

Preparation Guide to the New European General Data Protection Regulation



The General Data Protection Regulation (GDPR) is to protect citizens' data rights and to ensure that companies must be more proactive in protecting data against both internal and external threats.

This responsibility will help create extra security awareness against cyberattacks looking to compromise one of the greatest **corporate assets: data.**

1. Introduction
2. The Application of the Regulation to Businesses
3. Obligations and Advantages
4. Panda's Adaptive Defense Can Help Companies Comply with the New Regulation
5. About Panda Security

1. Introduction

What is the GDPR?

The new General Data Protection Regulation was approved by the European Parliament and Council and it came into effect on 25 May, 2016, and will begin to be enforced from **25 May, 2018**.

The purpose of the two year period leading up to the enforcement of the Regulation is to give EU Member States, Institutions, and organizations that handle data the time to prepare and make the necessary arrangements to be in conformity with the regulation before the legislation becomes enforceable.

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 it is 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, also 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.

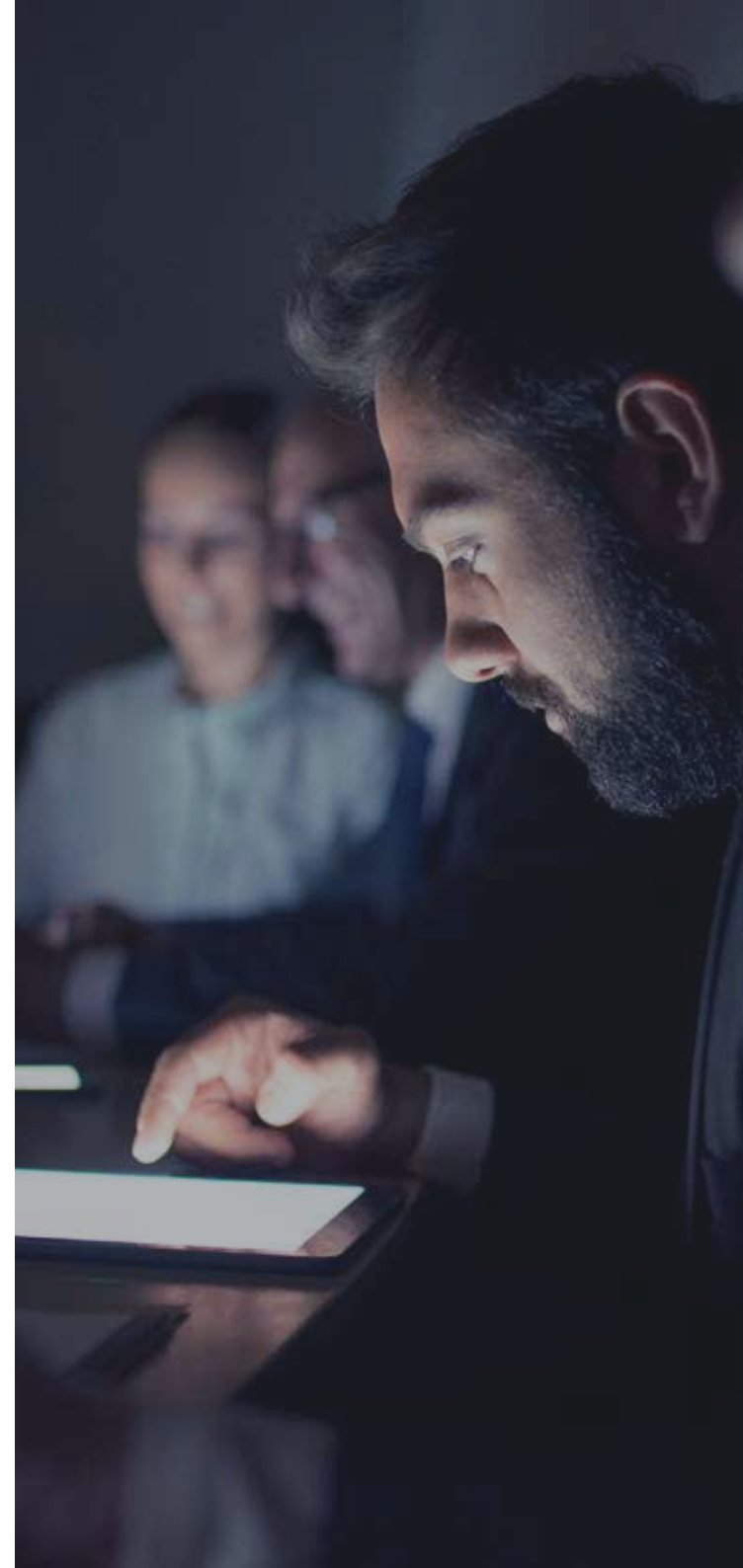
Another new addition is the reference to the processing of natural persons’ data by entities established outside the European Union that carry out activities that involve the processing of personal data of EU citizens, even if they do not have physical presence in the territory of the Union.

To this amendment is added the obligation for public entities to designate in certain cases a “Data Protection Officer” (DPO) to ensure compliance with the regulations. The main difference with a designated head of IT security is that the DPO must have duly accredited regulatory knowledge.

The regulation establishes the obligation to keep the Supervisory Authority notified of any security incidents that the company has suffered. The supervisory authority should be made aware of any breach within a maximum period of 72 hours of the company becoming aware of the incident.

Panda Security has put together this short guide to help understand the new regulation and adapt to the required changes in order to comply.

For all requirements and implications of the General Data Protection Regulation consult the official Regulation (EU) 2016/679. Contact the Supervisory Authority if in doubt (ico.org.uk).



2. The Application of the Regulation to Businesses

How does it affect your business?

For organizations dealing with data, **prevention** is the core element of the Regulation. The “proactive responsibility” of companies will play a differential role here. Acting only when a breach has already occurred is insufficient as a strategy, since that breach can cause irreparable damage to interested parties that can be very difficult to compensate. It is therefore a matter of utmost importance to implement data protection into the initial planning phase itself.

Although companies do not have to comply with the new measures quite yet, we advise **the importance of working with vision and anticipation as a competitive advantage**. It may be useful for organizations to start assessing the implementation of some of the planned measures starting now, incorporating such practices as:

- Performing risk analysis of your data systems, starting by identifying the type of processing they carry out.

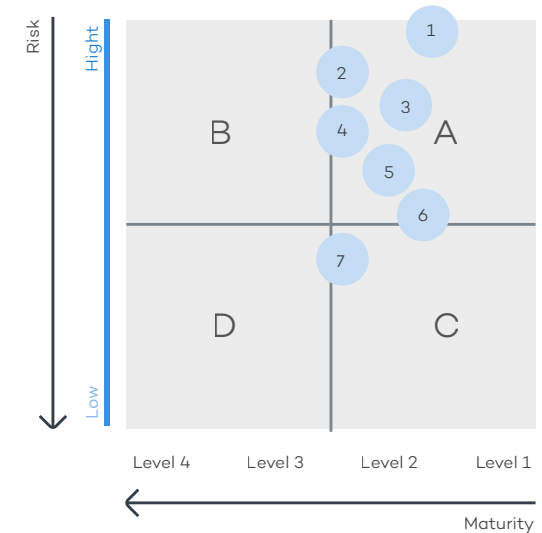
- Keeping records of data processing activities.
- Implementing impact assessments and any other foreseeable measures.
- Designing and implementing procedures to adequately notify authorities or interested parties of any security incidents that may occur.

Having a plan of action is crucial to preparing for the GDPR. Companies should begin by assessing their current standing with regard to being in compliance with the GDPR.

The first step would be to make sure that their treatment of personal data is 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 key information is stored which allows other information to be identified (pseudonymisation).
- How data identification, modification, erasure, and transferal is granted to the interested party upon request.
- How the privacy policy is communicated and is saved, at the time of data capture. 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.



KEY

Circles

1. Third party management
2. Training and awareness
3. Risk Management
4. Policy
5. Data leakage
6. Treating customer fairly
7. Incident management

Sectors

- A. Higher risk
Lower maturity
- B. Higher risk
Higher maturity
- C. Lower risk
Lower maturity
- D. Lower risk
Higher maturity

Figure 1. Businesses face many challenges in preparing for the EU GDPR in the coming months. The first step is to understand their current state and establish what follows in this report to move towards conformity.

3. Obligations and Advantages

The Regulation implies a deeper commitment to data protection on the part of organizations, both public and private. This does not mean that it should be a greater burden on companies, but rather that in many cases, the ways of managing data protection will be different from current practices.

The advantage of early compliance is that potential hurdles can be dealt with well in advance. Detecting shortcomings, obstacles, mistakes in rolling out new practices, etc., will be much more efficient at a stage when new measures are not yet obligatory and subject to oversight.

This approach will allow for errors to be corrected in time for the obligatory application of the Regulation and before sanctions and other non-compliance repercussions are introduced.

Repercussions of Non-Compliance

If businesses are not in compliance with the Regulation by May 25, 2018, they can face:

- **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 not being prepared for security incidents or not reporting properly.
- **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 supervisory authority audits, which could affect the normal functioning of the company.
- The possible **suspension of your services** to 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, businesses will avoid these problems and gain the trust of customers.

Advantages of early compliance: 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. This is a strong point in favor of early compliance. The GDPR even mentions the possibility of reaching a common European data protection seal, and although for now the GDPR provides few details, it is expected that this mechanism to demonstrate adherence to the legislation will be developed in the coming months.



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



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



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

4. Panda's Adaptive Defense Can Help Companies Comply with the New Regulation

Organizations are facing two major challenges leading up to May 2018: **addressing the need to adapt data security practices and technologies**, and **building awareness** of the risks involved, whether on a direct economic level or when it comes to the company's reputation or business practices.

A proactive attitude is crucial in this regard, and being prepared for the prevention of any incident is now more important than ever. The same can be said of the ability to carry out detailed technical forensic analyses of incidents at any moment.

Businesses that have put their trust in Adaptive Defense and its optional Advanced Reporting Tool are already well on their way to complying with the GDPR. It offers:

- **Prevention:** Adaptive Defense features an internal audit system to verify the security status of the IT infrastructure at any given time, checking for malicious processes. In the implementation of the action plan for compliance with the GDPR, it proves to be an invaluable tool.
- **Protection** of personal data processed on a business's systems, stopping, for example, any untrusted process from running.
- **Risk reduction, key activity information and endpoint status**, which helps to establish security protocols and keeps administrators aware of vulnerable devices, anomalous internal and external network activity, etc.
- **Control mechanisms and data management for the DPO**, who will be notified in real time of security incidents, and has the information available as to whether these incidents involved personal data files.
- **Tools** to satisfy the requirement to **notify authorities of security incidents within 72 hours of breach awareness**. Thanks to forensic analysis tools, alerts, and visibility of all running processes that Adaptive Defense with Advanced Reporting Tool offers, your company will be equipped with the resources to quickly issue a report and come up with a plan of action to avoid future incidents.

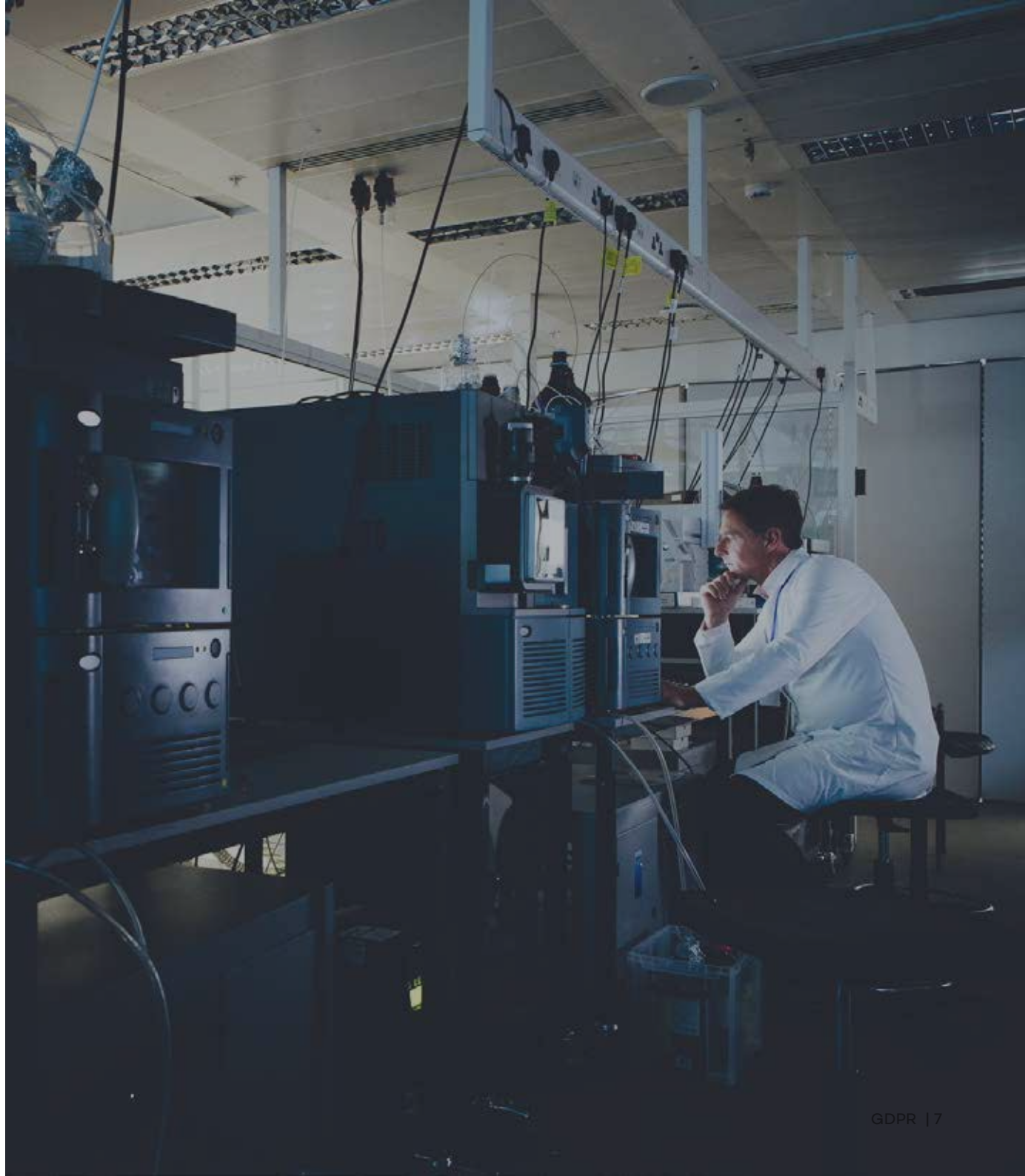
© Adaptive Defense 360



5. About Panda Security

Panda Security is a **leading global provider of advanced cybersecurity solutions** and in systems management and monitoring tools. Since its inception in 1990, it has consistently maintained a spirit of innovation and marked **some of the most important advances** in the world of cybersecurity.

Currently, the development of advanced cybersecurity strategies is at the core of its business model. Panda Security has a presence in more than 80 countries with products translated into 23 languages and over 30 million clients worldwide.




More information at:
www.inspiredtech.co.uk/panda-security

by calling:

0333 320 1021

or by email sales@inspiredtech.co.uk





🎯 Adaptive Defense 360

Limitless Visibility, Absolute Control

