PALADION
HIGH SPEED CYBER DEFENSE

General Data Protection Regulation

GDPR Handbook for Information Security Managers

Author:
Paladion Consulting Practice

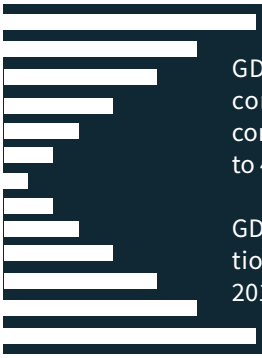
TABLE OF CONTENTS

1. Why Does the EU General Data Protection Regulation Now Exist?.....1
2. What Data Must Be Protected?.....1
3. Does GDPR Apply to Organisations Outside the EU?.....2
4. What are the GDPR Penalties for Non-Compliance?.....3
5. Will Your Organisation be Ready in Time for GDPR?.....4
6. Controller or Processor, How Do You Become GDPR Compliant?.....5
   6.1. Data Controller.....5
   6.2. Data Processor.....5
7. How Paladion Can Help You Achieve GDPR Compliance.....7
   7.1. Paladion's High Speed Approach for GDPR Implementation.....8
   7.2. Paladion Service for GDPR Compliance Monitoring and Ongoing Maintenance.....12
8. Adherence to Code of Conduct and Certification.....13
9. Contact.....13
   About Paladion.....

1. Why Does the EU General Data Protection Regulation Now Exist?

Today's organisations collect, analyse, and use the personal information of individuals, their family information, social media profiles, images and much more. Administrations, employers, and commercial enterprises are all responsible for the safe, confidential, appropriate handling of such personal data. Without adequate data security controls, personal privacy could be breached leading to prejudice suffered by individuals, loss of customer trust, and damage to the reputation and business of enterprises and organisations.

The European Union General Data Protection Regulation (EU GDPR) has been defined to give EU citizens control over their personal data and simplify the regulatory framework for international businesses and organisations to operate in the EU. It replaces the Directive 95/46/EC of 1995.



GDPR aims to unify the data protection laws of the different EU member countries for a common approach to protect the data of EU citizens. It can be considered as the most comprehensive data protection law ever defined, with penalties for non-compliance of up to 4% of global annual revenue for an organisation.

GDPR is in effect now and enforcement of the regulation will begin with a year. Organisations working with data belonging to EU citizens must comply with GDPR before 25 May 2018.

GDPR can reduce compliance effort for organisations through its harmonisation of data protection regulations across the 28 EU member states. On the other hand, it may require additional compliance effort through the introduction of new rights for individuals and rules for mandatory breach notification.

2. What Data Must Be Protected?

Any information that can be used directly or indirectly to identify an individual constitutes personal data and must be protected, according to GDPR. The table below gives examples.

General Information	Organisational Information	Special Categories of Data
Name and Gender	Personal data collected for the purpose of recruitment	Racial or ethnic origin
Identification Number	Government-issued staff id numbers	Political opinions
Location data	Salary and payroll information	Religious or philosophical beliefs
Date of birth	Performance evaluation results	Trade union membership
Data pertaining to the physical, psychological, genetic, mental, cultural, economic or social identify of an individual	Performance evaluation results	Trade union membership
Online identifiers e.g. IP addresses, cookies	Benefits related to employment	Biometric data
Medical records and health information		

3. Does GDPR Apply to Organisations Outside the EU?

Regardless of the geographic location, GDPR applies to all organisations that collect, process, store, and transmit the personal data of, or monitor the behaviour of EU citizens (also referred to as data subjects).

4. What are the GDPR Penalties for Non-Compliance?

GDPR fines for non-compliance can be significant. A data subject who has suffered material or non-material damage owing to the infringement of GDPR has the right to receive compensation from the data controller or data processor.

GDPR Terminology

- Data subject - individual whose personal data is collected or processed
- Data controller - collects personal data
- Data processor - processes personal data on behalf of the controller
- Supervisory authority - national data protection authority that enforces the GDPR and responds to complaints from data subjects

In addition, the GDPR supervisory authority can impose administrative fines:

- Non-compliance with obligations as a data controller or a data processor can result in a fine of up to 10 million euros or 2% of annual global turnover (whichever is higher).
- Infringement of the principles of processing and violation of the rights of a data subject can result in a fine of up to 20 million euros or 4% of annual global turnover (whichever is higher).

The levels of fines imposed are based on:

- The nature, gravity, and duration of the infringement
- The intentional or negligent character of infringement
- The action taken by the controller or processor to mitigate the damage suffered by data subjects
- The degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them
- Any relevant previous infringements by the controller or processor
- Compliance with approved codes of conduct or approved certification mechanisms

5. Will Your Organisation be Ready in Time for GDPR?

The first step towards readiness is to assess your current situation. Key questions to be asked include the ones in the table below.

Scope of Activity	Data Breach Notification	Need for Data Protection Officers
Does your organisation collect or process the personal data of EU citizens (as an employer, as a commercial enterprise, or in any other way)?	Is your organisation set up to notify a data breach to a supervisory authority within 72 hours?	Does your organisation engage in extensive and systematic monitoring of personal data or process high volumes of personal data?
Data Protection Impact Assessment	**Demonstrating Lawful Processing and Consent**	**Personal Data Protection**
Has your organization identified the types of processing that are likely to result in high risk for the rights and freedom of individuals and is there a plan to mitigate the risk?	Does your organization maintain clear records of the consent given by data subjects prior to processing their data?	Can your organization demonstrate adequate technical and organisational measures to ensure security of personal data?
Privacy by Design and Default	**Rights of Data Subjects**	**Proof of compliance**
Are data protection and privacy measures designed into your organisation's processes and systems, and set to minimum compliance levels or higher by default?	Is your organisation set up to comply with the new GDPR "right tobe forgotten", "right to data portability", and "right to object to profiling"?	Does your organisation have a compliance management programme and can it prove that it meets GDPR requirements?

6. Controller or Processor, How Do You Become GDPR Compliant?

6.1. Data Controller

Your organisation is a **controller** if it decides the 'why' and the 'how' of a data processing activity. In other words, an organisation is a controller if

- It collects personal data and determines the purposes for which data is collected
- It decides which items of personal data to collect, i.e. the content of the data
- It decides the purpose or purposes for which the data will be used
- It decides which individual's data should be collected
- It decides whether to disclose the data, and if so, to whom
- It decides how long to retain the data or whether to make non-routine amendments to the data

6.2. Data Processor

Your organisation is a **processor**, if

- It follows the instruction of controller (client) regarding the processing to be done on the data that is collected on behalf of the controller
- It decides what IT systems or other methods are to be used to process personal data
- It decides the means used to retrieve personal data about individuals
- It decides how to store the personal data
- It decides the method for ensuring adherence to a retention schedule

NB: An organisation may be both a controller and a processor at the same time. For example, a processor can have its own data controller responsibilities for its employees' records.

Controllers

An organisation or entity that collects personal data and determines the purpose and manner in which processing of personal data is done.

Controllers can belong to almost any sector, including BFSI (banking, financial services, and insurance), telecom, retail, energy, government and public authorities, and all B2C companies and corporates that work with personal data belonging to EU nationals and residents.

Processors

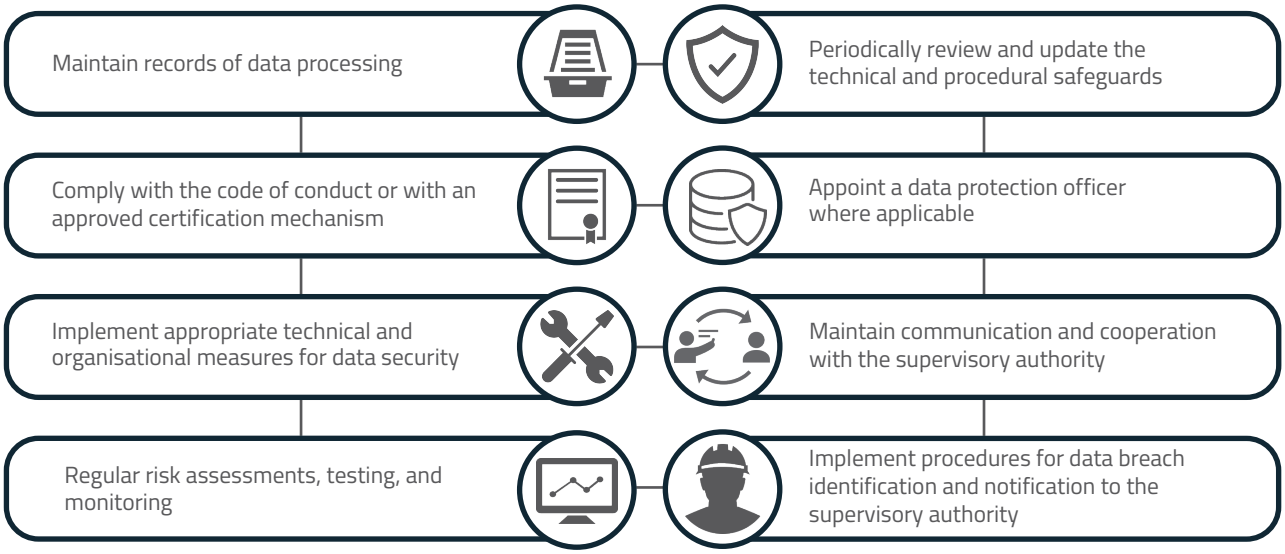
A person, agency or organisation that processes EU personal data on behalf of a controller. Processing includes collection, recording, storage, structuring, adaptation, alteration, consulting, use, dissemination, disclosure by transmission, alignment or combination, erasure or destruction.

Applies to cloud service providers, data aggregators, data processors, and outsourced companies processing data of EU citizens, regardless of whether the processing takes place in the European Union or not.

Controller Responsibilities	Processor Responsibilities
Conduct Data Protection Impact Assessment (DPIA) and risk mitigation	Ensure data is processed only on written instructions from controller
Safeguard the rights of data subjects	Ensure consent from controller when sub-contractors are used
Implement data protection principles – by design and by default	Ensure contracts with sub-processors are legally enforceable
Define and document responsibilities and liability when joint controllers are involved	Assist the controller in respecting the rights of data subjects
	Act only on documented consent from the controller when data is sent to other countries for processing
	Sign confidentiality agreements with personnel who work with EU data

Maintain stringent and legally binding contracts with third parties and data processors	Delete and return all personal data to the controller at the end of service Ensure security of data, including confidentiality, integrity, availability, access control and resilience Delete and return all personal data to the controller at the end of service

Common Controller and Processor Responsibilities

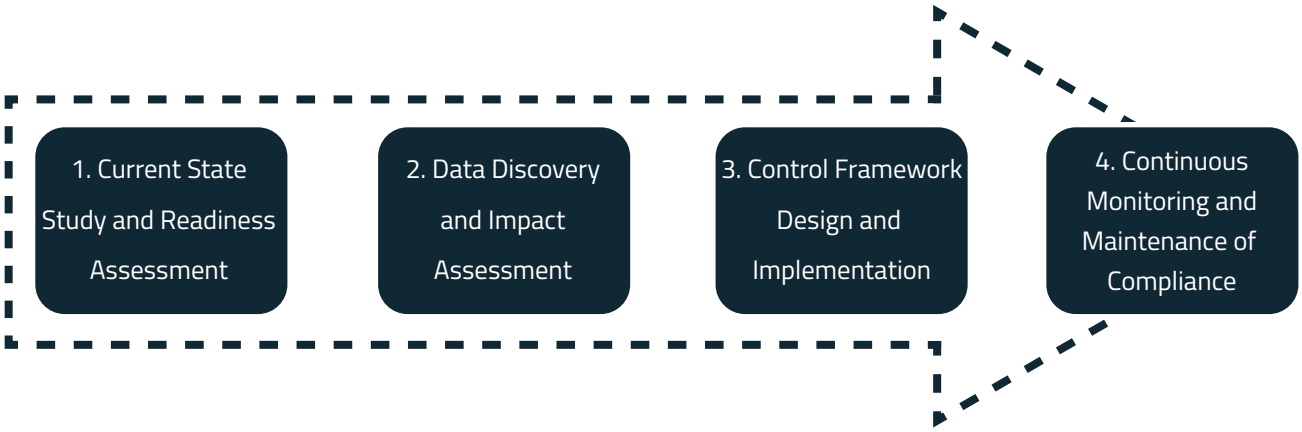


7. How Paladion Can Help You Achieve GDPR Compliance

GDPR has a significant impact on organisations in terms of financial investment and effort needed to comply with each of the stringent requirements of the articles of the regulation.

Paladion has designed a four-phase approach containing a total of seven steps and one continuing activity to:

- Help achieve compliance before the deadline of May 2018 and avoid any penalty
- Ensure regular monitoring and maintenance of compliance.



7.1. Paladion's High Speed Approach for GDPR Implementation

Phase 1 – Current State Study and Readiness Assessment

Step 1: GDPR readiness assessment

What We Do	How We Do It	Outcome
Identify the current maturity and readiness	Via workshops, interviews, meetings with key stakeholders, self-assessment questionnaires	Dashboards showing present compliance level and mapping of current state to ideal state

Phase 2 – Data Discovery and Impact Assessment

Step 2: Know where the data resides

What We Do	How We Do It	Outcome
Understand your organisation's business	Interviews and discussions with stakeholders from all departments that process personal data	A comprehensive data register containing categories of personal data along with their classification

What We Do	How We Do It	Outcome
Identify and scope personal data Cross-departmental data flow mapping Data classification	Data discovery using interviews and assessments	Data flow diagrams

Step 3 – Data Protection Impact Analysis (DPIA)

What We Do	How We Do It	Outcome
Understand the processing operations which are subject to DPIA requirements Evaluate the threats to the rights and freedom of data subjects Evaluate the technical and operational threats Analyse the effectiveness of existing safeguards (if any) Quantify the risk to personal data	Interviews and targeted questionnaires Review of control implementation evidence	Personal data risk register Risk mitigation plan

Phase 3 Control Framework Design and Implementation

Step 4 – GDPR framework development

What We Do	How We Do It	Outcome
Define roles and responsibilities for senior management and GDPR implementation team	Preparation of policies	Privacy policy
Ensure appointment of a data protection officer (if required)	Customisation of procedures and templates per the needs and current processes of the organisation	Information security policy
Define organisation level policies for data privacy and information security	Review and signoff required from respective stakeholders	Procedure documents
Develop procedures for collection, fair processing and use of personal data		Vendor management framework
Develop procedures for enforcing security controls		Breach notification plan
Design processes for protecting the rights of data subjects		Forms and templates for the records needed
Design vendor management program		
Ensure binding corporate rules in place prior to data transfer		

Step 5 – Control implementation planning

What We Do	How We Do It	Outcome
Detailed roadmap of controls to be implemented, priority and sequence of implementation and responsibility for implementation	Preparation of a control implementation roadmap based on risk mitigation priority	Control implementation plan Advisory support for implementation of technical and procedural controls

Step 6 – Security and GDPR awareness training

What We Do	How We Do It	Outcome
Security and data protection awareness training for personnel having regular access to personal data Training on the importance of GDPR and the need for compliance	Awareness training using either classroom training, recorded presentations or using Paladion's online training portal	Awareness training attendance sheet Evaluation quiz results

Step 7 – Internal audit and certification readiness

What We Do	How We Do It	Outcome
Internal audits Verification of compliance to the prescribed code of conduct	Onsite or remote assessment and evidence validation done by an independent Paladion consultant	Compliance internal audit report

7.2. Paladion Service for GDPR Compliance Monitoring and Ongoing Maintenance

At any point, a controller or a processor should be capable of demonstrating compliance to GDPR, when requested by the supervisory authority. This requires continuous monitoring and evaluation of the effectiveness of controls.

Paladion can provide subject matter advisory support as well as an activity calendar for the year consisting of the set of activities below for maintaining compliance and certification.

Phase 4 – Continuous Monitoring and Compliance Maintenance

- Periodic data impact assessment and risk mitigation
- Bi-annual audits and monitoring of adherence to approved code of conduct
- Third party (processor) contract vetting and assessment of security risks
- Advisory support for bi-annual testing of the business continuity plan and ability to recover from a disaster and restore data
- Continuous monitoring of threats to critical information
- Continuous monitoring of logs and identification of indicators of breach
- Bi-annual testing of the effectiveness of breach response program
- Bi-annual security assessment of the applications that process personal data and the underlying network and IT infrastructure
- Data protection training and security awareness to end users
- Advisory support during cloud migration
- Advisory support for ensuring controls during cross border data processing

NB: The periodicity of the activities above and the timeline for each activity may vary depending on the nature of the organisation and the level of controls that are currently in place.

8. Adherence to Code of Conduct and Certification

The GDPR code of conduct is approved and published by the member state's supervisory authority for controllers and processors to adhere to. The code of conduct applies to each of the topics mentioned in the regulation, and provides guidance for controllers and processors for implementing the topic concerned. Compliance with codes of conduct is subject to monitoring, which may be carried out by suitably qualified, accredited bodies.

Member states, supervisory authorities, and the European data protection board encourage the adoption of certification and data protection seals for demonstrating compliance with GDPR. The certification is voluntary and can be done by certification bodies who are accredited by the supervisory authority of the respective member state. A certificate is valid for three years and is then subject to renewal.

9. Contact

If you would like to discuss GDPR compliance or the activities described above further, please contact:

For Europe, Middle East and Africa

Mr. Austin Kuruvilla – Regional Delivery Manager

Phone: (+97) 15254 79377
Email: austin.kuruvilla@paladion.net

For India and South-East Asia

Mr. Amjad Khan – IT Security Consultant (Delivery Manager)

Phone: (+91) 98867 33258
Email: amjad.khan@paladion.net

For USA

Mr. Hariharan Ananthakrishnan - Sr. Practice Manager, Breach Resilience & Consulting Services

Phone: +1 (571) 524 0513
Email: hariharan.a@paladion.net

About Paladion

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by analyst firms such as Gartner, Forrester, and IDC, and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

For more information, please visit www.paladion.net

PALADION
HIGH SPEED CYBER DEFENSE

Head Office: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-703-956-9468.

Bangalore: +91-80-42543444, **Doha:** +974 33777866, **Dubai:** +971-4-2595526, **Kuala Lumpur:** +60-3-7660-4988, **London:** +44(0)2071487475, **Mumbai:** +9102233655151, **Riyadh:** +966(0)114725163, **Toronto:** +1-416-273-5004, **Virginia:** +1-703-8713934

sales@paladion.net | www.paladion.net