GDPR COMPLIANCE REQUIREMENTS LIST

GDPR COMPLIANCE CHECKLIST FOR DATA CONTROLLERS

This is a checklist of works and guidelines in order to meet GDPR Compliance as a Data Controller in your Organization.
This list is far from exhaustive, and
depends on critical assets your handle.

CULTURETEK.ORG

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 visble 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 it's 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 practies and changes to the policies in your local environment

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

.

GDPR Data Map

Source How was this data collected? · Contact Form · External Organisation	Personal Data What data are you collecting? · Email Address · IP Address · Ethnic Origin · Phone Number	Reason Why are you collecting this data? · Marketing · CRM · Processing/ Analytics	Handling Explain how you will store the data, how it will be processed and who has access to it.	Disposal When is this data disposed? · Upon Request · After 6 Months	

TECHNICAL REQUIREMENTS LIST

BACK-END SECURITY CHECKLIST FOR GDPR DATA CONTROLLER

This is a basic checklist of works and guidelines in order to harden your information System Security and facilitate your GDPR Compliance as a Data Controller.
This list is far from exhaustive, and depends on critical assets your handle.

CULTURETEK.ORG

YOUR COMPANY /1

- **Ensure your domain names are secured** — SEED / SERIES A / POST-SERIES A

  Check if your Domain names should be renewed regularly. If you have bought one from a third party you should also make sure that the authoritative configured name server is your own.

- **Secure all critical services** — SEED / SERIES A / POST-SERIES A

  Many companies rely on Google Apps, Slack, Wordpress… These services all have defaults that should be improved to increase the security level. All these services should be updated on a regular basis when relevant.

- **Wifi Check** — SEED / SERIES A / POST-SERIES A

  Sharing Wifi networks with guests or neighbors may give them the opportunity to gather information on your network, and allow them to access resources protected by source IP. Use an isolated and dedicated guest Wifi network. Set up a calendar reminder to change the password every two months, since this password is shared.

- **Guidelines care of your non tech employees** — SERIES A / POST-SERIES A

  Non tech employees are less used to technical tricks and can be deceived more easily than others, opening the door to ransomware or confidentiality issues. They should be trained and empowered to be distrustful and to preserve the company's assets.

- **Security incident response plan** — POST-SERIES A

  Provide a security incident plan. This will allow whoever is in charge at the time of a breach to communicate accordingly about an incident and will allow the fastest response in technical / communication terms.

- **Guidelines for internal security policy** — POST-SERIES A

  Provide a short document stating the security requirements in your company and defining who is responsible and who is Concerned with all aspects of security.

YOUR EMPLOYEES /2

- **Provide security practices and guidelines** — SEED / SERIES A / POST-SERIES A

  Humans are often the weakest links in the chain of security. By explaining how an attacker could infiltrate your company, you will increase their awareness and thus minimize the chance of them falling for such a trap.

- **Enforcement of 2FA services** — SEED / SERIES A / POST-SERIES A

  Your employees should all use 2-factor authentication. It means that if their password gets stolen, the attacker cannot use it without the second factor. As a CTO your role is to make sure everyone complies with this rule.

- **Provide centralized password manager solution to ensure you only use strong passwords** — SEED / SERIES A / POST-SERIES A

  Using a complex and unique password for every website is great advice, but it can be very difficult to remember all of them. Password managers are a great way to manage these, since they will remember everything for you with a master password.

- **Onboarding / offboarding checklist** — SEED / SERIES A / POST-SERIES

  Provide a checklist of all the steps you need to enforce when an employee, contractor, intern, etc… joins your company. A similar list can also be used when the someone is leaving your team.

- **Provide a centralized account management** — SERIES A / POST-SERIES A

  A centralized place with all user authorizations is the best way not to forget anything once you need to update a user profile (e.g. if an internship came to its end). It is also great place to define standard account creation you need for a given user.

YOUR APPS /3

- **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 by 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.