# Free Template: Data Protection Policy in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018

**Explanatory notes to this template**

The template is not exhaustive and may not include all required elements. In addition, the template may contain elements that do not apply to individual companies. It is therefore always necessary for the person responsible to adapt and supplement the template accordingly. If necessary, you will find information on this in the comments.

**Usage rights for our free template**

This template is created and regularly updated by the specialists at activeMind.legal UK Ltd. The template cannot address all conceivable special cases. It cannot and should not replace legal advice on data protection or other legal advice.

All liability is excluded!

All rights to the template are reserved. You are permitted and free to use the text provided by us for your own (including commercial) purposes.

We offer neither support nor advice for this free service and kindly ask you to refrain from such requests.

If you publish the template or parts of it, the reference and link to htttps://www.activemind.uk must be left in the text.

# Data Protection Policy

## Goal of the data protection policy

The goal of the data protection policy is to depict regulatory data protection aspects in one summarising document. It can also be used as the basis for data protection inspections, e.g. by the customer within the scope of a data processing agreement. This is not only to ensure compliance with the United Kingdom General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018 but also to provide proof of compliance.

## Preamble

Brief description of the company and motivation to comply with data protection.

## Security policy and responsibilities in the company

* For a company, in addition to existing corporate objectives, the highest data protection goals are to be defined and documented. Data protection goals are based on data protection principles and must be individually modified for every company.
* Determination of roles and responsibilities (e.g. representatives of the company, operational data protection officers, coordinators or data protection team and operational managers)
* Commitment to continuous improvement of a data protection management system
* Training, sensitisation and obligation of the employees

## Legal framework in the company

* Industry-specific legal or conduct regulations for handling personal data
* Requirements of internal and external parties
* Applicable laws, possibly with special local regulations

## Documentation

* Conducted internal and external inspections
* Data protection need: determination of protection need with regard to confidentiality, integrity and availability.

## Existing technical and organisational measures (TOM)

Appropriate technical and organisational measures that must be implemented and substantiated, taking into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs.

The description of the implemented TOM can, for example, be based on Art. 32 of the UK GDPR:

* Pseudonymisation (Art. 32 (1) (a) of the UK GDPR; Art. 25 (1) of the UK GDPR)
* Encryption (Art. 32 (1) (a) of the UK GDPR)
* Confidentiality (Art. 32 (1) (b) of the UK GDPR)
	+ Access Control
	+ Entry Control
	+ Authorisation Control
	+ Separation Control
* Integrity (Art. 32 (1) (b) of the UK GDPR)
	+ Transfer Control
	+ Input Control
* Availability and Resilience (Art. 32 (1) (b) of the UK GDPR)
	+ Availability Control
	+ Resilience Control
* Recoverability (Art. 32 (1) (c) of the UK GDPR)
* Procedures for Regular Review, Assessment and Evaluation (Art. 32 (1) (d) of the UK GDPR; Art. 25 (1) of the UK GDPR)
	+ Data-Protection-Management-System
	+ Incident-Response-Management-System
	+ Data Protection By Design and Default
	+ Order Control

*This document was created with the help of* [*www.activemind.uk*](http://www.activemind.uk) *– the experts for data protection and information security.*