
Is your Company ready for the EU's GDPR?
The clock is already ticking!
pandasecurity.com
panda

The GDPR regulations are a response to an increase in cyberattacks and stem from a need for greater collaboration between public and private entities to remedy this ongoing problem.

The creation of a common digital framework is **an extra security barrier for one of the greatest corporate assets: data.**

1. Introduction

The new General Data Protection Regulation (GDPR) was approved by the European Parliament and Council of the 27 April, 2016. It came into effect on 25 May, 2016, and will begin to be enforced **25 May, 2018.**

The GDPR sets standards to ensure a uniform level of protection in the processing of personal data of natural persons within the European Union and to the free movement of such data within Member States.

We've put together this simplified document to facilitate the understanding of the most relevant lines of the new regulatory framework and thus help organizations to obtain a top-level view of the changes that the framework will incorporate. Ultimately, the goal of this document is to help companies adjust to the new requirements.

We encourage the reader to consult the General Data Protection Regulation in full, where all requirements and their implications are given in detail.

2. Main Conclusions

The GDPR regulations are a response to an increase in cyberattacks and stem from a need for greater collaboration between public and private entities to remedy this ongoing problem. The creation of a common digital framework is an extra security barrier for one of the greatest corporate assets: data.

Companies will now have to make any security violations they suffer public and notify the affected users within 72 hours This will increase corporate network security budgets. A mandate such as this is already in effect in the United States.

The focus of corporate security has shifted from infrastructures to people (identity and access management), something which has not always been adequately addressed.

The paradigm shift that lead to the adoption of the GDPR derives from a double necessity: on the one hand, to take preventative security measures with regard to data privacy, and, on the other hand, to accredit compliance and the delegation of responsibility.

New roles have emerged, such as the DPO (Data Protection Officer). The DPO will be responsible for reporting and advising on the company's obligations, supervising compliance, cooperating with the control authority, and acting as an intermediary with data holders.

In order to develop and implement a plan of action for businesses to adapt their practices to the GDPR, cybersecurity solutions in the company must be advanced and in line with the new paradigm, offering proactive rather than reactive security.

3. What is the General Data Protection Regulation?

The EU regulation seeks to protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data, whether they are processed by private entities or by public authorities.

The right to access, the right to rectification, the right to withdraw consent, the right to object, and two new rights are recognized: the right to erasure, alternatively called the "right to be forgotten", and the right to data portability.

Also detailed are the specifications of transparency requirements and the limitation of the processing of personal data for purposes of archiving in the public interest, or for scientific and historical research or statistical purposes.

Another new addition is the reference to the processing of Europeans' data by entities established in Europe and outside the European Union that carry out activities within the EU and that involve the processing of personal data, even if they do not have physical presence in the territory of the bloc.

To this amendment is added the obligation for public entities to designate in certain cases a DPO to ensure compliance with the regulations. The main difference with the Security Manager is that the DPO must have duly accredited regulatory knowledge.

This measure also affects almost all private companies. Although it depends in principle on the amount of data processed and the company's susceptibility to attacks, the regulation is somewhat ambiguous in this regard.

Additionally, the regulation establishes the obligation to keep the Data Protection Authority (DPA) notified of any security incidents that the company has suffered. This agency will even have the authority to require that the company make the details of these incidents public within a maximum period of 72 hours after becoming known.

4. Basic Information on the GDPR

1. Who does it affect?

The regulation affects any Company that handles the personal data of natural persons belonging to the EU, even if they are not physically present within the territory.

The term natural persons is understood to be not only customers, but also candidates, ex-clients and users of products and services that may have been acquired by a third party, as well as a company's employees and collaborators.

2. How much time do companies have to comply?

Although it was approved by the European Parliament and the Council on the 27th of April, 2016, and came into effect on the 25th May of that year, the legislation will not be applicable until 25 May, 2018.

3. What is considered to be Personal Data and subject to the GDPR?

Personal data is considered to be any information about a person whose identity is able to be determined, whether directly or indirectly, by name, ID number, location data, an online identifier, or information relating to the physical, physiological, genetic, economic, cultural or social identity of said person.

The GDPR applies to the treatment of personal data of natural persons that are located within the EU. Note that, curiously, the regulation is only applicable to living people.

It will affect businesses that process **the personal data of natural persons in EU Member States.**

It will be applicable **starting May 25, 2018.**

It will apply to the processing of **personal data of natural persons within the EU.**

4. What is considered to be Sensitive Personal Data?

The regulation establishes special categories of data which are considered sensitive and require special protection, either by their nature or by the relationship they may have with the fundamental rights and freedoms of individuals.

The regulation explicitly prohibits the processing of sensitive personal data which may reveal: ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union affiliation, genetic data, biometrics that allow the univocal identification of a person, and data relating to health, sex life, or sexual orientation.

As an exception to the prohibition, the regulation allows for special categories of data to be processed when the data subject has given his or her consent, or when it is necessary to protect his or her vital interests, or when the individual has made his or her data public, or where the processing of said data is legitimately carried out by a non-profit organization.

5. What are the consequences of violating regulations

The regulation authorizes regulators to impose particularly high fines that may amount to up to € 20,000,000 or 4% of the total annual global turnover of the previous financial year, whichever is greater. However, as we will see below, sanctions will not be the only consequences of non-compliance when it takes effect in 2018.

Some data is considered sensitive and requires special protection.

Fines of up to **20,000,000€** or **4% of the annual global turnover** of the previous year.

5. Some Rights and Requirements under the GDPR

The aim of the GDPR is to strengthen the protection of EU citizens' data. To do so, companies must comply with a set of requirements, enabling natural persons whose personal data is collected, stored and processed by said companies to retain a series of rights.

In this section, we collect some key requirements that the company must adhere to and the most relevant rights of natural persons that the new regulation lays out. Your understanding will help to better size up the amendments and the next steps to be taken in order to comply with the GDPR.

1. Obligation to report a data security incident

Security incidents concerning personal data must be notified to the corresponding control authority within 72 hours after it has been recorded.

The notification will include:

- Description of the nature of the incident and its impact.
- Number of data subjects concerned and the number of personal data records concerned.
- Name and contact information of the Data Protection Officer.
- Description of the likely consequences of the personal data breach.
- Description of the measures taken or proposed.

2. Tasks of the Data Protection Officer (DPO)

A company will be required to designate a Data Protection Officer if it is a public entity or the main activity is the routine and systematic large-scale processing of data including personal data or data related to prior convictions or criminal offences.

In the regulation, the term “large scale”, which is relative and ambiguous, is not defined in depth.

It is therefore required to allocate a DPO to almost all companies

The functions of the Data Protection Officer are the following:

- Inform and advise employees who handle data of their obligations.
- Supervise compliance with the regulation, including the allocation of responsibilities, raising awareness, and training staff participating in processing operations, and the related audits.
- To provide advice where requested as regards the data protection impact assessment and monitor its performance.
- Cooperate with the supervisory authority and act as its contact point.

3. Principle of transparency and consent

The principle of transparency requires that all information and communication relating to the processing of personal data be explicit and legitimate, easily accessible, and easy to understand.

In this communication, the following must be made completely clear:

- That personal data is being collected, used, consulted, and processed, and in particular, the purposes, the envisaged time limits, recipients, the logic implied in all automated processing and, at least where profiles are concerned, the consequences of said processing.
- The risks, rules, safeguards, and rights related to the processing of personal data.
- The way in which one can assert his or her rights with regard to the processing of personal data.

4. Incentive for pseudonymization

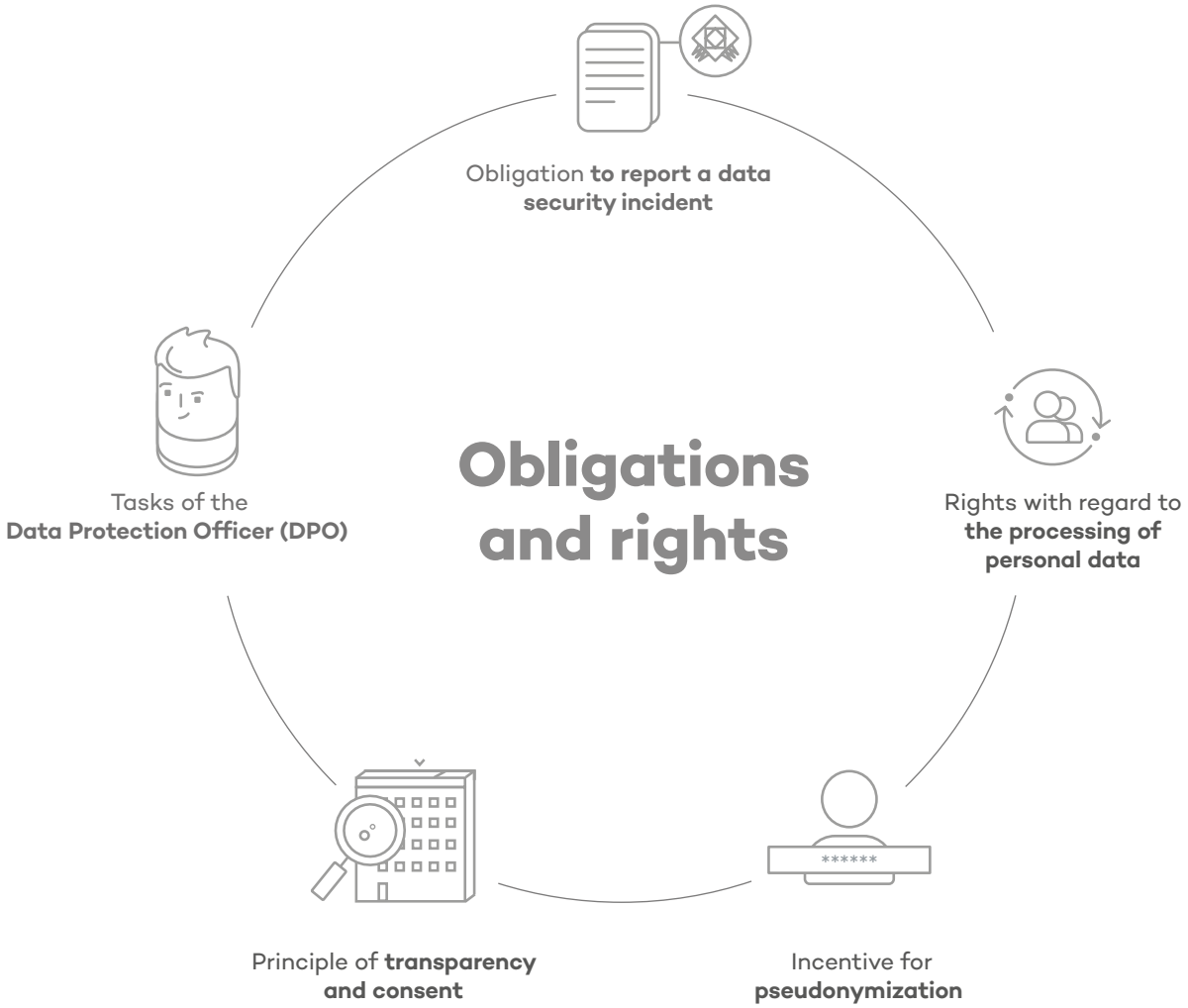
The focus of the GDPR is data relating to an identifiable individual. Therefore, the regulation does not affect data of unidentified or unidentifiable natural persons.

For this reason the GDPR creates incentives for companies to pseudonymize the data they collect. The pseudonymization is the separation of the data from the identifiers that allow direct identification of natural persons. Pseudonymization, therefore, can significantly reduce the risks associated with data processing, while maintaining its utility. Although the pseudonymous data is not completely exempt from the regulation, the GDPR eases several requirements for the controllers that use this technique.

5. Rights with regard to the processing of personal data

Companies must provide the interested party with the means of exercising their rights, including:

1. **The right to request and obtain** access to your personal data free of charge.
2. **The right to rectify and delete** personal data concerning you.
3. **The right to be forgotten,** or in other words, the right to have one's personal data removed and ceased to be treated if they are no longer necessary for the purposes for which they were collected or processed or if the interested party has withdrawn their consent to the treatment.
4. **The right to not be subject to profiling.** The interested party has the right to not be the subject of a decision based solely on an automated profile. Profiling is the treatment of data that helps to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
5. **The right to portability** of personal data, which requires companies to provide the personal data of interested parties in a commonly used format and to transfer this data to another company if they so request.



6. The application of the Regulation to businesses

The obligation to adopt data protection practices from the GDPR is a reality for virtually all companies operating in the EU markets.

Companies that do not adapt their practices will face sanctions and other problems just as serious. Making the first moves toward compliance as soon as possible should be seen as a priority, and at the same time as an opportunity, which will help to have greater visibility and control of data, a greater level of protection, and could even be a factor that sets you apart from the competition.

1. Sanctions and other problems stemming from non-compliance

If businesses do not comply with the regulation by 25 May, 2018, its date of implementation, they may be confronted with the following:

- **Direct or indirect economic repercussions.** These could result from security incidents coming from outside the company or from a company's own employees and collaborators.
- **PR Damages.** Damages to your reputation could result from security incidents not properly being reported to the public.
- **The loss of current or potential clients** may occur when the company is unable to demonstrate that it is in compliance with the regulation.
- The risk of **data-processing limits** or bans imposed by data protection audits, which could affect the normal functioning of a company.
- The possible **suspension of your service for your clients,** which could induce them to leave your service or even take **legal action.**
- **Reparations** that interested parties will have the right to claim in case of infringement.
- **Costly administration fines** that could reach up to 20,000,000€ or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

By complying with the regulation, companies will avoid the above problems, win consumer trust, and, as such, gain a competitive advantage.

Approved certification mechanism

Legislators have recognized that for many companies, **the ability to demonstrate that they adhere to the GDPR will be an advantage.** To this end, data protection certification mechanisms and data protection stamps are beginning to be introduced.

The GDPR even speaks about the possibility of reaching a common European data protection seal, and although for now the GDPR provides little details it is expected that this mechanism will be developed in the coming months.

2. Plan of action to be prepared for the GDPR

To adapt business practices to the GDPR, companies must begin by understanding their current position in their compliance to the regulation. An important first step will be for organizations to get their personal data processing procedures under control, including:

- Which personal data is being processed, including its collection, transferal, and storage.
- Where the information is, and who has access to it, including third parties.
- When and where it is transferred, including to third parties and transnationally.
- Which security measures are taken over the course of its life cycle.
- How the information is stored that allows the rest of information to be identified.
- How data identification, modification, erasure, and transferal is granted to the interested party upon request.
- How the privacy policy is communicated and archived, and in what way it is used for data processing.

By becoming aware of compliance gaps, companies will be well placed to assess the risk in their personal data processing practices and to develop prioritized remediation plans.

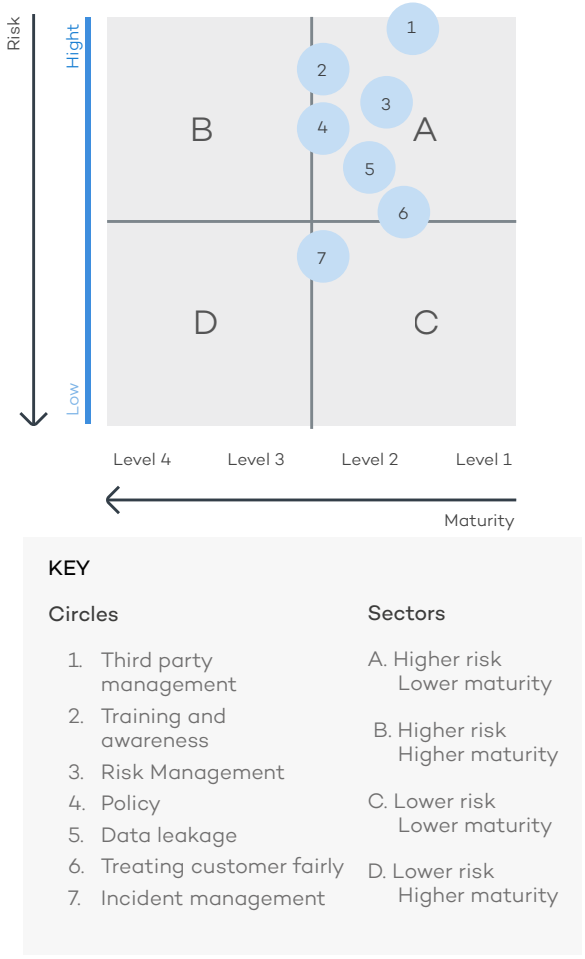


Figure 1. In the coming months, businesses will face many challenges in preparing for the GDPR. The first step is to assess where they currently stand.

7. The Reality of the Regulation for Businesses

In a survey conducted by Dell in September 2016 of a total of 821 employees responsible for data privacy at companies with more than 10% of customers in Europe, reveals that **both SMEs and large companies demonstrate a lack of knowledge about the new General Data Protection Regulation of the EU.**

In summary, companies **have no plan,** nor do they know **how to prepare** for its arrival. They also seem to be unaware of the repercussions that their non-compliance could have on both **data security** and **business** in general.

Thus, 82% of professionals in commercial and IT areas responsible for data security are **concerned** about compliance with the new regulation. Concern is greatest in Europe, most notably in Germany and Sweden, and especially in **large companies.**

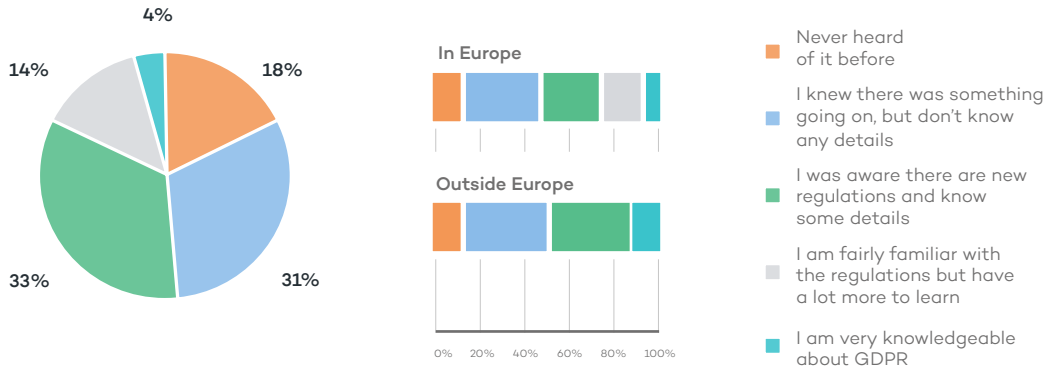


Figure 2. How would you describe your knowledge of the GDPR?

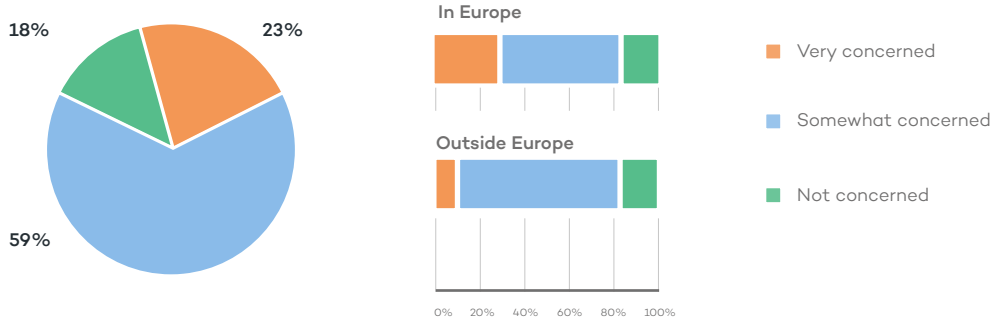


Figure 3. How concerned are you about GDPR compliance?

And this is in line with the fact that the **Germans** are the most prepared to apply the GDPR (4%), while the respondents in **Benelux** (Belgium, the Netherlands and Luxembourg) are those who claim to be the **least prepared.**

In fact, more than **80% say they know little or nothing** about the connotations it will carry, and only **3% of IT professionals are ready for it.**

The results of the survey also reflect that, while companies realize that a breach of the GDPR can have **an impact on both data security and its results, they are not clear** on the **extent** of the changes they should implement, nor the severity of penalties for non-compliance.

Only 23%, then, expect major changes to take place in their data security practices and on their technology.

More than 80% of respondents **know very little** about the new regulation, have no plan to implement the new regulation, and are unprepared. **Only 3% have a plan for its implementation.**

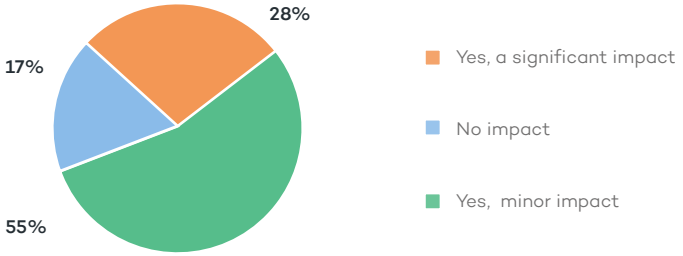


Figure 4. In your opinion, will the GDPR have an impact on your approach to data security?

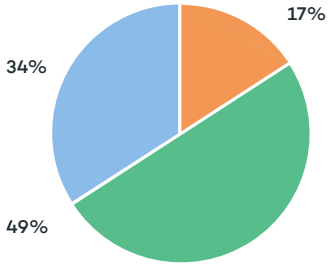


Figure 5. In your opinion, will the GDPR have an impact on your business results??

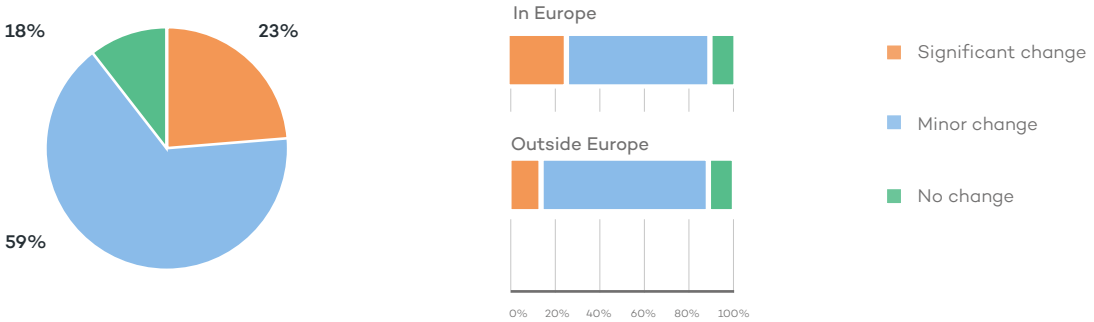


Figure 6. How much do you believe current technologies and practices will have to change as a result of the GDPR?

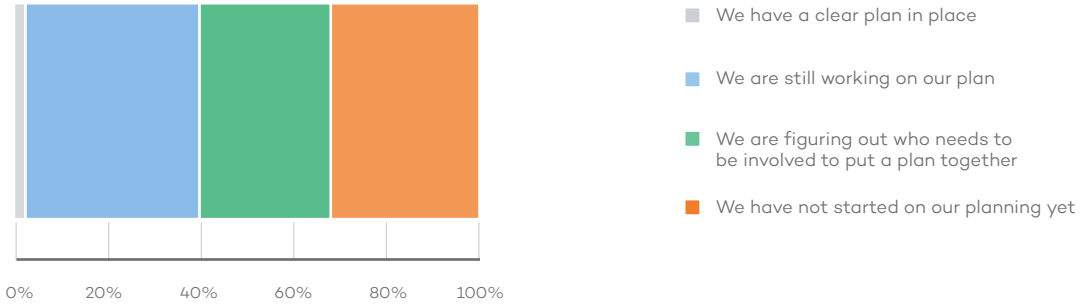


Figure 7. Does your company have a plan to prepare for the GDPR?

8. Panda's Adaptive Defense helps you meet the GDPR's compliance requirements

As we have just seen, there is, on the one hand, **a need to adapt data security practices and the technologies** that underpin them to the requirements of the new regulation and, on the other hand, companies' lack of knowledge with regard to their new obligations, the potential impact on their organizations, and the economic risks implied.

Once companies become aware of these factors, the process of assimilation will require a great effort of awareness building, training, analysis, and implementation of new practices and technology. All this effort runs the risk of being in vain if the wrong choices are made. Human error can lead to a systems security failure, and the data that is being managed by the company can be lost or stolen.

And even worse are the consequences: direct and indirect economic sanctions, reputational damage, loss of customers, limits imposed on your operations, customer complaints, and demands for compensation.

Panda Adaptive Defense minimizes these risks and helps to comply with the GDPR, based on two fundamental pillars: Security and Information Management.

These are the two keys. 1) Control over the data that is collected, stored, and processed in the company's different departments (HR, marketing, etc.), on both computers and servers, and 2) the adoption of security measures necessary to protect them from attackers.

Once companies become aware of these factors, the process of assimilation will require a great effort of awareness building, training, analysis, and implementation of new practices and technology.

From these bases, three lines of action can be drawn up that guarantee the security of data:

1. Preparation

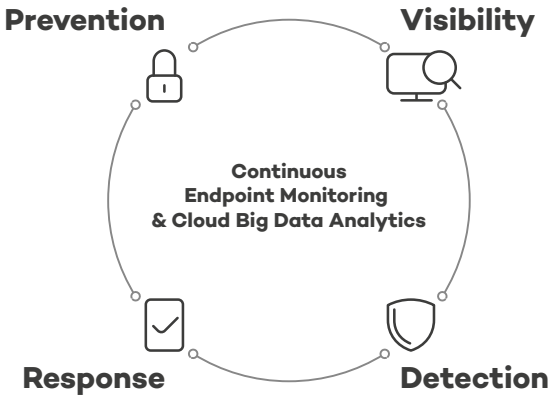
A proactive attitude is very important. A system's availability when it comes time to perform detailed forensic investigations is key to neutralizing an attack as soon as possible.

Adaptive Defense features an internal audit system to verify the security status of the IT infrastructure at any given time, even before the solution is deployed. In the implementation of the action plan for compliance with the GDPR, it proves to be an invaluable tool.

2. Protection

True security solutions must combine advanced technology with human and computer intelligence. In other words, machine learning with security experts at the helm. For a security solution to be taken seriously, it must offer the kind of prevention, detection, visibility and intelligence that can stop and prevent cyberattackers of any kind over and over again.

The protection requirements of a company, including those of the GDPR, puts pressure on security solutions to cover the following aspects that **Adaptive Defense** and **Adaptive Defense 360** provide:



- **Continuous monitoring,** by recording and monitoring all activity of running processes in order to stop untrusted software in its tracks at the time of execution, detect advanced threats in real time, respond in a matter of seconds, and recover instantaneously.
- **Detecting the execution of untrusted files,** which allows your company to reduce the surface of attacks being carried out. You should make sure that the security solution you are looking for classifies all applications running on your devices as either trusted or malicious.
- **Intelligent threat detection** A threat is always faster than any device that you wish to protect. So you, the user, shouldn't be the one saddled with the task of monitoring the response. Effective security solutions must be able to operate autonomously and automatically to adapt to the operating environment, which is unique to your organization.
- **Quick and automated response.** Organizations are saturated with the volume of events and alerts generated by their systems, but once the cybercriminal has infiltrated, the theft of information can happen in a matter of seconds. Therefore, the chosen security solution must be able to quickly identify an ongoing attack, establish measures to avoid damage and relieve the workload placed on systems. In this way, you can cut costs and automate tasks that previously took days to complete.

3. Visibility and Control

Data is a living thing. It grows, it changes, and even moves. Managing it in a way that complies with the new regulation is just the beginning. Once everything is in place to do so effectively, there's still the question of keeping constant tabs on it and knowing how to detect any anomalies that may occur.

The **Advanced Reporting Tool (ART),** Adaptive Defense's optional module, is a security intelligence tool that automatically generates reports on all endpoint activity.

The intelligence system gives companies the ability to identify unusual behaviors and attacks, as well as internal misbehavior. This is based on

the continuously monitored events occurring at the endpoints, sent to the Adaptive Defense Platform to be enriched. ART allows companies to:

- **Supervise and control** improper use of corporate resources.
- **Receive alerts** with regard to security indicators and corporate resource use, as well as files containing personal data.
- **Perform analyses** of key aspects regarding security incidents and anomalies in the access of personal data files.
- **Perform calculations and graphic visualization** on endpoint activity.

If a company's security department utilizes a corporate **SIEM** (Security Information Event Management), the open nature of the Adaptive Defense Platform facilitates real-time integration of the activity information monitored at the endpoints in the set of logs managed in the SIEM.
This allows the organization's security teams or the external Security Operations Center (SoC) to:

- **Expand their integral security approach** encompassing not only the perimeter network, but the endpoints.
- **Obtain a privileged view of attacks and their overall impact,** allowing in-depth forensic analysis.
- **Get the most** from the information gathered in order to better know the situation of your IT infrastructure and implement improvement strategies.
- **Enrich your SIEM data** by correlating it with additional data originating in endpoints, bringing a higher grade of corporate intelligence to your systems.

Panda Adaptive Defense ensures the security of the company and its data. The companies that have put their trust in Adaptive Defense have already made headway on the road to GDPR compliance. Here's what Adaptive Defense has brought to the table at these companies:

- **Protection** of personal data processed on a business's systems, stopping, for example, any untrusted process from running.
- **Risk reduction** and **key activity indicators and endpoint status,** which helps to establish security protocols and keeps administrators apprised of vulnerable devices, anomalous internal and external network activity, etc.

Figure 8. Example of the visibility provided by ART.

Figure 9. Geolocalization of a company's outgoing traffic.

- **Tools** to satisfy the requirement to **notify authorities of security incidents within the first 72 hours after a breach.** Thanks to forensic analysis tools, alerts, visibility, and the total control that Adaptive Defense/Adaptive Defense 360 offers, your company will always be set up with the adequate resources to quickly issue a report and come up with a plan of action to avoid future incidents.
- **Control mechanisms and data management for the DPO,** who will be notified in real time not only of security incidents, but also whether or not these incidents involve compromised personal data files. Both ART, via real time alerts, control panels, and reports, and the corporate SIEM notification systems will alert the DPO of anomalous activity involving access to personal data files.

9. Frequently asked questions about the GDPR

1. Who are the main entities and agents affected by the GDPR?

The European Data Protection Committee. The Committee is composed of a supervisory authority from each of the twenty-eight Member States and the European Data Protection Supervisor. The role of the Committee will be to review what is working and what is not working, and also give advice and provide guidance.

Supervisory Authorities. Independent public authority established by a Member State to enforce local legislation.

Processing supervisor. Natural or legal person, public authority, service or any other body that treats personal data on behalf of the controller. The manager does not determine the purpose and the means of treatment. They only process the data as requested by the controller.

Example: Outsourced payroll management company or cloud provider such as Microsoft Azure where data is collected, stored and processed.

If a provider is acting in accordance with requirements, this is a data controller. Under the old directive, a fine would be imposed only in case of non-compliance with the controller. Under the new regulation, the manager is also responsible for fulfilling his own obligations, such as having adequate security measures.

Controller or processor. The person or department responsible for defining what personal data the company needs and for what purpose. Then, the company requests the data from people (employees, customers, general public, etc.). A simple example could be a webpage that asks for your name and address to send you a package. The company that requests the information and establishes to what purpose it will be used is responsible for the data.

The controller must not only comply with the regulation, but also demonstrate compliance. This is one of the main differences between this regulation and others. The controller will have to be able to demonstrate compliance at any given time, following the requests of the Supervisory Authority or the interested party.

2. What will happen to the Data Protection Laws of Member States?

The regulation does not repeal them nor can they be repealed, as they are attributable to each Member State. The regulation causes the normative displacement of Member State Laws in anything that is in conflict with the European regulation. But these laws will remain in vigor until they can be completely repealed or modified to adapt them to the GDPR.

Consequently, it will be necessary to take into account both the GDPR and Member State law. When there is conflict between one and the other, then the one dictated by the GDPR will apply above the Member State law.

3. Should companies review their privacy notices?

The short answer: yes. In the information provided to interested parties, the regulation provides for the inclusion of issues which were not necessarily mandatory according to the regulation and many overlapping national laws. For example, it will be necessary to explain the legal basis for the processing of data, define its retention period, and advise interested parties that they can address their complaints to the Supervisory Authorities if they believe there is a problem with how their data is being handled. It is important to remember that the regulation expressly requires that the information provided be easy to understand and be presented in clear and concise language.

4. Does it change the way consent is to be obtained?

One of the fundamental bases for processing personal data is consent. The regulation requires that consent, in general, be voluntary, informed upon, specific, and unequivocal. In order to be able to consider that consent is unequivocal, the regulation requires that there be a declaration on the part of the interested parties or a positive indication that the interested party has given his or her agreement. Consent cannot be inferred from the silence or inaction of clients or other physical persons.

Companies should review how consent is obtained and recorded.

It must be taken into account that consent must be verifiable and that those who collect personal data must be able to demonstrate that the person concerned has given them their consent. Therefore, it is important to review the consent recording systems so that it can be verified by an audit.

5. Can I outsource or divide up DPO responsibilities?

Limited-budget companies can outsource or share DPO tasks. In Germany, under the Federal Data Protection Act, companies with more than 9 employees must appoint a DPO, but it is common practice to outsource the role to specialized data firms or law firms.

The regulation establishes that a business group may appoint a single DPO as long as he or she is easily accessible from each establishment. If you decide to outsource your DPO it would be necessary to establish a service level agreement (SLA) to ensure that you can comply with the GDPR. Compliance is achieved not only by checking the DPO checkbox, but also by having a DPO who can respond to the various requests of interested parties at any time.

6. When, how, and to whom do I report a security incident?

When? A security incident should be notified whenever it affects the personal data of natural persons, whether an incident results in loss or theft or if it is simply accessed.

If the incident is not reported promptly, it can result in fines of up to 10 million euros or 2% of annual turnover.

To whom? It is important to keep in mind that there are two different thresholds, one for notifying customers or the general public, and another for alerting the Supervisory Authority.

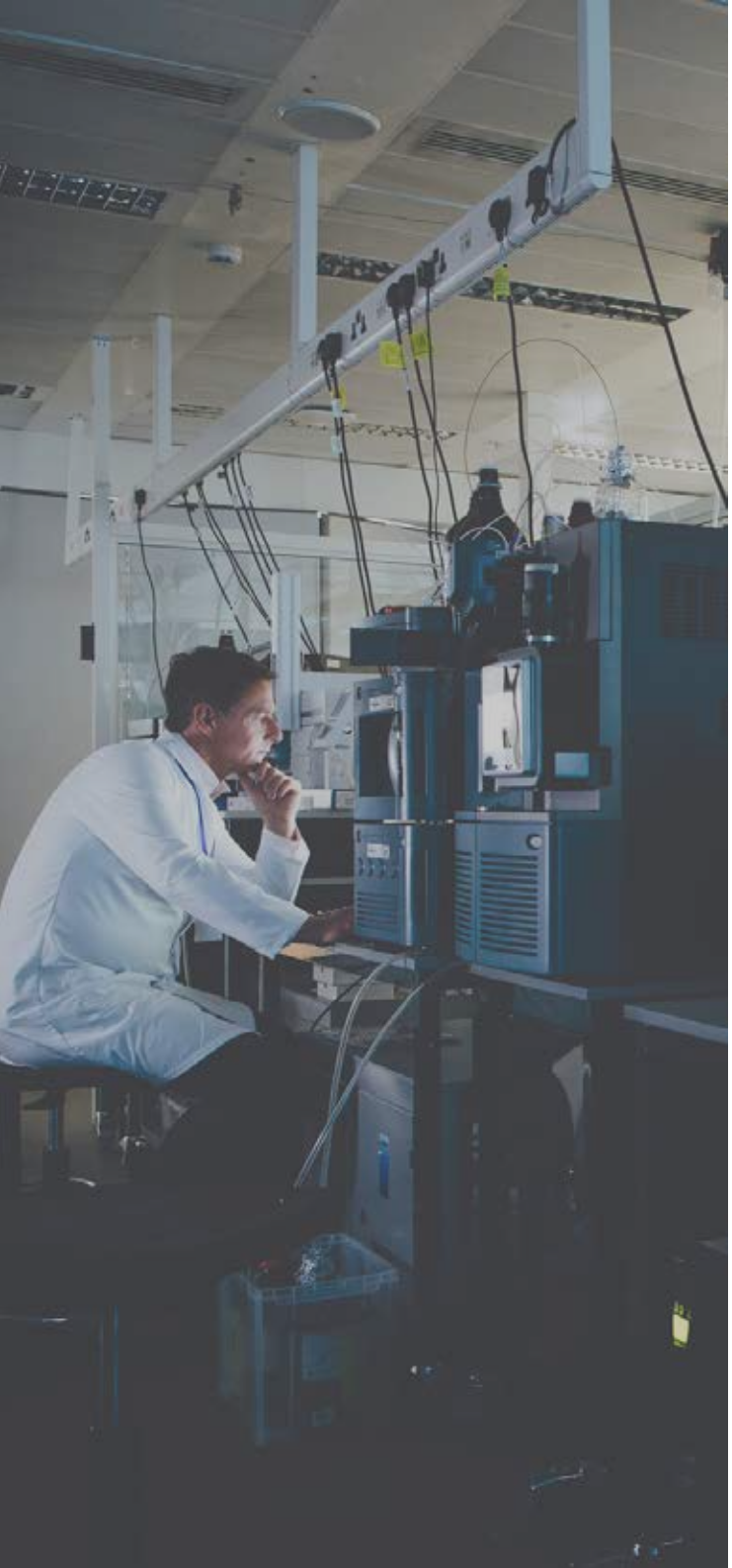
- If the personal data accessed includes any identifier, for example, email addresses, online account ID or IP, it will be necessary to notify the affected natural persons.
- If the data contains monetary information - bank account numbers or other financial identifiers - then the incident is likely to harm the individual and the Supervisory Authority must be notified.

How? In addition to describing the nature of the incident, the notification should mention the types of data, the number of individuals, and the number of records exposed. The company should describe the possible consequences of non compliance, as well as any mitigating efforts that need to be made.

What's the deadline? The notification to the Supervisory Authority should be issued within 72 hours after the incident.

How can you prepare yourself for it? You should make sure that you have an internal incident reporting procedure and that you have full details of the incident at your disposal, especially if personal data has been accessed. Remember that you must submit a dossier of corrective measures that have been carried out. For this you will need information on the attacker's entry routes, the setup of workstations attacked and their vulnerability, the affected systems, etc. This will make it easier to make decisions about whether to notify the public and Supervisory Authority.

In light of the short reporting deadlines for an incident, it is important to have robust attack detection, forensic investigation, real-time alerts and detailed reports to be analyzed and presented to the public and Supervisory Authority.



Panda Adaptive Defense is a company's greatest ally in the process of assimilating to the GDPR, offering:

- Protection of personal data processed in the company's systems.
- Reduced risk of being subject to attacks.
- Tools to fulfill requirements for reporting security incidents in the first 72 hours.
- Mechanisms of control and data management for the DPO, which provide notification in real time, not only of security incidents, but also of incidents in which potentially at risk files contain personal data.

7. Should companies start implementing the measures provided for in the regulation right away?

Not necessarily. The regulation is in effect, but will not be applicable until May 25, 2018.

However, it may be useful for companies to start assessing the implementation of some of the foreseeable measures:

- Perform risk analysis of your data systems, starting by identifying the type of processing they carry out.
- Establish data processing records.
- Implement impact assessments or any other foreseeable measures.
- Design and implement procedures to adequately notify authorities or interested parties of any security incidents that may occur.

Panda Adaptive Defense ensures the security of the company and its data and helps in the management of information. Companies that rely on Adaptive Defense are already well on their way to complying with the GDPR.

10- About Panda Security

This report uses data gathered by Panda Security's multi-disciplinary team, a network of experts founded in 1990 whose mission is to simplify complexity by creating new and better solutions to safeguard the digital lives of its users.

We openly share the knowledge of our expert technicians at PandaLabs, the laboratory that processes threats and neutralizes them in real time. We are developers that specialize in advanced cybersecurity, as well as product and marketing experts.

We are reinventing cybersecurity and making it accessible worldwide.

panda

More information:

www.pandasecurity.com/intelligence-platform

by calling:

+39 02 87 32 32 10

or by email

info@it.pandasecurity.com

panda

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda