is to give consumers ownership, control and security over their personal data.

What are the consequences for my organization?

GDPR, LGDP (Brazil), POPIA (South Africa) and CCPA (California) are all setting a new level for Customer Data protection in their respective jurisdictions. However, every law and regulation has common requirements around:

- Accountability and governance
- Consent and processing
- Notification and data rights
- Privacy by design
- Data breach notification
- Data localization
- Children's online privacy
- Contracting and procurement

It is clear that the GDPR, LGDP, POPIA and CCPA overlap significantly where data subject rights are concerned. The laws also overlap with regards to applying the regulation to persons in their jurisdictions based on residency rather than citizenship. But the commonalities end when it comes to the finer details of each law.

The regulations also differ significantly from the GDPR when it comes to violation penalties. For companies found to violate the regulation, LGDP fines them up to 2% of their yearly revenue or 50 million Braziian Reals ($12 million), whichever is higher. The POPIA's two legal penalties extend beyond the organization to individuals: a fine of between R1 million and R10 million ($67,000 to $675,000), or or imprisonment for one-to-ten years. CCPA has the lowest fines - $2,500 for each violation or $7,500, whichever is higher. Of course, all regulations allow for civil suit compensation if damage is suffered. Just as with the regulatory fines, however, civil suit compensations can vary per law.

LGDP, POPIA, and CCPA also differ significantly from GDPR when it comes to data breach notifications. Unlike GDPR, which requires alerting data subjects and authorities of a substantive data breach within 72 hours, the other regulations simply note that the notification must be made as soon as reasonably possible after the discovery of the compromise.

Do the LGDP, POPIA and CCPA have the same scope as GDPR?

Since LGDP and POPIA were inspired by the GDPR, the regulations apply to any organization that meets the data collection and/or processing criteria, without exception. In contrast, the CCPA has stipulations intended to ease the burden on small businesses by establishing a minimum criteria of data collection or processing. Thus, a business is subject to CCPA only if it has:

- $25 million in annual gross revenues
- 50,000 consumers, households or devices applicable to data collection/management/selling per year
- 50% of annual revenue is derived from selling consumer personal information

The CCPA introduced these new levels of requirements since the scope is extended to devices enabled with the Internet of Things (IoT) and any other device which uniquely identifies a particular household (e.g., WiFi-enabled washing machines, dog microchip, etc.).

While all of the regulations - GDPR, LGDP, POPIA and CCPA - are open to interpretation and still need to be tested through court systems, they resonate with an overall market concern. This growing privacy trend has lawyers everywhere writing or updating commercial contracts to comply with existing and coming regulations. Especially for B2B business agreements.

3 - Aligning to Customer Data Protection Realities

- If we aren't compliant already, should we hide, panic, or scramble?
- What should we focus on now?
- Is data collected prior to May 25, 2018 exempt from GDPR? What about LGDP, POPIA and CPPA?
- Who should be in charge of GDPR, LGDP, POPIA and/or CPPA compliance?

If we aren't compliant already, should we hide, panic, or scramble?

If you're not already well on your way to GDPR compliance, you've missed the deadline. However, there's no need to panic. According to industry statistics, you're far from the only one. However, continued noncompliance places your organization at risk and opens you up to civil lawsuits as well as government fines.

It's impossible to know how large-scale noncompliance will be addressed, but it's safe to say that the clock is ticking on the current grace period in which organizations can demonstrate they're making a good-faith effort and get by with a warning and perhaps some guidance on how to accelerate their efforts.

What should we focus on now?

Your best approach is to finalize your plan for compliance and to then start working on the most important parts of that plan so that you can clearly demonstrate your intention to comply with GDPR requirements.

1. Figure out what data you have and where it is

The process of identifying what personal data you have, how it's used, and where it's stored doesn't have to be complex, but it does have to be thorough. If Marketing sends prospect information to Sales via email, for example, those emails must be accounted for. Important details include:

- Which departments/teams collect personal data
- Whether the data is stored onsite or in the cloud
- If data processing is outsourced, the identity of the vendor and the type of system being used
- The sources of the data collection (websites, native mobile applications, other digital touchpoints)
- How different types of data are used and what they're used for
- The identity of any other parties who use or have access to the data
- What type of consent was given when the data was collected and where that documentation is stored

This information (as well as any difficulties you have finding the answers) will give you a good first snapshot of how much work you'll need to do to become GDPR compliant. It's also critical towards your ability to delete or anonymize a consumer's data upon request. This effort ultimately provide

you with the insights required to comply with additional data privacy regulations that are proposed or in effect in the various countries where you operate.

2. Develop or update your privacy policy

Your privacy policy should clearly state your alignment with the "spirit of the law" for protecting data privacy. Don't claim to be compliant if you're not; just state your commitment to protecting consumer data and reassure consumers that you're actively working to meet GDPR requirements.

3. Create an action plan

Identify each GDPR requirement that you've not yet met and assign each one to a "SWAT" team that will be responsible for developing a plan to achieve compliance. Specific items may include:

- Accountability and governance
- Consent and processing
- Children's privacy protection
- Notifications (customers/internal)
- Data rights and procedures
- Records processing
- Privacy by design
- Data breach notification
- Data localization
- Contracting and procurement

4. Understand your prospect and customer data sources

One of the key prerequisites for GDPR compliance is understanding what personal data you collect and where it is stored. That can seem daunting at first, but it becomes manageable when you break it down into key elements:

- Who are the departments or teams that operate systems which collect personal data?
- What types of hardware and software are used to collect the personal data, and are they on the organization's premise or located in the cloud?
- What are the user-facing sources for data collection? (e.g., websites, native mobile applications, other digital touchpoints, etc.)
- How is the data processed and for what reason?
- Where is the data eventually stored and maintained, and if it is sent outside of the organization, to whom and why?
- Has prospect or customer consent been requested and obtained? If so, when? And has proof been logged in the system?

This basic information provides a good initial snapshot into an organization's GDPR readiness. It also provides support for complying with related regulations, such as CCPA, LGDP or POPIA.

Any level of difficulty in answering these questions is a good indicator that the organization will face challenges in complying with a user's request for data pseudonymization or deletion, thereby falling short of customer data privacy compliance.

5. Identify your priorities

Once you have each working group's plan, identify your priorities based on the value to your organization (cost/benefit analysis).

6. Document your accomplishments

Have each working group document their accomplishments as proof of your good-faith intentions to achieve GDPR compliance.

Is data collected prior to May 25, 2018 exempt from GDPR? What about LGDP, POPIA, and CPPA?

No, there is no grandfather clause in the GDPR. Existing data is subject to the same requirements as data collected after May 25, 2018. Some organizations have chosen to address this by asking customers to re-authorize consent based on the new standards. Others have chosen to delete existing data and start over with systems that are GDPR-compliant from the outset.

With regards to the CPPA, as of its effective date (January 1, 2020), it requires organizations to re-examine personal data collected within the prior 12 month period. LGDP (effective August 1, 2020) and POPIA (effective June 1, 2021) will adopt the same approach as GDPR, applying their principles to all consumer data regardless of collection timeframe.

Who should be in charge of GDPR, LGDP, POPIA or CPPA compliance?

There is no one specific title or position that's best suited to be in charge of GDPR compliance. In general, the ideal person is someone authorized and endorsed by the CEO or other executive leadership to spearhead GDPR compliance and to monitor and maintain compliance going forward. While the ability to negotiate and build relationships is important, unequivocal support from the C-suite is an absolute necessity.

4 - Are customer data marketing technologies the enemy of privacy?

The rise of customer data unification …

As companies utilize software and data collection systems more readily through their customer journies, the need for that data to deliver a consistent customer experience becomes more and more mandatory.

A unified and efficient customer experience cannot be achieved without a unified view of your customer, which in turn cannot be achieved without aggregating the relevant data collected from the various systems that interact with your customers.

For the last 5 years, the concept of a "Customer Data Platform" (or CDP) has become more and more widespread among marketers as the tool to unify disparate customer data silos. Further, this unified data allows CDPs to help manage the customer experience across various digital channels, building a 360-degree view of the customer in that process.

The CDP Institute, managed by Raab Associates Inc., defined Customer Data Platforms as a category in 2013. As they state, "Modern marketing requires a unified view of customer data to support coordinated, optimal treatment of each customer and prospect across all channels throughout the customer life cycle. Customer Data Platforms allow marketers to create this unified view."

However, aggregating that much customer data, no matter the touchpoint, is becoming a real challenge. The more companies break data silos, the more they need to be careful with regards to customer data privacy challenges.

… Versus the rise of customer data privacy: Are there any tools or services you can buy to help achieve compliance?

Or, to boil it down even further, is a data privacy adherent, 360-degree view of your customer even possible?

The short answer is yes. How? Because a true customer journey cannot be built at the cost of the customer's data privacy…and especially without his or her consent!

Rather than seeing this as a constraint, enterprises should look at it as an opportunity (using the right tools) to build trust, and with trust, improve their data quality. The end result is a better customer experience that will eventually lead to revenue growth and increased customer satisfaction.

How do you implement a trust-based customer journey?

Following Customer Data Privacy requirements is a good - and mandatory – first step: as previously stated, the core principle of Data Privacy laws is to let customers understand what you are doing with their data and to get consent to gather and control it.

The future ISO standard coming from the PC317 workgroup "Consumer protection: privacy by design for consumer goods and services" (which Jahia is participating in) will help by setting recommendations in regards to the way you should build your product and services given these new regulatory changes.

Implementing tools that put your customers in control of their own data only builds upon that trust. It doesn't mean every customer will delete his or her data and say "no" to everything; Rather, the fact that the client can do it later changes their relationship with the brand. Don't forget – customers like to have brands "know" them. It helps things move quicker when they need support or are looking for advice on how to use or buy something else from the brand.

As for other important and structural software commodities - Because both client data privacy management and customer data collection are such core requirements, related standardization and open source projects have been initiated by two of the most trusted communities in the software industry:

Since 2015, under the umbrella of the OASIS standardization consortium, a specific technical committee was chartered to assist organizations that currently struggle to create and deliver consistent personalized experiences across channels, markets, and systems with data privacy by design. The Customer Data Platform specification (or CXS technical committee) aims to simplify management, integration, and interoperability between solutions providing services like Web Content Management, CRM, Big Data, Machine Learning, Digital Marketing, and Data Management Platforms.

As a mirror of this standardization initiative, the Apache Unomi project provides the first open source customer data platform and acts as the implementation of the OASIS' Customer Data Platform specification initiative - all while promoting ethical web experience management and increased user privacy controls.

At the end of the day, though, there is no single tool that can help you achieve 100% compliance. There are, however, tools that address various aspects — locating and categorizing unstructured personal data hidden in emails, for example. There are also tools developed for other purposes that make compliance easier. Some CRM platforms, for example, have anonymization features, meaning that they irreversibly destroy any way of reconstructing the data and connecting it to a particular individual. Some offer pseudonymization, which cloaks a person's identity so that additional information is needed to reconnect the data to the related individual.

Before purchasing any tool to help with an aspect of customer data privacy compliance, consult with your subject matter experts. Gather input on whether you have the skills you need in-house or whether it would be smarter to purchase a tool — or even outsource a specific aspect of compliance.

Conclusion

May 25, 2018 has come and gone. CCPA has come – LGDPR andPOPIA aren't far behind. Other data privacy regulations throughout the US and other parts of the world are soon to follow. While it appears that many organizations didn't meet the deadline, it's important to make as much progress as you can and continue to demonstrate good-faith efforts to regulatory bodies and users alike. Rather than being a destination, GDPR is becoming a milestone for every organization's data privacy compliance journey.

In the long-term, GDPR will shift the industry and how personal data is managed. It's not something you do once, file away in a drawer, and never think about again. Instead, it introduces a fundamental shift in the way businesses use personal data - one that will forever change common marketing activities.

Many thought leaders are already adapting marketing best practices to meet this new reality. So, in addition to achieving compliance, it's important to figure out how your organization can accomplish its own marketing goals and, most importantly, how you can use these new laws to strengthen your client-centric approach to business.

Resources

Article 29 Working Party position and advice about consent
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

Article 29 Working Party guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679
https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826

Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr

The official source:
https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data- protection/data-protection-eu_en

The official text:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

General Data Protection Regulation – Guide for Processors – September 2017 edition from the CNIL (Commission Nationale de l'Informatique et des Libertés), a french public authority that aims to protect personal data, support innovation, preserve individual liberties -
https://www.cnil.fr/en/general-data-protection-regulation-guide- assist-processors

OASIS' Customer Data Platform specification / Context Server standard (CXS) (p.26):
https://www.oasis-open.org/committees/tc_home. php?wg_abbrev=cxs

Apache Unomi project (p.26):
http://unomi apache.org

CPPA resource:
https://www.caprivacy.org
https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

LGDP resources:

Brazil's New Data Protection Law: An Overview and Four Key Takeaways for U.S. Companies
https://www.natlawreview.com/article/brazil-s-new-data-protection-law-overview-and-four-key-takeaways-us-companies

Official LGDP text
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

POPIA resources:

Official POPIA text
http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

The South African Institute of Chartered Accountants POPIA overview
https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx

About Jahia

At Jahia, we believe great digital experiences don't have to be complex. It only requires strong and continuous integration capabilities along with simple, intuitive interfaces that enable IT & Marketing to work together to build and manage multi-channel initiatives quickly and easily.

Leveraging our headless enabled, cloud-based platform, Jahia helps companies all across the world better utilize their content and customer data to deliver the right experience at the right time for truly personalized customer experiences. With an unparalleled level of flexibility and connectivity, ensuring our solutions can be adapted to suit their needs, Jahia cuts through the noise (and long implementation cycles) to Make Digital Simpler.

Founded in 2002 and headquartered in Switzerland, Jahia Solutions Group has its North American headquarters in Washington, D.C., with additional offices in Boston, Houston, Toronto, and throughout Europe. Jahia's loyal customer community counts hundreds of global brands and organizations, including Ben & Jerry's, Nationwide, NASA, and General Motors.

Contact us

Group HQ
Geneva, Switzerland
+41 22 361 34 24

North American HQ
Washington, D.C.
+1 202 656 7874

France, Paris
+33 1 44 79 33 79

Austria, Klagenfurt
+43 463 287 008

Germany, Freiburg
+49 211 178 377 36

Canada, Toronto
+1 905 257 7471

E: info@jahia.com

W: www.jahia.com