AvePoint

THE OPERATIONAL IMPACT OF THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR) ON IT

Dana Simberkoff
Chief Compliance & Risk Officer, AvePoint

The European Union General Data Protection Regulation (GDPR) has been years in the making. Originally proposed by the European Commission in January 2012, a final version was agreed upon in December 2015 after many discussions, papers, and directives. It now paves the way for a new era in data privacy for the European Union (EU) and global commerce. While organizations will have some time to come into compliance – before May 2018, when the regulation will be in full force – they should begin to rethink their privacy, security, and information governance strategy now.

The GDPR has global reach – it's not just for organizations with a physical presence in the EU. The broad terms of the GDPR mean that any company with a website offering goods or services (including cloud services) to citizens of the EU may be subject to the regulation. This marks a significant change to the previous law, which most courts generally agree only maintains jurisdiction over companies with an established business in a particular state. Moreover, the new law imposes significantly greater financial penalties (fines of up to four percent of annual global revenue for data breaches), and require:

- Privacy Impact Assessments (PIAs)
- Privacy and security "by design"
- Inventories and data mapping of personal information across your business systems
- Mandatory appointments of Data Protection Officers
- Evidence to validate "reasonable efforts" put forth in all of these areas

This is not a small undertaking. For many companies, it will require a major shift in the way their data is managed and maintained – even those that already have a privacy program in place. While new obligations for the CIO, CISO, and the business come into effect in May 2018, waiting until then to make the necessary changes to your privacy practices will be too late.

While there are many new obligations that companies will need to meet under the GDPR, this whitepaper will specifically focus on key operational impacts focused on data lifecycle management.

RISK & DATA LIFECYCLE

The good news about the GDPR is its requirements reflect many of the best practices for well-governed data and data life cycle management. The bad news is that few companies are actually implementing all (if any) of these directives at this time. The easiest way to achieve this will be through the use of automated technologies in combination with policies, education, and measurement to enable organizations to appropriately balance collaboration and transparency with data protection and privacy.

In essence, the obligations under the GDPR will mandate an overarching system across all information gateways that will allow organizations to implement a "risk-based" approach to data protection focusing on potential harm to individuals. It creates many new (and not new) obligations where more connection between the CPO, CISO, IT, and CIO will be needed. The IT obligations in particular will likely impact companies around the world the most because they may require a fundamental shift in operational processes for IT, business process optimization, and program management. Here are a few issues worthy of deeper consideration as they will carry a significant budgetary and operational impact (particularly on your IT department).

UNDERSTANDING THE GDPR

The GDPR defines specific roles in addition to key components of data privacy to more clearly outline responsibilities of organizations both directly to their customers as well as the responsibilities they maintain over any third party vendors or partners that are involved in any data transfers.

Defined Roles within the GDPR

Controller – The GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." The controller, therefore, is the entity that makes decisions about processing activities, regardless of whether it actually carries out any processing operations.

Processor – Under the GDPR, the term "processor" means a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." In other words, while the controller is the entity that makes decisions about processing activities,

the processor is any entity contracted by the controller for carrying out the processing. GDPR expands regulation of and accountability that controllers have for the actions of their data processors.

Key Components to the GDPR

To assist in that effort, several key operational elements are outlined in the GDPR, which we will partially review here under the distinct categories of:

- Consent, Choice, and Purpose Limitation
- Privacy and Security by Design
- Privacy Impact Assessment & Data Protection Impact Assessment
- Risk Based Approach to Data Protection, Data Inventory, and Data Mapping
- Joint Responsibilities of Controllers and Processors, and Demonstrating Accountability

Consent, Choice, and Purpose Limitation

Under the GDPR, companies must provide clear notice to their customers of the purpose for which their data is being collected and consent must be "freely given, specific, informed, and unambiguous." This is an incredibly important requirement for organizations to understand.

First, let's define two concepts "Notice" and "Opt-in". The Definition of a Privacy Notice is, "A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information." [1]

Often, privacy notices are presented as complex, multi-page documents written by attorneys to satisfy corporate legal obligations. These privacy notices are generally unintelligible to most average people – I myself cannot remember the last time I have fully read and understood a privacy policy – yet we click "I Accept" all the time. Privacy policies have, in some ways, made us a nation of liars. However, under the GDPR, these polices must be clear, concise, and understandable. Privacy notices should provide clear and effective communication of complex and important information to people with a basic education. Clear writing and effective presentation not only provides consumers with an understanding of the treatment of their personal information, but will save a company time and money spent on dealing with complaints due to confusion with complex privacy notices.

"Opt-in" is the idea that information-sharing will not occur unless consumers affirmatively allow it or request it. "Opt-out" is when businesses give consumers an opportunity to refuse sharing of information about themselves, after the presumption has already been made that they have

[1] (*Reference(s) in IAPP Certification Textbooks: F16; US16-18, 37; G95-97, 100)*

will choose to share their information. The consumer must "do something" to change that selection. In the "Opt-Out" scenario, the default setting is that you have agreed to share all of your information and must inform the business if you don't want to do so.

This is an incredibly important requirement for participating organizations to understand. It will directly impact companies in terms of how they:

- Collect information
- Record the purpose for which the information was recorded
- Store, use, and share the information

For example, if a company collects customer data to provide technical support, then they must clearly state that this is the reason they are collecting the data, and the data subject must proactively "opt-in" to allow his/her data to be collected for that purpose. Once the company receives that data, they can only use the data for that purpose, unless they have obtained specific and explicit permission from the customer to use it for other purposes. This means that as the organization stores the data in its systems, it will need to be clearly marked (for example with a metatag) so that it is not inadvertently combined with other data where it might be used for a different purpose.

This will also impact organizations that regularly share customer data with external parties, particularly if the sharing of information is not related to the original data collection purpose. It may also have implications for companies that hold data that they collect over a period of time and are later subject to a merger or acquisition. Also, the "opt-in" requirement (requiring explicit affirmative consent) will mean that many organizations will need to create layered consent mechanisms. They must allow the organizations to specifically demonstrate that an individual has chosen to have this type of data shared with third parties or to use the data for a separate purpose. As many organizations collect data (and obtain consent) through their websites or through an internet portal, this will require a major revamping of current consent mechanisms and opt-in/opt-out practices. This will of course be true for in person or non-web based consent forms.

Privacy and Security by Design (And by Default)

Anyone who has been a part of designing a home or building anything understands that it is always better to get your plans right in the beginning, as change is generally time-consuming and expensive. When it comes to privacy and security, implementing a standardized and repeatable process for both IT and the business from the very beginning of a project is ideal. Data Protection and Privacy Officers as well as their security and risk counterparts will be able to help provide advice, guidance, and review the project at every step of the process. Consider

using automation to allow your colleagues to request a PIA of the systems they are planning to build and deploy so that you can provide them with a reasonable estimate and timeline. Your involvement early on will save them from having to make last minute design changes or decisions with the clock to launch ticking. The GDPR requires not only privacy and security by design but also by default. This means that what was formerly considered to be a best practice will now be a mandate that is operationally demonstrable.

Privacy Impact Assessment (PIA) & Data Protection Impact Assessment (DPIA)

PIAs and DPIAs are a systematic process to "**assess privacy** risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify **privacy** risks, foresee problems and bring forward solutions." (www.iapp.org). Many organizations already conduct PIAs as part of a statutory or regulatory obligation, and the GDPR will also mandate PIAs for all high-risk data processing activities. Impact assessments, like security assessments, provide a good foundation to assess the potential and ongoing risk of systems and data flows within them so that privacy and data security teams can recommend and monitor appropriate controls. The International Association of Privacy Professionals (IAPP) exclusively distributes a free tool – the AvePoint Privacy Impact Assessment system – to help automate the process of conducting PIAs.

Risk-Based Approach to Data Protection, Data Inventory, and Data Mapping

The GDPR requires that companies utilize a "risk based approach" to manage their privacy and data protection programs. Throughout the GDPR, organizations that control the processing of personal data are encouraged to implement protective measures corresponding to the level of risk of their data processing activities. Although the GDPR does not say how organizations should assess and quantify risk, certain trends emerge from the sections where risk does appear that will guide organizations in implementing a risk-based approach.

The GDPR divides areas into High-Risk, Risk, and Low-Risk processing – with different requirements and obligations associated with each level. Risk analysis is contextual. Where the concept of risk appears in the GDPR, it is defined by reference to the "likelihood and severity" of a negative impact on data subject rights. Data controllers should account for "the nature, scope, context and purposes of the processing." At the most fundamental level, with regards to data security, controllers must implement (and choose processors that implement) "technical and organizational measures" appropriate to the risk of a data breach. Further, a new obligation is introduced in the GDPR that requires organizations that experience a breach to notify both the Data Protection Agencies (DPAs) and the individuals affected by the breach where individuals' are at high risk (discrimination, fraud, theft, financial loss, loss of reputation, etc.) While there are steps that can be taken to mitigate these notice requirements, it nonetheless means

organizations will have a new level of transparency to the public, DPAs, and customers when it comes to security controls or lack thereof.

As organizations think about the steps to operationalize their obligation to take a risk-based approach to data protection, they must fundamentally understand the nature of the data their company holds. This includes a complete understanding of how this data is collected or created, used, maintained, shared, and ultimately disposed. The data, combined with the context of the data (or intended use/activity with the data), along with the potential "harm" to the individual subject to that activity, is fundamentally what determines risk and drives appropriate data protection measures.

In this way, organizations can adopt a risk-based approach to compliance, understand the true value of the data they hold today, and appropriately mark it so that controls and safeguards can be applied to control where the data resides and who can access it.

So how do we define and think about risk within the context of GDPR? While this sounds like a bit of legalese, and may make IT professionals squirm at the idea of lawyers measuring shades of gray, it's relatively simple to find meaningful ways to operationalize this requirement. Start by taking the time to understand what kinds of data your business handles and uses as well as how your coworkers are using your internal systems in their day-to-day jobs. Understanding a "day in the life" of your colleagues will help you understand why and how they need to handle this protected data in the course of their daily work. The time you invest in understanding their requirements will pay off in spades as you will be able to craft solutions that meet their needs and your obligations.

Data Inventory & Data Mapping – The GDPR requires that you understand and maintain an up-to-date inventory of personally identifiable information (PII) as it flows through your systems and throughout your company along with contextual information about that data. What kinds of data are you trying to protect? Or, as I like to say, what are your "crown jewels"? Many companies worry about "dark data" that is not properly understood or data that exists across their enterprise systems (file shares, SharePoint, social systems, and other enterprise collaboration systems and networks). Understanding what and where this data is and properly classifying it will allow you to put the appropriate levels of protection in place. For example, many companies apply their security protocols in broad terms, using the same security procedures for everything. But, logically, do you need to put the same security protocols around protecting pictures from your company picnic as you do towards protecting your customers' credit card information?

Joint Responsibilities of Controllers and Processors

Under the GDPR, not only are companies responsible for ensuring that they are complying with their own stated privacy and data protection policies, but they also must ensure that the third parties with whom they share data they collect have comparable policies and operational procedures to their own.

Controllers are liable for the actions of the processors they select and responsible for compliance with the GDPR's personal data processing principles. When selecting a processor, controllers must only use processors that provide sufficient guarantees of their ability to implement the technical and organizational measures necessary to meet the requirements of the GDPR. Because companies will have ongoing responsibility (and liability) for downstream data processors, they will need to greatly increase their scrutiny around vendor selection and monitoring practices. Implementing a process for both vendor selection and ongoing vendor monitoring will be critically important.

Demonstrate Accountability by Setting Enforceable Policies

The GDPR requires that you not only create policies that meet its mandate, but that you operationalize those policies and be able to prove that you've done so. Your General Counsel's office and compliance team are tasked with understanding your statutory and regulatory obligations and helping your business to comply with these requirements. However, be sure that any policies you set internally can be measured, monitored, and enforced. Broad statements such as "we do not allow PII data in SharePoint", without the ability to enforce this policy or measure its effectiveness is not a sound data protection strategy. Don't leave your policies to chance or luck, and don't have a policy that sits on a shelf. Policies should be living breathing documents that reflect and direct the flow of your business. The new obligations will mandate an overarching system across all information gateways that will allow organizations to say what they are going to do (to achieve compliance), do it, and prove it – internally, for your auditors, regulators, or as part of your data protection best practices.

OPERATIONALIZING YOUR DATA LIFE CYCLE MANAGEMENT PRACTICES TO PREPARE FOR THE GDPR

At the center of all of the GDPR Obligations Principles is a core requirement for organizations to create a risk-based approach to data privacy and protection which is based on the concepts of transparency and accountability. As organizations think about the steps to operationalize their obligations they must understand that much of their data may be lost in data silos, file shares, or instant messages as well as inappropriately shared through social technologies, undiscoverable, and unprotected. So what can be seen as a "risk" may also be viewed as an "asset" when accessed and protected appropriately. Data tagging and classification allows an organization to gain better insight and control into the data that they hold and share. Metatags allow organization to optimize their e-discovery and record retention programs and at the same time protect and control the flow of information.

The remaining challenge is that many organizations have data classification policies that are theoretical rather than operational. In other words, there is a corporate policy that is unenforced, or left to the business users or data owners to implement. The challenge presented by a business user driven "trust" system is that it is difficult to predict the appropriateness and level of data being properly tagged. Are inappropriate discussions happening? Is sensitive or confidential information being shared? Are privacy and compliance policies being circumvented, either deliberately or inadvertently? Who do you trust: user or machine?

An effective data classification and data protection program will begin with governance and compliance policies; operationalize an automated approach to data discovery, tagging, and classification; and complete the circle with comprehensive controls that include data loss prevention, monitoring, and reporting. So what does this look like in practice?

1. First, contemplate how data is created or collected by your company. You should think about excessive collection, how you will provide notice (to individuals) about that collection, provide appropriate levels of choice, and keep appropriate records of that collection and creation.
2. Second, think about how you are going to use and maintain this data. Here you should consider inappropriate access, ensure that the data subjects' choices are being properly honored, address concerns around a potential new use or even misuse, consider how to address concerns around a breach, and also ensure that you are properly retaining the data for records management purposes.
3. Third, consider who (and with whom) this data is going to be shared. You should consider data sovereignty requirements and cross-border restrictions along with inappropriate, unauthorized, or excessive sharing.

4. Fourth, all data has an appropriate disposition period. You should keep data for as long as you are required to do so for records management, statutory, regulatory, or compliance requirements, and ensure you are not inadvertently disposing of it, but at the same time, as long as you have sensitive data you run the risk of breach.
5. Finally, understanding the difference between what can be shared and what should be shared is always the key. A good program must continually assess and review who needs access to what types of information. Privacy and security pros should work with their IT counterparts to automate controls around their enterprise systems to make it easier for employees to do the right thing than it is to do the wrong thing or to simply neglect the consequences of their actions. Once you've implemented your plan, be sure that you maintain regular and ongoing assessments.

This approach, combined with an automation layer, will assist you in achieving and maintain compliance. As you implement your program, understand that it will require an ongoing and iterative process of review to implement privacy and data protection by design and by default, and to implement technical controls and oversight through each stage of the development lifecycle. Your data inventory and PIA reports will also give you oversight into data as it flows through your business.

Operational Implementation-Privacy by Design

Through a programmatic approach and privacy design automation, privacy program managers and data protection officers can then develop a Service Level Agreement (SLA) with their colleagues in IT and the business. What would this look like in practice? Consider the following "high level" approach.

The business creates a new mandatory procedure that requires that all new IT systems, programs, campaigns or processes must go through a quick and automated approval process before moving forward. This would be required for all departments, so whether a program/concept or idea was born in central IT, marketing, or at the business unit level, this process would be applicable. Using a tool like APIA (or any other registration system), the sponsor of the new system would register the idea and be prompted to go through a brief series of questions about the system. The questions might be about the goal of the project, life cycle of the project, cost, branding, etc. For our purposes, the key questions would be centered around whether or not this initiative would include PII or sensitive PII of any kind. Based on the answer – "yes" or "no" – the next steps would apply as follows.

If the answer is "no" then for our purposes, no further action would be required other than perhaps to validate (again through automation) that no PII was in fact being used through the system. This is fairly simple to do through automated scanning, and could even be done

through regular reviews and audits. If the answer was "yes" then next steps would simply flow from there. At this point the privacy, data protection, and security teams could have a built in iterative review process and feedback loop – recommending appropriate procedures and technical controls to ensure that the sensitive data was made available to people that should have it and protected from those who should not. Additionally, by having this information at the beginning of a project, rather than after it is already designed and "fully baked", important data lifecycle management provisions can also be built in to ensure that data is retained for only as long as necessary and it is appropriately archived or destroyed (where appropriate) at the end of a program-to minimize exposure and risk to the business.

In this model, privacy, data protection and security check points can be built into the regular rhythm of this entire process from "concept stage, through development, testing, go-live, production and end of life." As a mandatory element of any new program (or review of an existing one), privacy by design and by default now becomes the "standard way" of doing business, and not an additional burden.

This standardized and repeatable process ensures that IT and the business understand and "bake in" the appropriate privacy and data protection controls as a project begins rather than only considering privacy as a check box exercise – often an add-on that is considered at the end of a project when it is about to go live. This enables not only privacy and data protection teams, but also security teams to help provide advice, guidance, and review at every step of the process. Further, teams should consider using automation to allow your colleagues to request a PIA of the systems they are planning to build and deploy so that the privacy team can provide them with a reasonable estimate and timeline. Your involvement early on will save them from having to make last minute design changes or decisions with the clock to launch ticking.

Making it easier for your employees to do their job successfully while creating an ever present culture of compliance will require you to adopt a risk-based approach to implementing your data protection program. While that often starts with the legal and compliance team and ends with the CISO, in fact it needs to focus also on a day in the life of your everyday business user. People often think of "brakes on cars" as being designed to stop cars-or slow them down. But in fact brakes allow you to drive your car really fast. Work very hard for your IT colleagues and business users to think of privacy and security controls in the same way. Rather than "stopping" the business from doing its job, instead the proper controls will allow you to realize the full potential of the data you do have-so that you can achieve all of the business objectives you've set out. Privacy by design builds those brakes into the system as part of the initial specification so that when you are ready to roll a program off the assembly line and out onto the road, you can drive away with full confidence in the data protection elements you've built in. APIA can be used to facilitate this process.

Data Life-Cycle Management

Understanding what and where dark data – or information that is stored and not understood – lives and properly classifying it will allow organizations to set the appropriate levels of protection in place. AvePoint has developed a best practice approach that allows organizations to mitigate the risk inherent with manual informal data governance, helping them understand and automate the process of evaluating, assessing, and reporting on the privacy implications of their enterprise IT systems.

Assessment	Validation	Control	Report
Understand existing policies and regulations Assess how users think they are managing information	Analyze current environment Identify gaps between expected and reality (exposure and risk)	Develop information classification taxonomy Define policies and processes to support the taxonomy	Recommend a roadmap to implement the policies and processes Develop high level change management strategy

There are four "operational" steps to practically implement this risk management strategy that will allow the organization to have policies and controls that reflect real life data protection and risk management within your organization.

1. **Assess:** Based upon the organization's policies and plans, understand what kind of sensitive data the company holds and how the systems it uses will collect and protect that data.
2. **Validate:** Prove that the data that may put the organization "at risk" is in the proper (appropriately identified and authorized) systems
3. **Control:** Protect sensitive information with appropriate controls for security and compliance, including geography (due to data sovereignty or geo-location restrictions), retention, and classification – reducing risk across the enterprise.
4. **Report:** Provide executive reports on Key Performance Indicators (KPIs), Key Control Indicators (KCIs), or Key Risk Indicators (KRIs) to highlight areas in the organization that need to be addressed to reduce risk, or report on progress made throughout the system, data, individual, and contractual lifecycle.

This robust and holistic approach brings power and simplicity to the world of data protection and classification, with user-assisted tagging and automated classification. In this way, organizations can adopt a risk-based approach to compliance, understand the true value of the data they hold today, and appropriately mark is so that controls and safeguards can be applied to control where it resides and who can access it. Thus, content is married with context, and metadata can help organizations truly certify with confidence that they are ready to comply with the GDPR.

For those of you that read the first few sentences of this whitepaper, stopped at the line "you will have two years to fully comply," and thought to yourselves that you will work on this sometime in 2017: Keep in mind that the obligations under this law may take months if not years for most companies to implement. Don't wait for a breach to happen to you – the fines under this law could be company-ending for some businesses. Don't allow your company to serve as an example to others of what not to do, but rather seize this opportunity to work proactively and swiftly to do what you need to get done.

The reality of the new GDPR is that it truly necessitates the glaring need for privacy professionals to learn to speak the language of IT, and for IT and Security professionals to work hard to find a common vocabulary with their privacy and legal counterparts. The easiest way to achieve this will be through the use of automated technologies in combination with policies, education, and measurement to enable organizations to appropriately balance collaboration and transparency with data protection and privacy.

ABOUT AVEPOINT

AvePoint is the Microsoft Cloud expert. Over 15,000 companies and 3 million cloud users worldwide trust AvePoint to migrate, manage, and protect their Office 365 and SharePoint data. AvePoint's integrated cloud, hybrid, and on-premises software solutions are enhanced by 24/7 support and award-winning services. Organizations across six continents and all industries rely on AvePoint to ease transition to the Microsoft Cloud, increase IT administrator productivity, and satisfy governance and compliance objectives.

A two-time Microsoft Partner of the Year Award winner, AvePoint has been named to the Inc. 500|5000 six times and the Deloitte Technology Fast 500™ five times. AvePoint is a Microsoft Global ISV Partner, Gold Application Development Partner, Gold Cloud Platform Partner, Gold Collaboration and Content Partner, and US Government GSA provider via strategic partnerships. Founded in 2001 and headquartered in Jersey City, NJ, AvePoint is privately held and backed by Goldman Sachs.