GDPR WITHOUT THE HYPE

A No-Nonsense Guide for IT Security

Based on an RSA®C Virtual Session with John Elliott, RSA Conference Contributor

The General Data Protection Regulation (GDPR) is something you probably can't fail to notice if you look at LinkedIn, Twitter or the internet in general. We're going to cut through the hype and cover the essentials that you need to know.

This primer is going to try to remove any fear, uncertainty and doubt that you may have about the GDPR. And hopefully the fear will be replaced with relief when you realize it's not as scary or as complicated as it's made out to be. However, there will still be a degree of uncertainty. This is because, until the regulation becomes applicable and we see how regulators enforce it, we don't know how big a stick they're going to use or whether they're going to have some really exciting carrots for us.

RSA®Conference | Where the world talks security

GDPR: the what, when, why, who and how

After covering the big picture, we'll then take a look at the important parts of the regulation and summarize it to help you answer the questions: What should you do now? What should you do tomorrow? What should you do over the next few months?

What: GDPR is a European Union (EU) regulation, officially called the General Data Protection Regulation or 2016/679/EU, and is directly applicable as law in all 28 EU countries. The regulation was published in April 2016. It concerns the protection of personal data, which means any information relating to an identified or identifiable natural person or what it calls a "data subject."

A "natural person" is what the regulation calls a living human being. If you read the regulation, and it says "natural person," it means a human being, and when it talks about "data subjects," that means human beings whose data you have.

When: GDPR is applicable from the 25th of May, 2018.

Why: The last EU data protection law came out in 1995. Back then, the typical person didn't own a mobile phone or even have access to the internet. The world has changed massively. The regulation as it's published applies equally in all EU countries, supporting a single EU digital market in goods and services. The EU wants to strengthen the rights of individuals over data about them (the definition of privacy) and to embed more accountability into GDPR than was included in the 1995 Data Protection Directive. It also wants to update data protection rules to be more in line with how the world operates today.

Who it applies to: There are two key definitions of who it applies to. The first are data controllers—all organizations that have relationships with data subjects. Second are data processors, which are organizations that work for data controllers and process personal data on the controllers' behalf.

The second concern is geographic. If you're a data controller or a processor established in the EU, then GDPR applies to you. It also applies to any organization processing the personal data of people in the EU—even if the organization itself is based outside of the EU.

How: GDPR consists of two sections. The first section is called "Recitals." It describes how the regulation should work and what it is aiming to achieve. As IT people, look at these as the business requirements.

The second section contains the 99 articles which are the actual regulations that organizations have to comply with. From the IT perspective, these are like code.

We are going to dig into the three major sections of GDPR: The general principles, the data subject's rights, and the responsibility of the controllers.

1. General Principles

- Whenever you process people's data, that activity needs to be lawful, fair and transparent.
- What you do with the data should be expected by the person whose data it is.
- You should only ever have enough data to do what your business or organization needs to do (data minimization).
- The data you keep must be accurate, and you only keep it for as long as you need it.
- Once you don't need somebody's data, you should delete it, and you should protect data with appropriate security.

In essence, have minimal data, secure it, make sure it's accurate, and keep it for just as long as you need it.

2. Data Subjects' Rights

Data subjects have specific rights over data about them:

- Data subjects have the right to know what you're going to do with their data.
- They can ask, at any time, for copies of all the data that you have about them, which you need to provide.
- They need to know your justification for why you have that data, and how long you're keeping it.
- If any of their data is incorrect, they've got the right to ask you to correct it, and you have the obligation to correct it as soon as is feasibly possible.
- A data subject can request that you erase their data. This is the so-called right to be forgotten. However, this is not an absolute right. For example, a customer with a loan can't ask the bank that's lending them the money to delete all their data. But if you don't have a justification for processing the data, if it is not part of a statutory obligation or fulfilling a contract, then the user can ask you to delete their data.
- They have the right to data portability. In other words, you need to give them their data in a machine-readable format. A good example of this is an online supermarket. You want to try a different supermarket, but it's a real pain to re-create your basket and all your favorites. The right to data portability says that you can go to the first supermarket and say, "Give me all my shopping data for the past two years because I want to send it to a different supermarket."
- Data subjects have the right to object to their data being processed in certain ways, such as profiling and direct marketing.
- They have the right not to be subjected to decision making that has a material effect on them as a result of automated processing. If a computer makes a decision that creates a material, legal effect on someone (such as denying credit, turning down a loan application etc.), they generally have the right to say, "Actually, I'd like a human to look at that, as well."
- You cannot charge a fee to a data subject who is exercising these rights, and you have to respond to them within a month.

3. Responsibility of the Controllers

There are 20 articles that cover what data controllers and data processors must do, and despite the hype, only three of them are about security. Some of the important responsibilities are:

- You must be accountable and be able to demonstrate compliance. That means having appropriate governance structures and polices, and sticking to them.
- You have to adopt data protection/ privacy by design. So when you're building systems, you have to integrate privacy into the design of those systems.
- If you are a certain type or size of company not established in the EU, you may need to appoint an EU representative.
- When using third-party processors, ensure that you do due diligence and that you have the right types of contracts.
- If you have over 250 employees or have certain types of data, you must keep records of processing, which can be accessible to the regulator at any time.
- If you have a breach, you need to tell your local regulator. Every European country has a data protection regulator. For example, that's the Information Commissioner in the UK; in France, it's the CNIL.
- If you have a breach, you have to inform the regulator within 72 hours, and if the risk is high, you also need to tell data subjects.
- Finally, some data controllers, depending on the size and the type of data they're dealing with, will have to appoint a data protection officer.

GDPR's core information security requirements are contained in Article 32, which begins: "Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of the varying likelihood and severity, for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

In English, that means you have to balance what you're doing with the data against the risk and severity for the rights and freedoms of natural persons (human beings) and then develop controls to reduce any potential harm. That's a risk assessment.

But unlike a typical InfoSec risk assessment, it's not about the impact on the organization. It's about the impact on data subjects. If something went wrong, how would that affect the data subject's privacy? Or their physical and mental integrity? WannaCry, for example, hit UK hospitals quite badly.

A number of operations were cancelled, and people couldn't get their blood test results. That was a breach of the availability of personal data that had a physical, material effect on people.

Once you've done your risk assessment, you then need to develop "appropriate technical and organizational measures to ensure an appropriate level of security." GDPR specifically mentions some concepts you have to think about, such as the pseudonymization and encryption of personal data.

The regulation also specifies that you have to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services that process personal data, that you must be able to restore availability in a timely manner, and finally that you must have processes (e.g. testing) for gaining assurance that your technical controls actually work.

In summary, Article 32 says you need to do risk assessments from the data subjects' perspective. You need to maintain the confidentiality, integrity and availability of personal data, and specifically you must consider whether pseudonymization or encryption would reduce the risk to the data subject. You need to consider how quickly a system needs to be recovered before a lack of availability will affect people's rights, and what assurance framework is in place.

> **"...the controller and processor shall implement appropriate technical...measures to ensure a level of security..."**

What if You Choose not to do GDPR? What's the Downside?

If you fail to comply with the core principles, anyone—data subjects, a solicitor representing the data subject, or a not-for-profit body—can complain to your local supervisory authority. You could be subjected to an administrative fine of up to €20 million, or 4% of your global turnover. Additionally, the person or body bringing the complaint can receive compensation for damage.

If you fail to adhere to any of the data subject's rights—for example, a data subject asks you for their data and you refuse—you could receive an administrative fine of €20 million, or 4% of global turnover, or a court could award damages.

If you fail to uphold the data controller responsibilities—for instance, your security's poor, or you don't post notification of a breach—you can receive an administrative fine from your local data protection authority of up to €10 million or 2% of global turnover.

However, a general breach of GDPR won't result in top-level penalties. But if you're processing a lot of sensitive data and you choose to ignore the regulation, you could expose your organization to really heavy fines.

Addressing GDPR: Getting Started

1 As an IT professional, you should start by asking the following questions:

- Do you have personal data of data subjects?
- Does the regulation apply to you?
- Who are your data subjects? (Data subjects typically include customers, contractors, current and former employees/colleagues, and prospective employees.)
- What type of data is it, and how much do you have?
- Do you have any special category data? (Certain types of data, if released, would have a serious effect on data subjects. In the regulation, it's classed as special category data —health records, people's sexuality, religious beliefs, and political beliefs—anything that would be used to discriminate against people.)
- Do you process data about criminal activities or criminal records?
- Do you have any financial data? Or data that could be used to create financial harm to people? How much of that data do you have?

2 Next, work out the big picture. Is GDPR a big undertaking for you? Start off by making a catalog of all your systems and third parties. Is all your HR data in a single system, or do you have it in an applications system, a performance management system, a payroll system, an HR system, etc.? You need to get a picture of how much data your organization has and how complex it is, which will help you create a regulatory risk assessment for your organization.

Does GDPR pose a big risk for your organization because you're processing a lot of personal data and a lot of special category data across a lot of systems? The result of an organizational risk assessment should be able to tell you this.

3 Once you have the big picture, you need to create a governance framework for GDPR. You need to find someone in the organization who owns GDPR, who can procure a GDPR compliance budget, and who can talk to other managers about why this is important for the organization.

In some organizations, the leader is whoever has the customer data. In other organizations, it's the chief operating officer, the head of risk, or the head of finance. It should never be the CIO or head of IT: GDPR is not solely an IT issue.

4 The next step for IT is to map where all the data is. Where do you collect it? How do you collect it? Is it on a website? Where does it go to then? How do you store it? If you store data, do you have a process for deleting it?

If you've got a lot of data, do this selectively. Start with where you've identified high-risk data, then work down from high-risk data to low-risk data. The results should be fed to the legal team, who will check that all the processing you're doing is fair and lawful and allowed under the regulation. As a result, the legal team may update their privacy policy and how they communicate with data subjects. Your organization may also decide to appoint a data protection officer.

5 Having checked whether the processing is lawful and allowed, the next step is to delete unwanted data, such as duplicated data that was moved between systems or is on old systems that are no longer in use. You may have to delete records that the business has decided are no longer required, or that are beyond the data retention time they should have. So there will be quite a big data deletion exercise to go through. You may also need to delete specific fields within some databases.

6 What comes after the data deletion exercise? Hopefully, you're left only with data that you have a legal reason for processing, and that you need. Now it's time to do some risk assessments. Look at that data and ask yourself:

- What effect would a breach of confidentiality, integrity and availability have on a data subject?
- What third-party risks are there?
- Are the right contracts in place with third parties?
- Are you happy with the security of those third parties?

7 You might discover some vendors processing data outside the EU, so you need to talk to your legal team and ask them to deal with that.

The next thing is to work out how to respond—or whether you're going to respond—to all those potential data subject requests.

- How will you verify the identity of the person making the request?
- How will you give people copies of their data?
- How will you erase data or restrict processing?
- What about people who object to automated processing?
- How will you handle requests to correct data?
- Are you likely to receive data portability requests?

Once you've assessed all your risks, you need to prioritize them. With a prioritized list, you can decide the order of what to do between now and May 25, 2018.

This is also a really good time to look at your access control, in particular, to assess everyone's privileged access so that only the minimum necessary number of people have access to personal data.

You'll also review your organization's baseline security posture based on the risks you've identified, on what's normal for your type of business, and on cost. You might decide to use pseudonymization to create different security zones. For example, you may have a high security zone where you actually keep identifiable personal data, and a low security zone where all the data is pseudonymized, and then manage the boundary between a high security zone and a low security zone.

8 For any currently active projects, you should perform data protection/privacy impact assessments. It will be much cheaper to add privacy-enhancing technology to an in-flight project now than it will be to add it afterwards.

Based on the size of your organization or the types of data it processes, you may need to create formal records of processing. These could be requested on demand by the local supervisor in your country, and they're essential to be able to demonstrate accountability. If you look at Article 30, the records of processing must answer these questions:

- Why are you processing this personal data?
- What are the categories of data?
- Who are the data subjects?
- Who do you disclose this data to?
- How long do you keep this data?
- How would you describe your technical and organizational security measures?

You also must create incident response plans. Most InfoSec professionals have plans in place, but you need incident response plans that deal with how GDPR defines an incident:

"A personal data breach means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data, however that happens."

So a personal data breach includes a loss of availability or a loss of integrity, as well as a loss of confidentiality. Remember, if you have a personal data breach, you have to notify the appropriate authority in your country within 72 hours. If the breach exposes data subjects to high risk, you will also need to notify the data subjects.

The way to do that well is to make sure you have a breach management plan, test the plan, and make sure your legal and communications teams are involved.

In summary, preparing for GDPR involves:

- Working out where the data is
- Deleting unwanted data
- Doing some risk assessments
- Working out how to respond to data subjects' requests
- Creating a risk register, which will give you a list of things to do
- Creating records of processing
- Drafting and testing an incident response plan

Making GDPR Compliance Business as Usual

You're also encouraged to work out how to integrate the GDPR requirements into your normal business processes, because you'll have obligations to abide by the core principles, respond to data subject requests, and carry out your responsibilities as a data controller on an ongoing basis.

For example, any business analysis that involves personal data must be able to answer the question, "Do we have the legal right to do this with the personal data?" You need to start designing systems by asking, "What's the minimum data we need?" New projects must define data retention periods from day one.

If a data subject exercises one of their rights, you must know how to do it. In any new system you build, how will you support all those data subjects' rights, such as the right to be forgotten or the right to have copies of all the information you hold?

You also need to build privacy by design or data protection by design into your software development and change life cycle. You need to do risk assessments from the perspective of data subjects, not just the perspective of the organization, and consider third-party risks in more detail. And finally, you need to create governance and documentation so you can demonstrate ongoing accountability.

Final Thoughts

The best way to prepare for and deal with the General Data Protection Regulation is to ignore most of the hype. Remember, only three articles out of ninety-nine are information security-related. There's a lot of business change and culture change that needs to happen in your organization. Start by working out whether GDPR applies to you. Talk to the legal team. Then do that big picture exercise. Find out who your data subjects are, how much data you have, how many systems you have, and how to comply with GDPR. Then use this plan to help you incorporate these principles into your business processes.

The mission of RSA Conference is to help professionals stay on top of cybersecurity trends, issues, and solutions. Visit rsaconference.com today to read posts from industry leaders, watch videos, view more special reports like this one and receive special offers on upcoming conferences.

Visit RSA Conference.com

About John Elliott

You can find John on Twitter @withoutfire and on Pluralsight, where he authors regulation-focused training courses for IT professionals.

This paper is intended for information security and IT professionals—it provides general guidance, and it isn't legal advice. You should always consult a qualified lawyer if you want to find out specific information about how GDPR will affect your organization.

Follow us on: #RSAC