

Your organisation's role:

- **Data Controller: You determine why data is processed.**

Your data

- Your company has a list of all types of personal information it holds, the source of that information, who you share it with, what you do with it and how long you will keep it?

This is a list of the actual types (columns) of information being held (eg Name, social security nr, address,..). For each type, a source should be documented, the parties this information is shared with, the purpose of the information and the duration for which the company will keep this information.

- **GDPR Article 30 – Records of processing activities**
- **GDPR Data Map Template**

- Your company has a list of places where it keeps personal information and the ways data flows between them?

This could be a list of databases (eg Mysql), but it could also include offline datastores (paper).

- **GDPR Article 30 – Records of processing activities**

- Your company has a publicly accessible privacy policy that outlines all processes related to personal data?

You should include information about all processes related to the handling of personal information. This document should include (or have links to) the types of personal information the company holds, and where it holds them. Your privacy policy should include a lawful basis to explain why the company needs to process personal information. It should contain a reason for data processing, eg the fulfillment of a contract.

- **GDPR Article 30 – Records of processing activities**
- **GDPR Article 6 – Lawfulness of processing**

Accountability & management

- Your company has appointed a Data Protection Officer (DPO)?

A DPO is only required in three scenarios: (1) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (2) the core activities of the business consist of processing operations which, by virtue of their nature, scope, and/or purposes, require regular and systematic monitoring of data subjects on a large scale, or (3) the core activities of the business consist of processing on a large scale special categories of data (sensitive data) pursuant to Article 9 and personal data relating to criminal convictions or offenses pursuant to Article 10. If a DPO is required, the DPO should have knowledge of GDPR guidelines as well as knowledge about the internal processes that involve personal information.

- **GDPR Article 37 – Designation of the data protection officer**
-

- Create awareness among decision makers about GDPR guidelines

Make sure key people and decision makers have up-to-date knowledge about the data protection legislation.

- **GDPR Article 25 – Data protection by design and by default**
-

- Make sure your technical security is up to date.

Use the Back End Security checklist we provide as a starting point below.

- **Security System checklist**
 - **GDPR Article 25 – Data protection by design and by default**
-

-
- Train staff to be aware of data protection

A lot of security vulnerabilities involve cooperation of an unwitting person with access to internal systems. Make sure your employees are aware of these risks.

- **GDPR Article 25 – Data protection by design and by default**
-

- You have a list of sub-processors and your privacy policy mentions your use of this sub-processor?

You should inform your users or employees of the use of any sub-processor. They should consent by accepting your privacy policy.

- **GDPR Article 28 – Processor**
 - **GDPR Article 33 – Notification of a personal data breach to the supervisory authority**
 - **GDPR Article 34 – Communication of a personal data breach to the data subject**
-

- There must be a contract in place with any data processors that you share data with!

The contract should contain explicit instructions for the storage or processing of data by the processor. The contract should set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. For example, this could include a contract with your hosting provider. The same contract requirements apply when a processor engages a sub-processor to assist it in fulfilling processing activities on behalf of the controller

- **GDPR Article 28 – Processor**
- **GDPR Article 29 – Processing under the authority of the controller or processor**

New rights

- Your users can easily request access to their personal information

If you do not already have a process defined for this, we've made an easy online form below. Your users can easily update their own personal information to keep it accurate.

- **GDPR Article 16 – Right to rectification**
-

- You automatically delete data that your business no longer has any use for?

You should automate deletion of data you no longer need. For example, you should automatically delete data for users whose contracts have not been renewed.

- **GDPR Article 5 – Principles relating to processing of personal data**
-

- Your users must easily request deletion of their personal data

- **GDPR Article 17 – Right to erasure ('right to be forgotten')**
-

- Your users can easily request that you stop processing their data

- **GDPR Article 18 – Right to restriction of processing**
-

- Your users can easily request that their data be delivered to themselves or a 3rd party

- **GDPR Article 20 – Right to data portability**

- Your users can easily object to profiling or automated decision making that could impact them

This is only applicable if your company does profiling or any other automated decision making. If you do not already have a process defined for this, we've made an easy online form below.

- **Article 22 – Automated individual decision-making, including profiling**
-

Consent

- Where processing is based on consent, such consent must be freely given, specific, informed, and revocable

If your website collects personal information in some way, you should have an easily visible link to your privacy policy and confirm that the user accepts your terms and conditions. Consent requires an affirmative action, so pre-ticked boxes are not permitted.

- **GDPR Article 7 – Conditions for consent**
-

- Your privacy policy should be written in clear and understandable terms

It should be written in clear and simple terms and not conceal its intent in any way. Failing to do so could void the agreement entirely. When providing services to children, the privacy policy should be easy enough for them to understand.

- **Watchdog service for terms of service: Terms of Service; Didn't Read**
 - **GDPR Article 7.2 – Conditions for consent**
-

- It should be as easy for your users to withdraw consent as it was to give it in the first place.

- **GDPR Article 7.3 – Conditions for consent**

- You regularly review policies for changes, effectiveness, changes in handling of data and changes to the state of affairs of other countries your data flows to?

You should follow up on best practices and changes to the policies in your local environment

- **GDPR Article 25 – Data protection by design and by default**



○ Restrict internal services by IP addresses

SERIES A / POST-SERIES A

Everything non-public should only be accessible through a bounce host (e.g. no direct access to databases).

○ Centralize and archive your log data

SERIES A / POST-SERIES A

Logs are necessary to trace what happened after an incident, find where the attacker came from, and possible even who they are. Many solutions exist to gather your logs. You need to take care about that the system time configured on each of your machines is in sync so that you can easily cross-correlate logs.

○ Protect your applications from DDoS attacks

SERIES A / POST-SERIES A

A Distributed Denial-of-Service Attack (DDoS) can have devastating consequences on businesses. Basic DDoS protections can easily be integrated with a CDN such as:

○ Check for unusual patterns in your metrics

SERIES A / POST-SERIES A

Takeovers will often be used to steal your data or setup your servers to be used as bouncers. These can be detected by watching for unusual patterns in metrics such as network bandwidth, CPU and memory consumption, and disk usage.

○ Monitor your dependencies

SEED / SERIES A / POST-SERIES A

Applications are built using dozens of third party libraries. A single flaw in any of these libraries may put your entire application at risk. Some tools allow you to monitor your dependencies against vulnerabilities:

○ Use a real-time protection service

SERIES A / POST-SERIES A

Provide tools to protect web applications from attacks at runtime. The protection logic is inserted into applications. They protect against all major vulnerabilities (SQL injections, XSS attacks, account takeovers, code injections, etc...) without false positives.