malt

Compliance Kit Data Protection & Security

APRIL 2024

Introduction

There's a lot of talk about the protection of personal data, especially since May 25, 2018 when obligations were established to protection personal data (GDPR - General Data Protection Regulation). But what does this mean for you and your work?

GDPR requirements also apply to freelancers. If you understand how they apply to you and how to implement them, then adhering to the requirements can be a real opportunity for you to stand out.

Table of contents

Chapter 1

Applicable regulation

& main principles of data protection

Chapter 2

Ensure compliance

Measures to put in place to protect your information system and ensure compliance

Chapter 3

Working on projects via Malt

Data protection and security obligations when working on projects via Malt

Chapter 4

Remote work: best practises

Guidelines and best practises to follow

BONUS

Useful available resources

Chapter 1

Applicable regulation

& Main principles of data protection

Regulations governing personal data processing are outlined in the GDPR, adopted by all European countries and enforced as of May 25, 2018.

Objectives

Enhance individuals' control and rights over their information

Enforce data accountability

Streamline cooperation between EU actors

Who is concerned?

All organizations

- **established in the EU**

OR

- **whose activities target EU residents**

Link full text

What is **personal data?**

Personal data is "all information relating to a physical or identifiable person".

Some examples:

First and last name · Cookies · IP address

Photos and videos · Client contact details

Income · Prospect contact info

Email and postal address

What is processing of personal data?

“Processing” means any operation or set of operations performed upon personal data.

- Collection
- Storing
- Transmission
- Modification
- Consultation
- Use
- Communication
- Deletion

Main principles of data protection

Purpose

Data about individuals cannot be collected, or processed without a precise, legal and legitimate purpose.

Proportionality & Accuracy

Processed data must be pertinent, accurate, and strictly necessary to the purpose.

Limited storage retention

A defined storage retention must be fixed based on the category of data processed and the purpose of the processing.

Security & Confidentiality

Only authorised persons can have access to personal data which is confidential and must be secured.

Individual's rights

Each individual has various rights when it comes to the processing of their personal data, including; the right of deletion, objection, access, limitation, portability, as well as the right to withdraw consent, complain to the authorities, and control the fate of their data.

Understanding your role in processing personal data is crucial

The **Data Controller** determines the purpose and the means of the processing.

The **Data Processor** processes personal data on behalf of, and following the instructions of, the Data Controller.

As a freelancer working on a project, your role is that of a Data Processor, who is following the instructions of the customer acting as the Data Controller.

Both Data Controller and Data Processor must comply with the GDPR.

Data Processor rules:

- Ensure the protection and confidentiality of personal data provided by and processed on behalf of the Data Controller
- Subprocessing is not authorised without the express consent of the Data Controller
- Restrict personal data usage only to the purpose as defined by the Data Controller
- Assist and cooperate with the Data Controller

As defined in the GDPR, you are a Data Processor who must uphold these obligations when processing client personal data.

Guidelines from the European Data Protection Board

Chapter 2

Ensure compliance

Measures to put in place to protect your information system and ensure compliance

Steps to reach compliance

Create **a register** of the data you process by identifying the purpose, the type of processing, who has access to the data, and the data retention period.

Respect the rights of individuals: be aware of the rights of individuals when you process personal data.

Sort the data: only process data necessary to working on the project, and limit access and retention. Identify sensitive data: "Do I have the right to process this data?".

Secure the data: risk-level approach based on data sensitivity; use strong password, conduct backups, update your antivirus software, encrypt data when necessary.

Measures for a healthy information system

Install a firewall

Keep the information system up to date: do regular software and tool updates

Set up an automatic session time-out to lock if not used after a certain duration

Regular backups

Limit mobile device (USB keys, external hard drives) connections only to the essential

Deactivate "autorun" on removable devices

Guidelines for a healthy information system - Source ANSSI

Chapter 3

Working on projects via Malt

Data protection and security obligations when working on projects via Malt

As a freelancer:

You work for and under the instruction (as defined by the GDPR) of the client, who is the Data Controller;

You may be required to process personal data in the course of carrying out the project;

You must ensure the protection and security of the personal data you process.

Typical instructions from customers

Process data only according to the purpose defined by the client

Keep a register up to date and ready in case of audit

Only retain data for the duration of the project, and delete or return the data once the project is validated

Take all the necessary precautions to ensure the security of the data

Provide help and answers should an individual request to exercise their rights or should a competent authority inspect

Help conduct a privacy impact assessment

Inform the customer in case of data breach

You must inform the customer if the data that’s been entrusted to you has been accidentally or illicitly destroyed, lost, altered, leaked to non-authorized people or organizations; stored or processed by another manner than intended or accessed by an unauthorised person.

You only have a little time: 48 to 72 hours on average.
If applicable, you should verify the notification conditions in the contract you may have signed.

Notifications must contain at least the following information:

- Type of violation
- Categories and approximate number of people affected by the breach and of personal data records concerned
- A point of contact who can supply additional information
- Probable consequences of the breach
- Measures taken to remediate the data breach and measures to mitigate any negative consequences.

Guidelines - European Data Protection Board

The “fate of the data” once the project is completed

The reflexes to have:

- Delete data to which the customer gave you access for the purpose of the project, and any possible copies (except legal obligations)
- Provide certification of destruction if the customer requests it;
- Return material lent by the customer for the duration of the project
- Anonymise data not subject to intellectual property

Chapter 4

Remote work: best practises

Guidelines and best practises

Inherent risks of remote work

When you work off site *(at home, on public transportation, in a co-working space)*, generally your physical protection resources are not the same as on an organization's premises .

In all these workplaces not controlled by the customer the following risks are exacerbated:

- Loss or theft of material
- Unauthorised access to the organization information system
- Compromise of data contained in stolen, lost or borrowed material
- Loss of confidentiality or integrity

The questions to ask yourself first:

The project: Do the project's conditions let you to work remotely?

Authorisation: Work outside the entity's premises may be forbidden due to high-level data sensitivity or activity; regulatory constraints, industry-specific restrictions.

Settings: The customer may impose certain settings to work remotely.

Best practices

Confidentiality: use privacy filter on screens when traveling

Absence: keep your devices and files with you at all times

Passwords: protect devices with different strong and complex passwords

Locking: shorten inactivity timeout to automatically lock the user session

WIFI: do not connect to public wifi, prefer sharing your connection instead

Peripherals: do not connect your equipment to workstations or devices that are not trusted.

BONUS

Available resources

Resources provided by Malt

We recommend you carefully read this **Compliance Kit** and the **Security Checklist**. They outline all the security requirements to follow while working on your project.

Data protection authorities contact

🇧🇪 Autorité de la protection des données / Gegevens Beschermings Autoriteit (link)

🇩🇪 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (link)

🇪🇸 Agencia Española de Protección de Datos - APPD (link)

🇳🇱 Autoriteit Persoonsgegevens (link)

🇬🇧 Information Commissioner’s Office - ICO (link)

🇨🇭 Federal Data Protection and Information Commissioner (link)

External resources

Training

You are invited to learn about data and security protection. We encourage you to follow these mainly online courses to learn about the basics of data protection and computer system security.

For guidelines from the European Data Protection Board:
https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_fr

Security guidelines from the French Data protection authority (CNIL):
https://www.cnil.fr/sites/cnil/files/atoms/files/guide_security-personal-data_en.pdf