SeeUnity™

The main differences between the DPD and the GDPR and how to address those moving forward

Plus, free checklist to make sure you are in compliance with the GDPR!

Introduction

In December of 2015, the European Union (EU) voted to implement the General Data Protection Regulation (GDPR) in place of the outdated Data Protection Directive (DPD.) The DPD was established in 1995 and was aimed to protect the personal data of EU citizens from misuse. While the DPD had good intentions and worked well for the time it was originally established, a lot has changed in the world of information. Due to this, the EU thought it necessary for the law to change too. The GDPR is meant to replace the DPD, and, as a regulation, it will span across the EU as uniform law, and be the first of its kind to try to implement a global initiative.

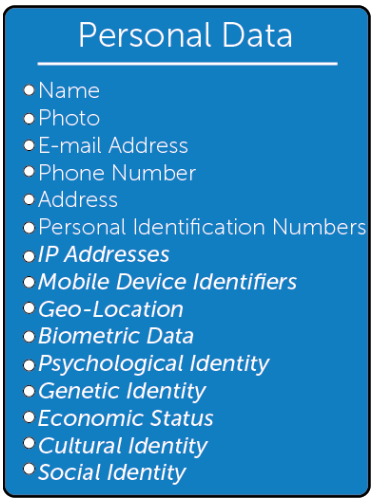
The aim of the GDPR is to enable the people of the EU to better control their personal data. We will talk about specific ways the GDPR will do that in this whitepaper. The change came as 67% of Europeans expressed that they were concerned about not having control over their personal data and information they provide online, according to a recent Eurobarometer survey.

In this whitepaper we will address six of the important changes to come under the GDPR. We will also help guide you with next steps as you prepare for the regulation to take effect in May of 2018. These six changes are:

1. Personal Data Redefined
2. Individual Rights
3. Data Controllers vs. Data Processors
4. Information Governance and Security
5. Data Breach Notification and Penalties
6. Global Impact

Personal Data Redefined

The most important change from the GDPR is the definition of personal data. Where personal data was previously defined in the DPD as a person's name, photo, email address, phone number, address, or any personal identification number (social security, bank account, etc.), it



will have a much broader definition under the GDPR. Under the GDPR things like IP addresses, mobile device identifiers, geo-location, and biometric data (finger prints, retina scans, etc.) will constitute personal data. In addition, things like an individual's physical, psychological, genetic, mental, economic, cultural, or social identity are also covered by the GDPR.

The change in the definition of personal data is important because it reflects the changes in technology and the way that organizations collect data about people. Though this change is positive for the people of the EU who want their data to be protected, it complicates marketing and sales efforts. Specifically, "profiling", the practice of developing a snapshot of an individual's preferences through the use of browser history, purchase history, etc. would no longer be acceptable under the GDPR unless it has been explicitly consented to by the individual.

Individual Rights

The purpose of the GDPR is to give the people of the EU better control over how their data is used, if at all. One of the hot topics of this is consent. An explicit opt-in will be required for the processing of any personal data. Consent for the use of personal data needs to be informed, specific, and unambiguous. This could very well put an end to the long drawn out user agreements that hardly anyone reads these days. Descriptions for use will be short and straight to the point. Consumers cannot be asked to agree to contract terms in exchange for their consent either. This means many companies will have to review their terms of use agreements. In addition to that, different types of data will require separate consent to avoid the idea of an "all or nothing" choice to individuals. Silence or inactivity also does not constitute consent.

Another right that the people of the EU will be able to flex is the right of access to their data. Under the GDPR, data subjects have the right to obtain from the data controller information on how their data is being used (where and for what purpose.) The controller must provide this information along with a copy of their personal data, free of charge, in an electronic format. This is meant to make the use of personal data more transparent and empower the individuals of the EU.

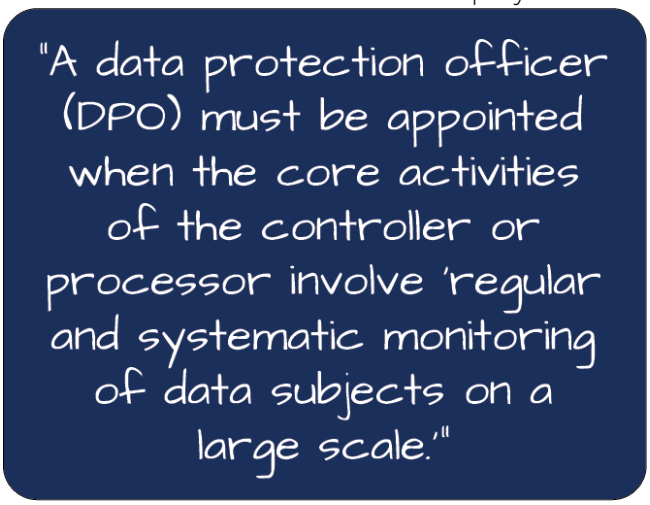
Just as an individual will have the right to access their personal data under the GDPR, they will also be able to ask that they "be forgotten" and the controllers must erase all of their personal data, cease further use of that data, and, if applicable, halt any third party use of that data. For example, an individual may ask to be forgotten when the personal data is no longer relevant to the original purposes for procession, or if the data subject is withdrawing their consent. Individuals will also have the right to have their data transferred from one good or service provider to another.

Data Controller vs. Data Processor

Data controllers are defined as "the natural legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data." A big difference

between the DPD and the GDPR is the addition of regulation of data processors. Data processors are defined as "the natural legal person, public authority, agency or other body, which processes data on behalf of the controller." Previously, under the DPD, only data controllers were held accountable for anything that went wrong. Under the GDPR data processors will be required to have a contract with the data controller to process personal data. Processors will also be liable for the security of personal data.

To emphasize the accountability of both data processors and data controllers, a data protection officer will need to be designated under the GDPR. A data protection officer must be appointed when the core activities of the controller or processor involve "regular and systematic monitoring of data subjects on a large scale." This officer can be an established employee within your company. They just need to be knowledgeable about how the company is collecting or processing personal data. Both controllers and processors will be required to maintain documentation describing their data protection policies and keep record of their data processing activities. (Organizations with fewer than 250 employees do not have to maintain records of processing, whether they are a controller or a processor). They will also be required to conduct impact assessments where there is high risk of data breach.



Information Governance and Security

The GDPR requires that systems and processes consider compliance with the regulation at the inception of their business concept. This is what they call "privacy by design." The privacy of the data collected is taken into account at all steps of the business processes and most importantly at the inception of the product or service concept. Privacy by design also requires that controllers discard personal data when it is no longer required.

Earlier we mentioned the idea of impact assessments. For the security of the personal data collected and processed by controllers and processors, impact assessments should be done. These impact assessments are required for automated data processing activities, large scale processing of certain kinds of data, and systematic monitoring of a publicly accessible area on a large scale.

Data Breach Notification and Penalties

Under the DPD, EU member states were free to adopt different data breach notification laws. This meant that when companies suffered data breaches in the EU, they had to research and ensure compliance with each member state. With the adoption of the GDPR, there will be a single requirement to follow. That rule requires that data controllers notify the supervisory authority of a personal data breach within 72 hours of learning about the breach. This notification should lay out the nature of the breach, the categories and approximate number of

individuals impacted, and the contact information of the organization's data protection officer. Included should be the likely consequences of the breach, and what the controller has done to address and mitigate the breach. A data processor is required to notify a controller of the data breach "without undue delay."

As mentioned above, the GDPR extends the rights of individuals with regard to their personal data. When a data breach occurs, controllers must notify individuals "when the personal data breach is likely to result in a high risk to the rights and freedoms of individuals" and they must do so "without undue delay." This notification should also include the contact information of the organization's data protection officer, the likely outcomes of the breach, and how the company plans on rectifying the situation. There is some gray area in this part of the regulation. The controller does not have to provide notice if the controller had implemented appropriate protection measures and applied those measures to the affected data, took subsequent measures to ensure that the risks to data subjects' rights would be unlikely to materialize, or notification would require "disproportionate effort."

While everyone might be taking steps in the right direction, some may not be doing everything they can to protect personal data. For those controllers or processors, there are some hefty fines to be paid. Under the Directive, the amount of administrative penalties was left up to the member states. Usually, those fines would be small and were very rarely applied. Under the GDPR, penalties will be mandatory and uniform over all the EU states. These penalties could be imposed for any negligent or intentional violation of the GDPR. Depending on the violation, companies could pay up to 20 Million Euros or 4% of their global turnover (whichever is greater.) This would be for violations such as: lacking consent to process data or violating privacy by design. For lesser violations like records not in order, or not notifying the supervisory authority or data subject about a breach could result in a fine of 2% of global turnover.

Global Impact

How the GDPR is written plays a huge role in whom exactly will be affected once the regulation goes into effect in May of 2018. The GDPR states that the regulation applies to the processing of personal data of subjects located in the EU, even if the controller or processor is not established in the EU. In general, any company that markets goods or services to EU residents can be subject to the GDPR. This is regardless of the physical location of the business itself. This provision in the GDPR essentially makes it a worldwide law. The DPD was not nearly as expansive in its geographical reach, and that is partially because it did not plan for the use of digital personal data like IP addresses.

If you are in the U.S. you are probably thinking, "what does this mean for my company?" Even though your business is not in the EU, you must still be in compliance with the regulation if you market your goods or services in any of the EU member states. The GDPR will require that both controllers and processors that regularly collect or process personal data from EU citizens on a large scale to appoint a local representative in the EU states where they do their business. This is more likely to apply to any U.S. based SaaS providers whose clients and customers include companies with large numbers of EU end users or employees.

Another impact to the U.S. based companies is the data breach response plans. Above we noted that under the GDPR, organizations have 72 hours to notify supervisory authorities. This time period is significantly shorter than any U.S. statute. In most cases, 72 hours after a breach people are still scrambling to figure out exactly what happened and what the impact will be. They will need to be careful to not overstate or understate the impacts of the breach. The GDPR also has a much broader and vaguer definition of a trigger for a data breach than most of the U.S. state statutes. In the U.S., obligation to notify typically includes data that was compromised with the combination of first name or initial and last name, with some other unique identifier such as a social security number, driver's license number, financial account and passcode, unique biometric identifiers, or medical information. The GDPR is much vaguer, requiring that notification be given when the breach can lead to identity theft, discrimination, or loss of confidentiality of information. The result of all this could be an increase in global notifications of data breach.

How to Address These Moving Forward

It is undeniable that the GDPR is going to affect all of us in some way, shape, or form. What we need to do is start taking action toward compliance with the GDPR. As a general rule, if personal data was protected under the DPD, it will be protected under the GDPR. What you must consider is all of the additional data that will now fall under the definition of personal data. Start by assessing how much of that data your organization collects or processes, and begin implementing measures to keep that data locked down. When it comes to data breaches, it might be appropriate to start conducting those impact assessments to see how likely a breach is or how much risk is involved in controlling and processing personal data. For organizations who are just getting started, it would be wise to start off with the privacy by design concept and go from there. If you are an organization that does a lot of marketing and promoting of goods or services in the EU, you are definitely going to have to comply with the GDPR. So from now until May of 2018, your priority should be doing what you can to be in compliance with the GDPR.

Preparing for the GDPR Checklist

- ❑ **Broaden your definition of personal information** to include new forms of protected personal data like IP addresses, mobile device identifiers, geo-location, biometric data. In addition to those, psychological identity, genetic identity, economic status, cultural identity, and social identity are also protected by the GDPR.
- ❑ **Determine how you will handle collecting consent** of individuals to collect their personal information. Be sure to define very clearly how you will use personal data as to keep trust.
- ❑ **Update and simplify your user agreements.** Make sure they are readable and easily understandable by the individual you want to collect data from. This will most likely do away with the long, drawn out agreements that we are all guilty of not reading.
- ❑ **Determine how you will handle requests** for how personal information is being handled. The GDPR requires that the information be given to an asking individual in an electronic format in a timely manner.
- ❑ **Ensure that you have the proper protocols** set up to delete individuals' information upon request. The individuals have the right to be forgotten, so make sure you can fulfill that right with ease in that situation.
- ❑ **Determine whether you are a Data Processor or Data Controller**. Do you simply collect the data, and/or are you a third party that processes the data? Either way, you have to be compliant with the GDPR and are equally responsible for any breach in security.
- ❑ **Determine if you need to appoint a Data Protection Officer**. The answer to this for any company collecting or processing data of individuals in the EU is going to be "yes." A DPO may be an already established employee.
- ❑ **Determine how you will design your privacy protocols**. Privacy by design is a key element built into the GDPR. Figure out how you are going to get the privacy standards built into your business.
- ❑ **Discard personal data that is no longer being used**. If you're not using the personal data, there is no reason to risk a potential penalty or fine for the continuation of holding it. Stay on the safe side and discard the data if there is no longer a use for it.
- ❑ **Conduct an impact assessment**. This will help define what the risks of a data breach are, and help address any holes that are found in governance initiatives.
- ❑ **Ensure you have a plan in place** that complies with data breach notification laws. Similar to the point above, make sure you know whom and how to notify if something does happen.
- ❑ **If you're a business not located in the EU,** determine if you're liable for the GDPR. While many non-EU businesses will be affected by this, there is an exception with regard to maintaining records of processing. Educate yourself and your staff to be certain if this regulation applies to you.