Understanding GDPR and creating a plan for May 25, 2018 and beyond

Because the way you manage your customer data will define you as a company

By Elie Auvray and Kristina Podnar

Elie Auvray

Elie co-founded Jahia Solutions Group SA, led as CEO through 2017 and currently serves as the company's Chief Product Officer and Board Member. Jahia aims to make Digital simpler. Jahia's open source Digital Experience Platform brings together content management, data marketing and great integrations to help its customers deliver the best digital experiences - but not at the cost of customer data privacy.
Being a passionate software entrepreneur with 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 Master of Business & Tax Law from the University of Paris 2 (Panthéon - Assas), holds a Masters Degree in Contract Law, Major in Tech Contract from the University of Paris 5 (René Descartes) and is a graduate from the Business Law Institute (IDA) of the University of Paris 2 (Panthéon – Assas).

e-mail: eauvray@jahia.com

Kristina Podnar

Kristina is a digital governance advisor with nearly 20 years of management consulting experience. She has a history of successfully deploying complex digital transformation projects for global 1000, government, and not-for-profit organizations as well as an aptitude for solving organizational challenges related to IT and digital governance issues.
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).

e-mail: me@kpodnar.com

The way you manage your customer data will define you as a company

When the world opens for business on May 25, 2018, the European Union's General Data Privacy Regulation will be in effect, permanently changing the way businesses around the world collect, process, and store data on EU prospects and customers. Early indications suggest that many organizations don't fully grasp the magnitude of the new legislation or the extent of its requirements:

- When Veritas conducted a survey of organizations from around the globe, 31% indicated that they were already GDPR compliant. However, when questions turned to specific requirements, it became clear that many of them fell short. In fact, 98% of the organizations that initially believed themselves to be in compliant were mistaken.

- In a study conducted by Varonis, 38% of respondents indicated that their organizations don't view becoming compliant by the May 25 deadline as a priority.

- In another survey conducted by TrustArc, 61% of respondents reported that they hadn't begun implementation of their plan for compliance, and 4% of that group hadn't even started the planning process.

- Gartner predicts that, by the end of 2018, more than half of affected organizations will still be non-compliant.

This white paper is intended to address the fundamental reasons for such dismal numbers:

1. Failure by organizations of all sizes to recognize the value of their customers' personal data and the implied social contract of protecting that data,

2. **Failure to understand the law**, whether and how the law affects their organization, and

3. Clear understanding of the law's requirements, which extend **to integrating privacy into core business processes and, eventually, at the core of the business itself**.

Contents

01

Introduction to the GDPR

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

Introduction to the GDPR

What is it?

The GDPR is the **European Union's General Data Protection Regulation**, which goes 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?

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 citizens as well as on non-citizens while they reside in the EU.

- Non-EU companies that employ EU citizens (regardless of location)
- Non-EU companies that collect, process, or store data on EU citizens (even, for example, an IP address for a single individual)

In general, it would be a mistake for organizations to simply assume that they're not affected because they have no physical presence in the EU.

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 citizen or current resident, regardless of whether the related activity takes place within the EU.

Increased penalties

Non-compliant organizations can be fined up to 4% of (global) annual sales or €20 million, (US $24 million), whichever is greater. Fines will be 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 will no longer be able to 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 (downloading a white paper, for example) can't be used for another purpose (such as targeting 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.

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 to then transfer that data to another processor.

Privacy by design

The concept of privacy by design isn't new, but the GDPR is 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 only as much data as is truly necessary rather than collecting as much as is 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.

02

What the GDPR means 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 exceptions?
- 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?

What the GDPR means for your organization

The previous section provides a broad overview, but it takes a deeper understanding to become truly GDPR compliant. This section provides additional information on some of the more important aspects of the GDPR.

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 names, 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 citizens (regardless of where they live) or current EU residents
- Employ EU citizens
- Monitor the behavior of EU citizens or residents
- Collect, process, or hold the personal data of EU citizens or residents

The number of EU citizens or 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 citizens and 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 would 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 deliver products or services to European citizens.

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 roles of both processor and controller.

But keep in mind that, even when organizations do outsource one or both of those roles, that doesn't absolve them of the 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 customer:

- Provide guarantees that the way you process the personal data meets GDPR requirements
- Provide guarantees that the way you 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.

Is user consent always mandatory or is there an exceptions?

As we already mentioned, starting on May 25, companies will be able to collect prospect or customer data:

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

The first two scenarios are quite 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 of the processing is based on a 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.

1. 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 purpose. 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.

2. 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.

3. 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 the 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, what you should better do is simple:

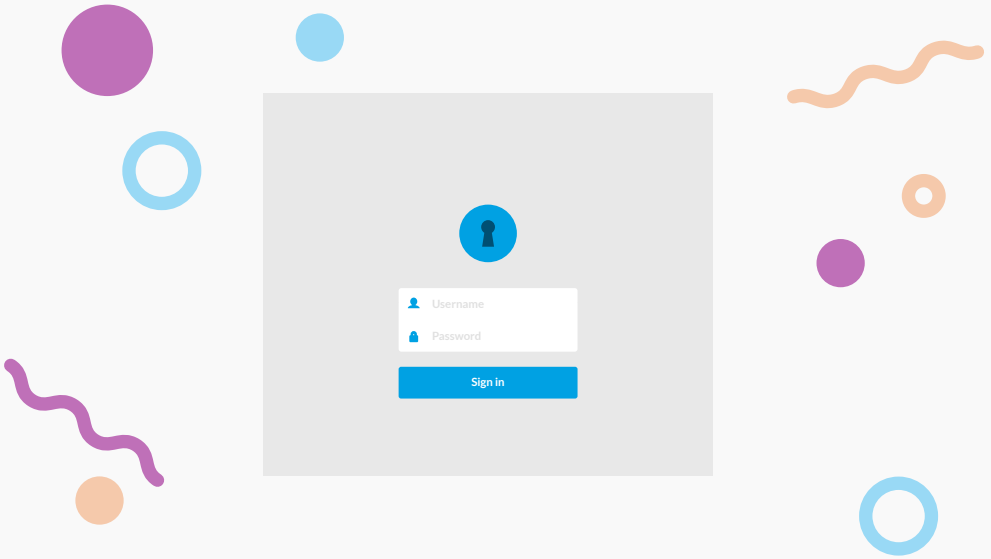
Consider that consent is king.

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 B2C companies to 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 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. You can't extract personal information from mortgage applications and use it to communicate with applicants for unrelated purposes, for example.

03

Aligning to GDPR realities

- Should we hide, panic, or scramble to be compliant by May 25, 2018?
- What should we focus on between now and May 25, 2018?
- Is data collected prior to May 25, 2018 exempt from GDPR?
- Who should be in charge of GDPR compliance?
- Are there any tools or services we can buy to help us achieve compliance?

Should we hide, panic, or scramble to be compliant by May 25, 2018?

If you're not already well on your way to GDPR compliance, it's unlikely that you'll be fully compliant by May 25. But, according to the statistics reported in the introduction to this white paper, you'll be far from the only one.

While it's impossible to know how such wide-scale noncompliance will be addressed, it's likely that there will be a grace period in which organizations that can demonstrate they're making a good-faith effort will get by with a warning and perhaps some guidance on how to accelerate their efforts.

What should we focus on between now and May 25, 2018?

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.

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. In addition, it's critical to your ability to delete or anonymize a consumer's data upon request.

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.

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 for achieving compliance. Specific items may include:

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

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, such as understanding:

- Who are the departments or teams that operate systems which collect personal data?
- What type of hardware and software is used to collect the personal data, and is it on the organization's premise or is it 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 the prospect or customer consent has been requested and obtained? If so, when? And has proof been logged in the system?

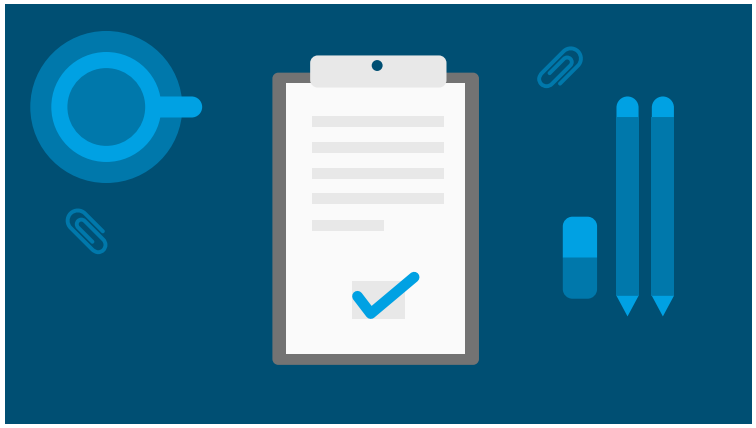
This basic information provides a good initial snapshot into an organization's GDPR readiness. Any level of difficulty in answering these questions is a good indicator that the organization will face challenges in complying with a user's request for data pseudonymization or deletion, thereby falling short of GDPR compliance.

Identify your priorities

Once you have each working group's plan, identify your priorities based on value to your organization (cost/benefit analysis) and your ability to make quantifiable inroads by May 25, 2018.

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?

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

Who should be in charge of GDPR 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.

Are there any tools or services we can buy to help us achieve compliance?

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.

As for other important and structural software commodities, because both client data privacy management and customer data collection are a core and transversal requirement, 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 **Context Server standard** (CXS) 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 CXS standard while promoting ethical web experience management and increased user privacy controls.

Before purchasing any tool to help with an aspect of GDPR 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.

04

Your organization and GDPR after May 25, 2018

- Will there be marketing after GDPR?
- Evolving to privacy by design

Will there be marketing after GDPR?

Yes, there will always be marketing. It is possible to have client privacy coexist with powerful digital marketing systems. But the GDPR will significantly change the way many marketers do business, especially when it comes to using consumer data to deliver marketing content.

Data has transformed the world of marketing, enabling organizations to target their customers with an extraordinary level of of granularity and accuracy. From purchased databases to tracking a particular consumer's website behavior, data has been plentiful and easy to obtain.

The GDPR, however, will significantly restrict marketers' access to the data they've relied on for the last several years. For one thing, marketers will be able to collect only as much data as is necessary and relevant for the activity in question.

They won't be able to request information on household income, for example, from a user who just wants to sign up for a newsletter.

In addition, it's been a common practice among marketers to collect email addresses for purposes like downloading a white paper and to then continue using those addresses to send marketing emails. Under the GDPR, that will no longer be allowed. Any data that's collected can be used for that purpose only unless the consumer gives explicit consent for it to be used for additional purposes.

The end result is that marketers will have to earn the right to communicate with consumers. Marketers are used to having to compete for attention; now they'll have to compete just for the right to have their content show up in a consumer's inbox. In the long run, that should raise the bar for quality content globally.

Evolving to privacy by design

While GDPR is currently on everyone's radar due to the impending deadline, it's really only one component of a larger strategy around customer engagement and client intimacy every company should focus on with the help of digital tools.
It is possible to develop and sustain a customer relationship in alignment with GDPR, as long as your organization adopts a "customer privacy first" mentality.

To that end, being compliant is necessary, but not sufficient, for achieving a more effective business strategy. GDPR compliance is a way to accelerate the transformation a company has to make if they want to be customer-centric organization, which is a mandatory move at a digital age.

That's the opportunity behind the digital transformation and related personalization of the client relationship.

It's not about the feature (eg: a consent manager within your marketing automation software) but about what you can achieve with it: better customer relationships with trust and transparency.

This transparency would lead to increase the quality level of the data you collect from your customers because:

- They will understand why you need it and hopefully see the value
- You're giving them a way to control their data through anonymization, export, or deletion, reassuring them that, at any point in time, they can modify their consent

And a better data quality means better personalization, leading to a better service and/or product offering and, eventually, greater revenue.

Thus, as you see, it's not just about being GDPR compliant.

Within your company, if you push for GDPR compliance without perspective, you will fail because of the lack of alignment through your organization. But if you push a message such as: "*We are about to build a better digital customer relationship by strengthening the trust they have with us thanks to the way we collect data and use it for personalization, thus achieving a better service and eventually increasing our sales*", then it's a different story.

It frames GDPR compliance **as a consequence** but not **as the main goal.**

It's one of the reasons why such a project cannot be solely led by the head of Legal or IT but, as with any other major company transformation, should involve all leadership.

Conclusion

May 25, 2018, is approaching quickly. While it appears that many organizations won't meet the deadline, it's important to make as much progress as you can by that date so that you can demonstrate your good-faith efforts to regulatory bodies.

In the long term, however, the GDPR is much more than a date on the calendar. 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.

It's safe to say that many thought leaders are already busy adapting marketing best practices to this new reality. So, in addition to achieving compliance, it's important to look beyond the deadline and to start figuring out how your organization can accomplish its marketing goals in this new reality and most importantly gets major benefits from it as another way to strengthen a client centric approach of your business.

Resources

- 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
- **Article 29** Working Party position and advice about consent http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239
- **Article 29** Working Party guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963
- 2-3 minute videos on the key aspects of the GDPR in plain language
- UK Information Commissioner's Office (ICO) Getting ready for the GDPR Checklist
- **Survey of organizations from around the globe (p.3):** https://www.helpnetsecurity.com/2017/07/26/gdpr-readiness/
- **Study conducted by Varonis (p.3):** https://betanews.com/2017/12/06/organizations-not-ready-for-gdpr/

- Survey conducted by TrustArc (p.3): https://iapp.org/news/a/survey-61-percent-of-companies-have-not-started-gdpr-implementation/
- Gartner (p.3): https://www.gartner.com/newsroom/id/3701117
- GDPR (p.6): https://www.eugdpr.org/
- Key changes (p.8): https://www.eugdpr.org/key-changes.html
- 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.incubator.apache.org/

Understanding GDPR and creating a plan for May 25, 2018 and beyond

Because the way you manage your customer data will define you as a company