

A.18 Data processing policy - Visma Enterprise A/S

Classification: **Internal**

Applicability

This policy is applicable to the overall organisation of Visma Enterprise A/S including:

- Employees
 - External personnel (i.e. consultant) with frequent access to Visma Enterprise A/S's IT systems
-

1. Purpose

The purpose of this Data processing policy is to define and communicate the requirements to all Visma Enterprise A/S employees, consultants or affiliates when acting as a data processor.

2. Policy

When Visma Enterprise A/S acts as a Data Processor, the processing can only be conducted according to the instructions given by the Data Controller.

The instructions must be established in a Data Processing Agreement. No processing of the Data Controllers data can take place unless a Data Processing Agreement is established.

The Data Processing Agreement accepted by the Data Controller must be retained and any [changes and/or addendums must be documented](#).

A [record of processing activities](#) under Visma Enterprise A/S's responsibility and a [list or overview of data processing assets](#) must be maintained.

Requirements to Visma Enterprise A/S are:

- **Confidentiality**

The number of Visma employees with access to the Data Controllers data must be limited to those with work related purposes and who have committed themselves to confidentiality.

The list of Visma employees with access to the Data Controllers data must be reviewed periodically.

- **Security**

Visma enterprise A/S will implement appropriate measures to secure the Data Controllers Data.

All security measures are described in the [security policies](#) and [associated procedures](#).

- **Sub-processors**

Visma Enterprise A/S can only use sub-processors accepted by the Data Controllers.

An updated list of accepted sub-processors is maintained in Appendix B of the Data Processing Agreement (current version is located in the [appendix overview](#) at Visma Community)

Using any other sub-processors for the processing of the Data Controllers data is not allowed.

- **Transfer of data**

The Data Controllers data can only be processed within the EU/EEA.

Transfer to and processing of data in secure third countries (approved by the EU Commission) can only take place if accepted by the Data Controller.

- **[Assistance](#)**

Visma Enterprise A/S must be able to assist the Data Controller in the fulfilment of the Data Controllers obligations to respond to requests for exercising the data subject's rights.

A [procedure](#) describing how, is established and maintained.

- **Notification**

Visma Enterprise A/S must notify the Data Controller in case of personal data breach involving the Data Controller's data. The notification must take place within 24 hours after we get aware of the incident.

A [procedure](#) describing how Visma Enterprise A/S will notify the Data Controller in case of a personal data breach is established and maintained.

- **Data retention and deletion**

Visma Enterprise A/S will only process data on behalf of the Data Controller as long as a valid agreement (including a Data Processing Agreement) is present.

A [policy on data retention and deletion](#) is established and maintained.

This policy is supported by [Visma Group Policies & Statements](#)

3. Enforcement

Responsibility

All employees and external consultants shall be aware of and responsible for data processing.

Every person involved in the processing of data on behalf of a Data Controller is expected to comply with this policy, both during and, where appropriate, after his or her employment in the company.

Non-compliance

Violations of this policy must be reported to the employee's manager, who is responsible for the further handling of the incident.

If an employee overrides its duties within information security, the manager may take the appropriate disciplinary actions, under the supervision of HR.

The responsible host will take immediate action towards non-Visma Enterprise A/S employees.

Exceptions to the policy

Exceptions to this policy can be granted according to [Visma Enterprise A/S's Exception Policy](#)

Review and approval

This information security policy is reviewed and approved at least yearly by the Information Security Board (ISB).

Lates review and approval by ISB: [August 11 2022](#)

Accountable: [Information Security Board](#)

Responsible: Data Protection Manager
