# 

# Free checklist: Conducting a data protection audit

This is a free template or checklist from activeMind.legal for data protection and data security purposes. The latest version can be found [here](https://www.activemind.legal/downloads/). This document can be tailored to the needs of your company, saved and printed. Please note that activeMind.legal accepts no liability for errors.

If you have any questions or issues, please do not hesitate to contact us.

Your activeMind.legal team

Phone: +49 (0)89 / 91 92 94 – 900

E-Mail: info@activemind.legal

Web: https://www.activemind.legal

Checklist: Conducting a data protection audit

# Data protection management system

The first step is to review the general obligations that the GDPR imposes on a controller:

## Data protection management

* Do you have data protection guidelines, a data protection handbook or a data protection policy? These should define your organisation’s data protection principles.
* Are data deletion periods defined and implemented?
* Is IT use within your organisation defined?
* Is there a procedure for involving external parties in compliance with data protection law?

## Data protection responsibilities

* Did you appoint a data protection officer? Is his/her appointment documented?
* Have you provided the contact details of your DPO to the ICO and published them both within and outside of your organisation?
* Have further tasks and roles been assigned to other employees for the purpose of data protection?

## Personal data protection breaches (Art. 33 GDPR)

* Are there procedures in place to deal with a data breach and has responsibility for managing breaches been allocated to a dedicated person or team? As data protection breaches must be reported to the responsible supervisory authority within 72 hours, it is essential that defined procedures are in place (e.g. a personal data breach policy).

## Data subject requests (Art. 15-21 GDPR)

* Are there procedures in place to deal with requests from data subjects (e.g. a data subject’s rights policy) and has responsibility for dealing with requests been allocated? As a rule, such requests must be answered immediately, but within a maximum of one month. In exceptional cases, the deadline can be extended for up to three months.

## Processing on behalf of a controller (Art. 28 GDPR)

* Have all the necessary data processing agreements been checked and signed by both parties? Such agreements are required if another company (including those within the group) processes data on behalf of a data controller.

## Records of processing activities (Art. 30 GDPR)

* Is a detailed record of processing activities kept? Art. 30 GDPR defines what information a record should include. This information must be provided for each data processing activity. Examples can be found below under point 3.
* Does the record serve as a supporting document for the authorities? According to the GDPR, the purpose of the records is to provide information to supervisory authorities. It should therefore be possible to understand each record without further information.

## Data protection impact assessment (Art. 35 GDPR)

* Have the potential risks of each data processing activity been assessed?
* If there is a high risk for a data subject, has a data protection impact assessment been carried out?

## Obligation to provide information (Art. 13 GDPR)

* Have templates been created to fulfil the obligation to provide information to data subjects (see: customer and employee privacy notices)? Data subjects have the right to be informed about the use of their data, irrespective of the source of the data.
* Are obligations to provide information fulfilled where data is collected directly from data subjects?
* Are the information obligations fulfilled where data is received from third parties?
* Does your website include a privacy policy?

## Staff training

* Are employees trained regularly on data protection and does the training adequately cover the processing activities carried out? If not, employers are liable for errors made by his/her employees.

## Non-disclosure agreements

* Are employees and external service providers required to comply with data protection regulations before dealing with personal data?

# Information Security

Data protection requires companies to have adequate information security measures in place. Data can only be processed securely if appropriate technical and organisational measures are implemented. Examples of how to review individual technical and organizational measures (TOM) can be found in our checklist on how to review potential service providers.

## Pseudonymisation and encryption (Art. 32(1)a GDPR)

* Is data pseudonymised wherever possible? Pseudonymisation means that data can no longer be assigned to a specific data subject without the inclusion of additional information, and that this additional information is stored separately and is subject to appropriate technical and organisational measures. Please note: Unlike anonymised data, this data is subject to the regulations of the GDPR.
* Which devices are encrypted in your company?
* What type of encryption is used?

## Confidentiality (Art. 32(1) b GDPR)

* Physical access control: What measures are used to secure your company's premises?
* Electronic access control: How are data processing systems protected against access and unauthorised use?
* Internal access control: How do you prevent personal data from being processed by unauthorised persons?
* Isolation control: How do you ensure that data collected for different purposes is processed separately?

## Integrity (Art. 32(1) b GDPR)

* Data transfer control: How is data transferred (digitally and physically) to customers, clients or third parties and how is it protected?
* Data entry control: Is the management and maintenance of data monitored and documented?

## Availability and resilience (Art. 32(1) b GDPR)

* Availability control: Are systems set up to protect data against accidental destruction or loss?
* Resilience control: Can systems cope with risk-related changes and are they able to tolerate and compensate for disruptions?

## Rapid recovery (Art. 32 (1) c GDPR)

* Is there a procedure in place to restore the availability of personal data after a physical or technical incident?

## Procedures for regular review, assessment and evaluation (Art. 32 (1) d GDPR; Art. 25 (1) GDPR)

* Incident response procedure: Is there a procedure in place to prepare for security breaches and system failures and to identify, contain, remediate and recover from them?
* Privacy-friendly pre-ticked settings: Are the pre-ticked settings in data processing systems designed so that only data that is necessary for the specific processing purpose is processed. Is this data stored for as short a period as possible?
* Regular checks: Are technical and organisational measures regularly assessed to ensure they are effective?

# Processing activities

Each company’s data processing procedures should be assessed to determine whether they comply with the GDPR and the DPA. We are unable to provide specific examples as no two companies are the same and different companies experience different issues.

However, please find listed below examples of the most common data processing activities companies undertake/deal with:

## HR

* Job application procedures
* Personnel files

## Marketing

* Newsletters
* Web data analytics

## Sales

* CRM

## IT

* Backups
* E-mail processing

This list should be extended andtailored to company data processing activities.