# GDRP Aspects Of Importance When Developing An Application Which Processes User Data

By Oisin Hickey

C00247185

# Contents

# Main Principles

Within any form of application or system development there is several different areas which require careful handling and inspection regarding the handling, processing, and storage of the data of any user data in that application or system. This can mainly be attributed to ensuring that the CIA (Confidentiality, Integrity, and Accessibility) of the data is always the utmost priority while it exists or interacts within the application or system and these principals are enforced in law via GDPR.

## Confidentiality

The organisation must secure their users sensitive, private information from unlawful access in today's ever evolving online environment.

It is necessary to be able to define and enforce access levels and security measures for information to protect confidentiality such as access control lists, volume and file encryption, and file permissions.

## Integrity

Data integrity protects data from unauthorized deletion or modification, and it assures that if an authorized individual makes a change that should not have been made, the damage can be undone. It means that a user from any point of view in the system can be sure that they are looking at accurate, genuine, and unaltered data which was collected legally and safely in full compliance with GDPR.

## Accountability

This refers to your data's actual availability. Authentication techniques and access channels must all function properly to protect information and ensure that it is available when it is requested by a user or administrator.

This can be enforced by a system including solutions targeting hardware failures, hardware upgrades, such as networking equipment used to manage several network connections to route around various network outages, or UPS systems for power outages.

## GDPR Regulations

GDPR regulations are the focus of this report, however the CIA triad forms the backbone of most of these regulations, so they are worth briefly mentioning. The General Data Protection Regulation (GDPR) is the world's most stringent privacy and security law. Even though it was designed and passed by the European Union (EU), it imposes duties on organizations anywhere in the world collect, store or process data about any user. On May 25, 2018, the regulation went into full effect. Those who break the GDPR's privacy and security regulations will face severe fines, with penalties ranging in the tens of millions of euros and these different penalties varying depending on the entity or organisations size.

The GDPR signals Europe's hard stance on data privacy and security at a time when more individuals are committing their personal data to cloud services, multi-national companies or unknown third-party entities and data breaches are becoming more common and more destructive.

# Within The Software Development Process

## Privacy by Default & Design

GDPR makes following the Privacy by Design and Privacy by Default principles mandatory.

Privacy by Design states that you should consider how to ensure the maximum level of data security from the start of the app development process rather than putting it off until later down the line when parts of the application may be set in stone.

Privacy by Default states "The strictest privacy settings should apply by default, without any manual input from the end-user ..... any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service."

## Process Only Necessary Data

Outlined in Article 23 this means your software or system should only ask for data that is required by law, necessary to perform services, or justified by your legitimate interest. In both the necessary and unnecessary case, you must explain why you are gathering specific data. Data can be voluntarily provided by the user, such as when they want to share it with other users or optional information such as home address or phone number on a marketing survey.

## Pre-Established Coding Standards

Everyone in your project should use a pre-established list of coding libraries, tools, and frameworks to avoid unauthorized or excessive data acquisition or loss and a list of authorized coding and testing standards, approaches, and tools for all aspects of the development process.

Requesting that developers disable hazardous or beta tools, especially in APIs and third-party libraries like jQuery for example, is important as well as regular code evaluations which should within their structure, an audit for privacy by design, as well as data mapping and data security are just a few practical ways that coding standards can be carried out.

## Informing users & authorities of data breaches

In the event of a data breach, GDPR imposes rigorous deadlines for alerting app users as well as the appropriate authorities. The disclosure of such material to the data protection authorities must occur within 72 hours of its discovery.

To avoid potentially dangerous delays, consider investing in technology and systems that alert you when such dangers arise automatically e.g., Jetpack security system. It's also critical to have a plan in place for dealing with a data breach within your app, the best and quickest manner to tell your users and how to implement systems to ensure that functionality continues as normal in the form of a Disaster Recovery Plan.

## Exercise the right to be forgotten

The right to erasure, sometimes known as the "right to be forgotten," is highlighted in Article 17 of the GDPR. If a user requests that their data be deleted from your database and at least one of the conditions in Article 17 of the GDPR is met, you must comply.

In this case, you must delete all personal information you have on them from the system. Furthermore, after a data retention period expires, the data should be destroyed or anonymized —

either automatically or by user action. This entails providing a mechanism for users to remove their accounts, as well as any data they no longer require for certain valid objectives.

### Allowing A User To Consent

One of the most important GDPR regulations is to obtain user consent each time personal data is collected, used, or transferred. This permission must be given before you begin collecting data and if you lack a solid legal basis for processing their personal data, you must ask them to consent to the processing of their data. If you just process data necessary to deliver services to the user, you don't need to ask permission again mainly because a user can find it cumbersome to use a system which too heavily enforces GDPR principals

### Include A Privacy Policy

Include a clear Privacy policy in your application that explains the rights that GDPR gives users, such as the ability to withdraw consent at any time and file a complaint with the President of the Personal Data Protection Office. You often find these policies on various websites especially sites like Facebook or YouTube.

You must state:

- You state whether or if the program profiles its users and whether data is shared with other entities, including third nations.

- In addition, you must indicate what type of data the program will analyse and for how long.

This Privacy Policy must be publicly accessible to anyone who wishes to view it.

### Implement Encryption & Decryption For Data Security

Article 32 of GDPR states software developers must ensure the ongoing confidentiality, integrity, availability (the CIA triad mentioned in main principals) and resilience of the data collected, processed or transmitted by their application. A famous case that comes to mind is that of Sony Inc. when their PlayStation servers were breached, and their entirely unencrypted database was leaked to the public and various nefarious hacker groups

All backups should also be encrypted in full in case the backups or their storage hardware is compromised or stolen.

## Conclusion

From researching, reading, and attempting to implement GDPR it’s clear that the points mentioned above are of the utmost importance regarding GDPR in the software development lifecycle. From various past cases where these criteria weren’t met to common modern-day scenarios, GDPR enforces the privacy, security and safety of people’s data and lives. It does appear that GDPR, although existing at every step of a project and it’s existence is very important on a foundational level, at the very bedrock of a systems structure and architecture.

## References

https://www.forcepoint.com/cyber-edu/cia-triad

https://gdpr-info.eu/art-5-gdpr/