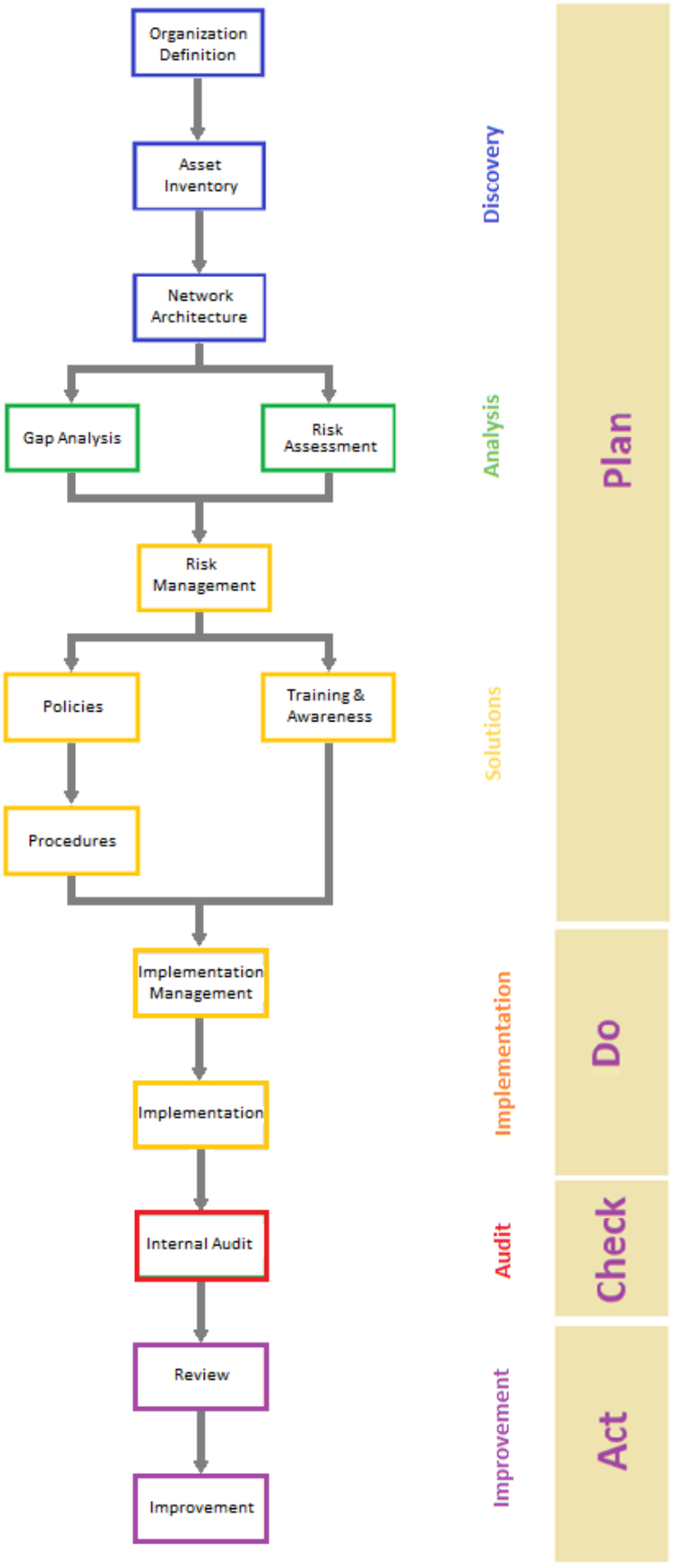
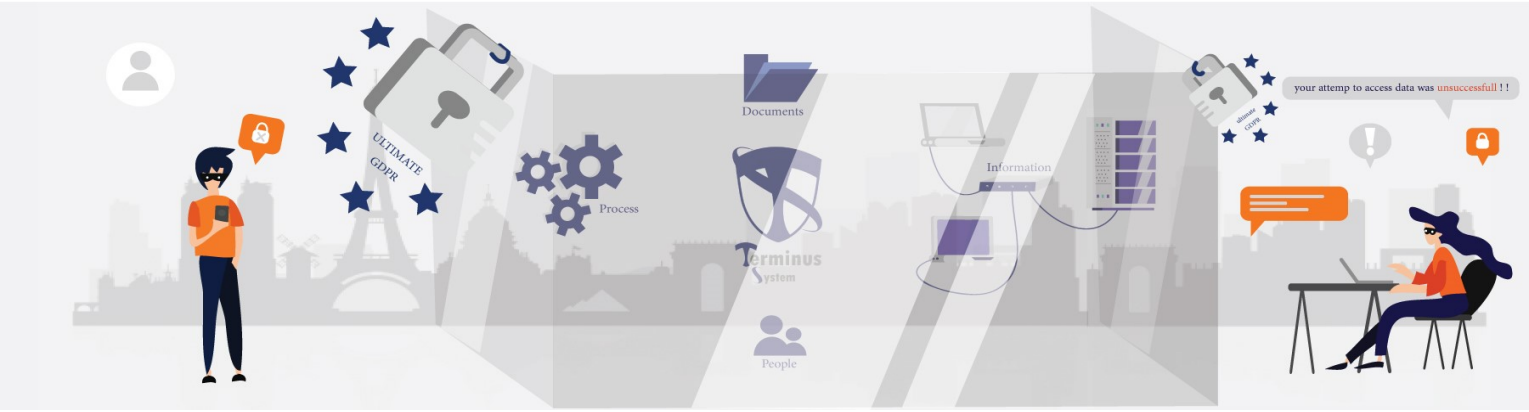
Ultimate GDPR





Organizations collect and process a huge amount of personal data for their daily operations. Most of the time, individuals have little or no awareness about how much of their personal data resides in various organizations' databases. As an organization stores more and more personal data, its risk of data loss or a data breach goes up. To avoid these security risks, many groups are calling for regulations that:

- Set high standards of privacy and security in personal data processing and retention.
- Offer individuals more visibility and control over who has their personal data, how it's collected, how long it will be retained, and what it will be used for.

The General Data Protection Regulation (GDPR) is Europe's newest data protection law, designed to unify and improve the privacy of personal data across Europe. The GDPR intends to provide European Union (EU) residents with more visibility and control over the way their personal data is collected and processed. May 25 marked the deadline for enterprises worldwide to comply with the provisions of the GDPR.

The sweeping regulation from the European Union (EU) is intended to revolutionize the relationships of data holders or processors and the people associated with that data (also known as data subjects). The GDPR protects the personal data of data subjects from the EU, including citizens, visitors and noncitizen residents, regardless of where their data is being held or processed — and penalties for noncompliance can be substantial.

GDPR conformance is a challenge for many enterprises, even ones with no current EU-resident customers or employees. Companies around the world will be affected if they hire employees with EU citizenship (including dual citizenship) — or if they ever develop customer or business-partner relationships involving EU citizens or residents.

GDPR conformance is a challenge for many enterprises, even ones with no current EU-resident customers or employees. Companies around the world will be affected if they hire employees with EU citizenship (including dual citizenship) — or if they ever develop customer or business-partner relationships involving EU citizens or residents.

But what is one of the hardest parts of getting ready (and maintaining readiness) for the GDPR? Knowing where to start. The obligations the regulation imposes could spark changes in nearly every part of your enterprise — from customer outreach via social media and data protection to archiving transaction records. There are 99 articles and 173 recitals in the GDPR that establish all obligations and requirements that organizations will have to comply with when the GDPR goes into full effect on May 25, 2018.

Who does the GDPR apply to?

The GDPR applies to all businesses that:

- Operate in the EU.
- Process the personal data of EU residents (regardless of location).
- Provide goods or services to people in the EU (regardless of where processing takes place).

What are the consequences of not complying with the GDPR?

Once the GDPR is enforced, organizations could face a few different penalties for non-compliance depending on the infraction. Possible consequences include:

- Suspending all data processing.
- Paying a fine of up to four percent of their annual worldwide turnover or 20 million euros—whichever is higher.
- Other sanctions including warnings, reprimands, and corrective orders.

GDPR: Why Data Protection Is Difficult

The GDPR focuses on securing and ensuring the privacy of EU citizens' personal and sensitive personal data. Data, including personal data, is hard to control because it's dynamic, distributed and in demand. As data grows, changes and multiplies, keeping track of it becomes more difficult. Your business can't stop to reexamine and classify data every time a customer record is updated. (Learn more about how to accelerate your GDPR efforts.)

In the age of big data analytics, cloud computing and mobile access, organizations can struggle to keep track of all their data sources. Data is increasingly accessible — and in increasingly complex combinations. Due to this, figuring out every place you hold the personal information of even a single EU data subject is an enormous challenge — and with hundreds or thousands of customers, a vastly bigger one.

How should personal data be processed?

The GDPR has defined six important principles on how personal data should be processed. It mandates that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner (Lawful, fair, and transparent).
- Collected only for specified, explicit, and legitimate purposes. Data should not be further processed in a manner that conflicts with these initial purposes (Purpose limitation).
- Adequate, relevant, and limited to what is necessary (Data minimization).
- Accurate and, where necessary, kept up-to-date (Data accuracy).
- Processed in a way that data subjects can't be identified once their data has been used for its original purpose (Storage limitation).
- Processed in a manner that ensures security of personal data. This includes protection from accidental loss, destruction, or damage by implementing required technical and organizations measures (Data integrity and confidentiality).

How to start?

For a regulation as complex as the GDPR, going at it alone can mean wasted time and uncertainty. Software tools, such as ***Terminus System Ultimate GDPR***, can help you face these challenges with higher efficiency and accuracy, at a low cost and with minimal operational overhead — whether your data is on-premises or stored in the cloud.

Wherever you are on the road to GDPR readiness, there are steps you can take to help your enterprise find GDPR personal data, uncover risk and take action.

What is Ultimate GDPR?

The **Ultimate GDPR is a very smart and advanced tool that** helps you to regulate collecting, store, process, and transfer personal data. This advanced and smart solution, has six steps and provides a holistic approach to help you on your journey towards GDPR compliance. .

Discovery

The first step towards GDPR compliance is identifying where personal data resides. An inventory of your organization's personal data is a prerequisite for GDPR compliance. During the data discovery phase, you need to know:

- Where and in what form personal data is stored.
- What types of personal data are stored.
- Who has access to personal data, including when, where, and how personal data is used.

To achieve these goals the followings should be done:

- Organization Definition
- Asset Inventory
- Network Architecture

Analysis

After data discovery, the next step is to establish accountability in the flow of personal data within your organization. Enforce policies, rules, and regulations to ensure data handling, sharing, and storage techniques are in compliance with the GDPR. Some important questions organizations should answer during this phase include:

- What's the lawful basis for holding this personal data?
- Is any personal data shared with third parties? If so, why?
- How is personal data processed?
- How long can personal data be stored?
- How do we track a data subject's personal data?

To achieve these goals the followings should be done:

- Risk Assessment
- Gap Analysis

Solutions

The GDPR mandates that data be stored, processed, and shared in a manner that ensures its security. Depending on the type, context, location, and volume of personal data that your organization stores, you may need to implement measures such as encryption, pseudonymization, and anonymization to reduce the risk of data exposure. During the securing phase, you need to ask yourself:

- What technical and organizational measures are in place to safeguard personal data?
- Can you detect and respond to system infiltrations or data breaches in real time?
- Are regular data protection impact assessments being carried out?
- What are your organization's provisions for handling the data breach notification process?
- Is there a data security incidence response plan in place?

To achieve these goals the followings should be done:

- Risk Management
- Policies
- Procedures
- Training & Awareness

Implementation

The goal of this phase is to implement the solutions. In this phase, implementation of the solutions presented in the previous phase will be considered. Risk treatment solutions are divided into two main technical and system parts, each with the following components:

- Technical solutions which are Configuration modification, Providing new hardware and/or software
- System solutions which are Implementation of training and awareness courses, Implementation of policies and procedures

To achieve these goals the followings should be done:

- Implementation Management
- Implementation

Audit

In this phase, the effectiveness of the implemented solutions is measured. In fact, by assessing the organization's information security status before and after the implementation phase, the effectiveness of the implementation of the solutions is measured.

To achieve these goals the followings should be done:

- Internal Audit

Improvement

GDPR compliance isn't a one-shot exercise; it's a continuous process of keeping up with a consistently evolving compliance environment, changing technologies, and data privacy requirements to demonstrate compliance at any point of time. In the last phase, all remaining issues observed in the Audit phase are removed and the final corrections in the system are considered.

To achieve these goals the followings should be done:

- Review
- Improvement

Terminus System

www.Terminus-System.com