Contents

Chapter 1

GDPR Data Protection Handbook - Metadata

Document-ID: 0000
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: {{ meta.status }}
Classification: {{ meta.classification }}
Last Update: {{ meta.date }}

1.1 Handbook Information

Handbook Title: GDPR Data Protection Handbook
Organization: {{ meta.organization }}
Author: Andreas Huemmer [andreas.huemmer@adminsend.de]
Scope: {{ meta.scope }}
Valid From: {{ meta.valid_from }}
Next Review: {{ meta.next_review }}

1.2 Document Purpose

This handbook documents the organization's data protection measures and processes in accordance with the General Data Protection Regulation (GDPR - EU 2016/679). It describes the structure, processes, responsibilities, and procedures for ensuring the protection of personal data.

1.3 Scope

The Data Protection Management System applies to: - {{ meta.gdpr_scope }}

1.4 Normative References

- Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)
- National data protection laws and adaptations
- Relevant sector-specific data protection regulations

1.5 Change History

Version	Date	Author	Change
{{ meta.version }}	{{ meta.date }}	Andreas Huemmer [andreas.huemmer@adminsend.de]	Initial version

ewpage

Chapter 2

Scope and Application

Document-ID: 0010
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

2.1 Purpose

This document defines the scope and application of the General Data Protection Regulation (GDPR) for {{ meta.organization }}. It establishes which processing activities of personal data fall under GDPR and which exceptions apply.

2.2 Material Scope (Art. 2 GDPR)

2.2.1 Applicable Processing

GDPR applies to the wholly or partly automated processing of personal data and to the non-automated processing of personal data which form part of a filing system or are intended to form part of a filing system.

In our organization this includes:

Processing Area	Description	Automated	Filing System
[TODO: e.g., Customer Management]	[TODO: Description]	Yes/No	Yes/No
[TODO: e.g., HR Management]	[TODO: Description]	Yes/No	Yes/No
[TODO: e.g., Marketing]	[TODO: Description]	Yes/No	Yes/No
[TODO: e.g., Supplier Management]	[TODO: Description]	Yes/No	Yes/No

2.2.2 Exceptions from Scope

According to Art. 2(2) GDPR, the regulation does not apply to processing of personal data:

1. **In the course of an activity outside the scope of Union law** (Art. 2(2)(a))
   - [TODO: Check relevance for organization]
2. **By Member States in the course of CFSP activities** (Art. 2(2)(b))
   - [TODO: Check relevance for organization]
3. **By natural persons in the course of purely personal or household activities** (Art. 2(2)(c))
   - [TODO: Check relevance for organization]
4. **By competent authorities for prevention, investigation, detection or prosecution of criminal offences** (Art. 2(2)(d))
   - [TODO: Check relevance for organization]

2.3 Territorial Scope (Art. 3 GDPR)

2.3.1 Establishment Principle (Art. 3(1))

GDPR applies to processing of personal data in the context of activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union.

Our organization's establishments:

Location	Country	EU/EEA	Processing Activities
[TODO: Headquarters]	[TODO: Country]	Yes/No	[TODO: Activities]
[TODO: Branch]	[TODO: Country]	Yes/No	[TODO: Activities]

2.3.2 Targeting Principle (Art. 3(2))

GDPR also applies to processing of personal data of data subjects in the Union by a controller or processor not established in the Union, where the processing activities relate to:

1. **Offering goods or services to data subjects in the Union** (Art. 3(2)(a))
   - [TODO: Describe offerings to EU citizens]
   - [TODO: Document targeting activities]
2. **Monitoring behavior of data subjects in the Union** (Art. 3(2)(b))
   - [TODO: Describe tracking/profiling of EU citizens]
   - [TODO: Document online behavior monitoring]

2.3.3 Representative Obligation (Art. 27)

When Art. 3(2) applies and the controller or processor is not established in the Union, a representative must be designated in the Union.

Status: [TODO: Representative required? Yes/No]
Representative: [TODO: Name and contact details, if applicable]

2.4 Personal Data

2.4.1 Definition (Art. 4(1))

Personal data means any information relating to an identified or identifiable natural person.

In our organization we process:

Data Category	Examples	Special Category (Art. 9)
[TODO: e.g., Contact Data]	[TODO: Name, Email, Phone]	No
[TODO: e.g., Contract Data]	[TODO: Customer ID, Orders]	No
[TODO: e.g., Health Data]	[TODO: Description]	Yes
[TODO: e.g., Financial Data]	[TODO: Bank Details, Salary]	No

2.4.2 Special Categories (Art. 9)

Special categories of personal data are subject to enhanced protection requirements: - Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Genetic data - Biometric data for unique identification - Health data - Data concerning sex life or sexual orientation

Processing special categories: [TODO: Yes/No]
Legal basis: [TODO: Art. 9(2)(a)-(j)]

2.5 Cross-Border Processing

2.5.1 Data Transfers to Third Countries

Status: [TODO: Are data transferred to third countries? Yes/No]

Third Country	Purpose	Legal Basis	Safeguards
[TODO: Country]	[TODO: Purpose]	[TODO: Art. 45/46/49]	[TODO: Safeguards]

2.5.2 Intra-Group Data Exchange

Status: [TODO: Intra-group data exchange? Yes/No]
Binding Corporate Rules (BCR): [TODO: In place? Yes/No]

2.6 National Derogations

GDPR contains derogation clauses allowing Member States to adopt more specific provisions.

Relevant national regulations: - [TODO: e.g., national data protection laws] - [TODO: Sector-specific regulations] - [TODO: Other national adaptations]

2.7 Review and Updates

2.7.1 Review Frequency

The scope is reviewed: - **Regularly:** [TODO: e.g., annually] - **As needed:** Upon significant changes in processing activities - **For new products/services:** Before introduction

2.7.2 Responsibilities

- **Responsible for review:** [TODO: Data Protection Officer/Role]
- **Approval:** [TODO: Management/Role]
- **Documentation:** [TODO: Data Protection Team/Role]

2.8 Links to Other Documents

- **Records of Processing Activities (Art. 30):** Detailed listing of all processing
- **Data Protection Principles (Art. 5):** Principles for all processing
- **Legal Bases (Art. 6):** Lawfulness of processing
- **Data Transfers (Art. 44-50):** Rules for third country transfers

---

Next Steps: 1. Identify all processing activities in your organization 2. Check territorial scope (establishments, targeting principle) 3. Document exceptions and special cases 4. Create records of processing activities (Art. 30) 5. Review regularly upon changes

ewpage

Chapter 3

Roles and Responsibilities

Document-ID: 0020
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

3.1 Purpose

This document defines the roles and responsibilities in data protection management of {{ meta.organization }} according to GDPR. It establishes who is responsible for which data protection tasks and how collaboration is organized.

3.2 Key Roles under GDPR

3.2.1 Controller (Art. 4(7))

Definition: Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

In our organization:

Controller	Department	Processing Activities	Contact
[TODO: Name/Role]	[TODO: Department]	[TODO: Activities]	[TODO: Contact]

3.2.2 Processor (Art. 4(8))

Definition: Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Our processors:

Processor	Service	Processed Data	DPA in Place
[TODO: Name]	[TODO: Service]	[TODO: Data Categories]	Yes/No

3.2.3 Data Subject (Art. 4(1))

Definition: Identified or identifiable natural person whose personal data is processed.

Categories of data subjects: - [TODO: e.g., Customers] - [TODO: e.g., Employees] - [TODO: e.g., Applicants] - [TODO: e.g., Supplier Contacts] - [TODO: e.g., Website Visitors]

3.2.4 Data Protection Officer (Art. 37-39)

Designation Obligation: [TODO: Yes/No - Justification according to Art. 37]

Data Protection Officer: - **Name:** [TODO: Name] - **Contact:** [TODO: Email, Phone] - **Position:** Internal/External - **Qualification:** [TODO: Professional qualities]

Tasks of DPO (Art. 39): - Inform and advise controller and employees - Monitor compliance with GDPR - Advise on data protection impact assessments - Cooperate with supervisory authority - Act as contact point for supervisory authority

3.3 Organizational Roles

3.3.1 Management

Responsibilities: - Overall responsibility for data protection compliance - Provision of resources - Approval of data protection policies - Accountability (Art. 5(2))

Contact: [TODO: Name, Contact]

3.3.2 Data Protection Coordinators

Role: Decentralized data protection officers in departments

Department	Coordinator	Responsibilities	Contact
[TODO: IT]	[TODO: Name]	[TODO: Tasks]	[TODO: Contact]
[TODO: HR]	[TODO: Name]	[TODO: Tasks]	[TODO: Contact]
[TODO: Marketing]	[TODO: Name]	[TODO: Tasks]	[TODO: Contact]

3.3.3 Information Security Officer

Responsibilities: - Technical and organizational measures (Art. 32) - IT security concept - Incident response - Cooperation with Data Protection Officer

Contact: [TODO: Name, Contact]

3.4 RACI Matrix Data Protection Processes

Process	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Data Protection Policies	[TODO]	[TODO]	[TODO]	[TODO]
DPIA Execution	[TODO]	[TODO]	[TODO]	[TODO]
Data Subject Requests	[TODO]	[TODO]	[TODO]	[TODO]
Breach Notification	[TODO]	[TODO]	[TODO]	[TODO]
Training	[TODO]	[TODO]	[TODO]	[TODO]
DPA Management	[TODO]	[TODO]	[TODO]	[TODO]

3.5 Joint Controllers (Art. 26)

Status: [TODO: Are there joint controller arrangements? Yes/No]

Partner	Processing Purpose	Agreement	Contact
[TODO: Name]	[TODO: Purpose]	[TODO: Date]	[TODO: Contact]

3.6 Representative (Art. 27)

Required: [TODO: Yes/No - for non-EU establishment with EU processing]

Representative in the EU: - **Name:** [TODO: Name] - **Address:** [TODO: Address] - **Contact:** [TODO: Email, Phone]

3.7 Training and Awareness

3.7.1 Training Program

Target Group	Training Content	Frequency	Responsible
All Employees	Data Protection Basics	Annually	[TODO]
Management	Data Protection Management	Annually	[TODO]
IT Staff	Technical Measures	Semi-annually	[TODO]
HR	Employee Data Protection	Annually	[TODO]

3.8 Communication and Reporting

3.8.1 Internal Communication

- **Data Protection Newsletter:** [TODO: Frequency]

- **Intranet Page:** [TODO: URL]
- **Data Protection Hotline:** [TODO: Contact]

3.8.2 Reporting

Report	Recipient	Frequency	Responsible
Data Protection Status	Management	Quarterly	DPO
Incident Report	Management	As needed	DPO
Audit Results	Management	Annually	DPO

3.9 Contact with Supervisory Authority

Competent Supervisory Authority: [TODO: Name of authority]
Address: [TODO: Address]
Contact: [TODO: Email, Phone, Website]
Organization Contact: [TODO: Data Protection Officer]

Next Steps: 1. Designate all relevant roles and responsibilities 2. Create complete RACI matrix 3. Check designation obligation for Data Protection Officer 4. Document all processor relationships 5. Implement training program

ewpage

Chapter 4

Data Protection Principles

Document-ID: 0030
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

4.1 Purpose

This document describes the data protection principles according to Art. 5 GDPR and their implementation in {{ meta.organization }}. These principles must be observed in every processing of personal data.

4.2 Principles according to Art. 5(1) GDPR

4.2.1 1. Lawfulness, Fairness and Transparency (Art. 5(1)(a))

Principle:
Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Implementation in our organization: - [TODO: Check legal basis before each processing] - [TODO: Transparent privacy notices] - [TODO: Clear information at data collection] - [TODO: Fair processing practices]

4.2.2 2. Purpose Limitation (Art. 5(1)(b))

Principle:
Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

Implementation in our organization: - [TODO: Clear purpose definition at data collection] - [TODO: Check purpose compatibility for further processing] - [TODO: Documentation in records

of processing activities]

4.2.3 3. Data Minimization (Art. 5(1)(c))

Principle:
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Implementation in our organization: - [TODO: Check necessity at data collection] - [TODO: Regular review of stored data] - [TODO: Avoid "nice-to-have" data]

4.2.4 4. Accuracy (Art. 5(1)(d))

Principle:
Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate data are erased or rectified without delay.

Implementation in our organization: - [TODO: Data update processes] - [TODO: Rectification options for data subjects] - [TODO: Regular data quality checks]

4.2.5 5. Storage Limitation (Art. 5(1)(e))

Principle:
Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

Implementation in our organization: - [TODO: Deletion concept with defined periods] - [TODO: Automated deletion routines] - [TODO: Archiving with access restrictions]

4.2.6 6. Integrity and Confidentiality (Art. 5(1)(f))

Principle:
Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Implementation in our organization: - [TODO: Technical and organizational measures (TOM)] - [TODO: Access control systems] - [TODO: Encryption] - [TODO: Backup strategies]

4.3 Accountability (Art. 5(2))

Principle:
The controller shall be responsible for, and be able to demonstrate compliance with, the principles.

Implementation in our organization:

Evidence	Document/Measure	Responsible
Records of Processing	Art. 30 Records	[TODO: DPO]
Legal Bases	Documentation per processing	[TODO: Department]
TOM	Security concept	[TODO: IT Security]
DPIA	DPIA reports	[TODO: DPO]
DPA	Contracts with processors	[TODO: Procurement/Legal]

Evidence	Document/Measure	Responsible
Training	Training records	[TODO: HR]
Data Breaches	Incident log	[TODO: DPO]

4.4 Implementation in Processing

4.4.1 Checklist for New Processing

- ☐ Purpose clearly defined and documented
- ☐ Legal basis identified (Art. 6 or Art. 9)
- ☐ Data minimization checked
- ☐ Storage period defined
- ☐ TOM defined and implemented
- ☐ Information obligations fulfilled (Art. 13-14)
- ☐ Records of processing activities updated
- ☐ DPIA conducted (if required)
- ☐ DPA concluded (for processing)

4.5 Controls and Monitoring

4.5.1 Regular Reviews

Control	Frequency	Responsible	Documentation
Records of Processing	Quarterly	DPO	Review protocol
Deletion Periods	Monthly	IT	Deletion log
Access Logs	Monthly	IT Security	Audit log
TOM Effectiveness	Annually	DPO	Audit report
Training Status	Quarterly	HR	Training matrix

Next Steps: 1. Review all processing for compliance with principles 2. Implement controls for each principle 3. Document evidence for accountability 4. Train employees on principles 5. Establish regular review processes

ewpage

Chapter 5

Lawfulness of Processing

Document-ID: 0040
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

5.1 Purpose

This document describes the legal bases for processing personal data in {{ meta.organization }} according to Art. 6 GDPR. Every processing must be based on at least one of these legal bases.

5.2 Legal Bases according to Art. 6(1) GDPR

5.2.1 Art. 6(1)(a) - Consent

Legal Basis:
The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Requirements for Consent: - Freely given - For specific purposes - Informed - Unambiguous - Withdrawable

Use Cases in our organization:

Processing Purpose	Data Types	Consent Form	Withdrawal Option
[TODO: e.g., Newsletter]	[TODO: Email, Name]	[TODO: Double-Opt-In]	[TODO: Unsubscribe link]
[TODO: e.g., Marketing Cookies]	[TODO: Tracking Data]	[TODO: Cookie Banner]	[TODO: Cookie Settings]

5.2.2 Art. 6(1)(b) - Contract Performance

Legal Basis:
Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

Use Cases in our organization:

Contract Type	Processing Purpose	Required Data	Storage Period
[TODO: Purchase Contract]	[TODO: Order Processing]	[TODO: Name, Address, Payment]	[TODO: Period]
[TODO: Employment Contract]	[TODO: HR Management]	[TODO: Personnel Data]	[TODO: Period]
[TODO: Service Contract]	[TODO: Service Provision]	[TODO: Contact Data]	[TODO: Period]

5.2.3 Art. 6(1)(c) - Legal Obligation

Legal Basis:
Processing is necessary for compliance with a legal obligation to which the controller is subject.

Use Cases in our organization:

Legal Obligation	Legal Basis	Processing Purpose	Data Types	Storage Period
[TODO: Tax Law]	[TODO: Tax Code]	[TODO: Accounting]	[TODO: Invoice Data]	[TODO: 10 years]
[TODO: Social Security]	[TODO: Social Code]	[TODO: Reporting]	[TODO: Social Data]	[TODO: Legal]
[TODO: Commercial Law]	[TODO: Commercial Code]	[TODO: Archiving]	[TODO: Business Data]	[TODO: 6-10 years]

5.2.4 Art. 6(1)(d) - Vital Interests

Legal Basis:
Processing is necessary to protect the vital interests of the data subject or another natural person.

Use Cases in our organization: - [TODO: e.g., Emergency contacts] - [TODO: e.g., Health emergencies] - [TODO: Only in exceptional cases]

5.2.5 Art. 6(1)(e) - Public Interest/Official Authority

Legal Basis:
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Applicability: [TODO: Relevant for public bodies - usually not applicable for private companies]

5.2.6 Art. 6(1)(f) - Legitimate Interests

Legal Basis:
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Three-Step Test: 1. Legitimate interest of the controller 2. Necessity of processing 3. Balancing of interests

Use Cases in our organization:

Processing Purpose	Legitimate Interest	Necessity	Balancing Test	Result
[TODO: Direct Marketing]	[TODO: Marketing]	[TODO: Justification]	[TODO: Balancing]	Lawful/Unlawful
[TODO: IT Security]	[TODO: System Protection]	[TODO: Justification]	[TODO: Balancing]	Lawful/Unlawful
[TODO: Video Surveillance]	[TODO: Security]	[TODO: Justification]	[TODO: Balancing]	Lawful/Unlawful

5.3 Documentation of Legal Bases

5.3.1 Records of Processing Activities (Art. 30)

For each processing activity, the legal basis must be documented:

Processing Activity	Purpose	Legal Basis	Data Types	Storage Period
[TODO: Customer Management]	[TODO: Contract Performance]	Art. 6(1)(b)	[TODO: Master Data]	[TODO: Period]
[TODO: Newsletter]	[TODO: Marketing]	Art. 6(1)(a)	[TODO: Email]	[TODO: Until Withdrawal]
[TODO: Accounting]	[TODO: Tax Law]	Art. 6(1)(c)	[TODO: Invoice Data]	[TODO: 10 years]

5.4 Review Process for New Processing

5.4.1 Legal Basis Checklist

1. **Purpose of processing clearly defined?** Yes/No
2. **Legal basis identified?** Yes/No
3. **For consent:**
   - Freely given? Yes/No
   - Informed? Yes/No
   - Withdrawable? Yes/No
4. **For contract performance:**
   - Objectively necessary? Yes/No

- No milder means? Yes/No

5. **For legitimate interests:**
   - Interest documented? Yes/No
   - Necessity checked? Yes/No
   - Balancing test performed? Yes/No
6. **Documentation in records?** Yes/No

Next Steps: 1. Identify legal basis for each processing activity 2. Document consents and their management 3. Perform balancing tests for legitimate interests 4. Update records of processing activities 5. Train employees on identifying legal bases

ewpage

Chapter 6

Special Categories of Personal Data

Document-ID: 0050
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

6.1 Purpose

This document describes the handling of special categories of personal data in {{ meta.organization }} according to Art. 9 GDPR. These sensitive data are subject to enhanced protection requirements.

6.2 Special Categories (Art. 9(1))

6.2.1 Processing Prohibition

Processing of the following data categories is generally prohibited: - Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Genetic data - Biometric data for the purpose of uniquely identifying a natural person - Health data - Data concerning a person's sex life or sexual orientation

6.2.2 Processing in our Organization

Status: [TODO: Are special categories processed? Yes/No]

Data Category	Processing Purpose	Legal Basis (Art. 9(2))	Data Subjects
[TODO: e.g., Health Data]	[TODO: Purpose]	[TODO: (a)-(j)]	[TODO: Employees]
[TODO: e.g., Biometric Data]	[TODO: Purpose]	[TODO: (a)-(j)]	[TODO: Group]

6.3 Exceptions from Processing Prohibition (Art. 9(2))

6.3.1 Art. 9(2)(a) - Explicit Consent

Requirements: - Explicit (not merely implied) consent - Freely given, informed, unambiguous - For specific purposes - Withdrawable

Use Cases: - [TODO: Describe cases with explicit consent] - [TODO: Consent form] - [TODO: Withdrawal process]

6.3.2 Art. 9(2)(b) - Employment and Social Security Law

Requirements: - Necessary for employment or social security law - Based on Union law, Member State law or collective agreement - Appropriate safeguards for fundamental rights

Use Cases: - [TODO: e.g., Sickness data for continued payment] - [TODO: e.g., Disability status] - [TODO: Specify national legal basis]

6.3.3 Art. 9(2)(c) - Protection of Vital Interests

Requirements: - Protection of vital interests - Data subject is physically or legally incapable of giving consent

Use Cases: - [TODO: e.g., Medical emergencies] - [TODO: Only in exceptional situations]

6.3.4 Art. 9(2)(d) - Processing by Foundations, Associations

Requirements: - Processing by foundation, association or other not-for-profit body - Within scope of legitimate activities - With appropriate safeguards

Applicability: [TODO: Relevant? Yes/No]

6.3.5 Art. 9(2)(e) - Manifestly Made Public Data

Requirements: - Data manifestly made public by the data subject

Use Cases: - [TODO: e.g., Public social media profiles] - [TODO: Caution with interpretation of "manifestly public"]

6.3.6 Art. 9(2)(f) - Legal Claims

Requirements: - Establishment, exercise or defense of legal claims - Courts acting in their judicial capacity

Use Cases: - [TODO: e.g., Employment tribunal proceedings] - [TODO: e.g., Damage claims]

6.3.7 Art. 9(2)(g) - Substantial Public Interest

Requirements: - Substantial public interest - Based on Union or Member State law - Proportionate to aim pursued - Appropriate safeguards

Applicability: [TODO: Relevant? Yes/No]

6.3.8 Art. 9(2)(h) - Healthcare and Occupational Medicine

Requirements: - Healthcare, occupational medicine, medical diagnosis - Based on Union or Member State law - Professional secrecy or statutory confidentiality obligation

Use Cases: - [TODO: e.g., Occupational physician] - [TODO: e.g., Workplace health and safety]

6.3.9 Art. 9(2)(i) - Public Interest in Public Health

Requirements: - Public interest in the area of public health - Protection against serious cross-border health threats - Based on Union or Member State law

Applicability: [TODO: Relevant? Yes/No]

6.3.10 Art. 9(2)(j) - Archiving, Research, Statistics

Requirements: - Archiving purposes in the public interest - Scientific or historical research purposes - Statistical purposes - Based on Union or Member State law - Appropriate safeguards

Use Cases: - [TODO: e.g., Scientific studies] - [TODO: e.g., Statistical evaluations]

6.4 Enhanced Protection Measures

6.4.1 Technical Measures

Measure	Description	Implemented
Encryption	[TODO: Encryption of sensitive data]	Yes/No
Access Control	[TODO: Strict access restrictions]	Yes/No
Pseudonymization	[TODO: Where possible]	Yes/No
Logging	[TODO: Log all access]	Yes/No
Separate Storage	[TODO: Separate from other data]	Yes/No

6.4.2 Organizational Measures

Measure	Description	Implemented
Need-to-know Principle	[TODO: Access only when necessary]	Yes/No
Confidentiality Obligation	[TODO: Special obligation]	Yes/No
Training	[TODO: Specialized training]	Yes/No
DPIA	[TODO: Data Protection Impact Assessment]	Yes/No
Incident Response	[TODO: Special breach processes]	Yes/No

6.5 Data Protection Impact Assessment (DPIA)

Requirement:
When processing special categories, a DPIA according to Art. 35 is generally required.

Status: [TODO: DPIA conducted? Yes/No]
Result: [TODO: Summary]
Measures: [TODO: Risk mitigation measures]

6.6 National Regulations

6.6.1 Example: Germany - BDSG

Relevant Provisions: - § 22 BDSG: Processing of special categories for employees - § 23 BDSG: Processing for scientific purposes - [TODO: Other relevant national regulations]

6.7 Documentation

6.7.1 Records of Processing Activities

For each processing of special categories, document: - Data category (Art. 9(1)) - Processing purpose - Legal basis (Art. 9(2)(a)-(j)) - Data subjects - Recipients - Storage period - TOM (enhanced protection measures) - DPIA reference

6.7.2 Evidence

- Documentation of exception grounds
- DPIA reports
- Consent declarations (for (a))
- National legal bases (for (b), (g), (h), (i), (j))
- TOM documentation

6.8 Data Subject Rights

Particularities: - Enhanced information obligations - Right of access includes legal basis - Right to object for legitimate interests - Withdrawal of consent possible at any time

6.9 Training and Awareness

Training Content: - Identification of special categories - Processing prohibition and exceptions - Enhanced protection measures - Incident response for data breaches - Sanctions for violations

Target Group: All employees with access to special categories

---

Next Steps: 1. Identify all processing of special categories 2. Check legal basis according to Art. 9(2) 3. Implement enhanced protection measures 4. Conduct DPIA 5. Train affected employees

ewpage

Chapter 7

Lawfulness, Fairness and Transparency

Document-ID: 0100
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

7.1 Purpose

This document describes the implementation of the principle of lawfulness, fairness and transparency in {{ meta.organization }}. This principle forms the basis for all data processing.

7.2 Principle according to Art. 5(1)(a) GDPR

Legal Requirement:
Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

7.2.1 Three Components

1. **Lawfulness:** Processing must be based on a legal basis according to Art. 6 or Art. 9 GDPR
2. **Fairness:** Fair and appropriate processing without deception
3. **Transparency:** Comprehensible and understandable information for data subjects

7.3 Implementation of Lawfulness

7.3.1 Legal Basis Assessment

Process before each new processing:

1. **Identification of Legal Basis**
   - Art. 6(1)(a): Consent
   - Art. 6(1)(b): Contract performance
   - Art. 6(1)(c): Legal obligation
   - Art. 6(1)(d): Vital interests
   - Art. 6(1)(e): Public interest
   - Art. 6(1)(f): Legitimate interests
2. **Documentation of Legal Basis**
   - In records of processing activities (Art. 30)
   - In privacy notices
   - In internal processing policies
3. **Regular Review**
   - Quarterly review of existing processing
   - When purposes or scope change

7.3.2 Measures in Our Organization

Measure	Description	Responsible	Status
[TODO: Legal Basis Check]	[TODO: Review process before new processing]	[TODO: DPO]	[TODO]
[TODO: Documentation]	[TODO: Maintain Art. 30 records]	[TODO: Department]	[TODO]
[TODO: Training]	[TODO: Employee training on legal bases]	[TODO: HR]	[TODO]

7.4 Implementation of Fairness

7.4.1 Fair Processing Practices

Principles: - No deception or misleading of data subjects - No hidden or unexpected processing - Appropriate and proportionate data processing - Consideration of legitimate expectations

7.4.2 Specific Measures

Avoiding Unfair Practices: - [TODO: No hidden consents in terms and conditions] - [TODO: Clear separation of mandatory and voluntary information] - [TODO: No coupling of services to unnecessary consents] - [TODO: Appropriate processing scope]

Examples of Fair Processing:

Processing Purpose	Fair Practice	Unfair Practice (to avoid)
[TODO: Newsletter]	[TODO: Separate consent, easy withdrawal]	[TODO: Hidden in T&C, complicated withdrawal]
[TODO: Customer Account]	[TODO: Only necessary data]	[TODO: Excessive data collection]
[TODO: Cookies]	[TODO: Real choice]	[TODO: Cookie wall without alternative]

7.5 Implementation of Transparency

7.5.1 Information Obligations

According to Art. 13-14 GDPR, data subjects must be informed about:

- Identity and contact details of controller
- Contact details of data protection officer
- Purposes and legal basis of processing
- Legitimate interests (for Art. 6(1)(f))
- Recipients or categories of recipients
- Intention to transfer to third countries
- Storage period
- Data subject rights
- Right to withdraw consent
- Right to lodge complaint with supervisory authority
- Obligation or voluntary nature of provision
- Automated decision-making

7.5.2 Transparency Mechanisms in Our Organization

Privacy Notices: - [TODO: Website privacy notice] - [TODO: App privacy notice] - [TODO: Privacy information at data collection] - [TODO: Information sheets for specific processing]

Requirements for Privacy Notices: - Understandable language (no excessive legal jargon) - Structured and clear presentation - Easily accessible and findable - Complete information according to Art. 13-14 - Multilingual for international users

7.5.3 Communication Channels

Channel	Purpose	Target Group	Update
[TODO: Website]	[TODO: Privacy notice]	[TODO: Website visitors]	[TODO: When changes occur]
[TODO: Email]	[TODO: Direct information at collection]	[TODO: Customers]	[TODO: At first contact]
[TODO: Form]	[TODO: Consent declaration]	[TODO: Data subjects]	[TODO: Before processing]
[TODO: Sign]	[TODO: Video surveillance]	[TODO: Visitors]	[TODO: Permanent]

7.6 Comprehensibility and Accessibility

7.6.1 Requirements for Information

Comprehensibility: - Clear and simple language - Avoidance of technical terms or their explanation - Structured presentation with headings - Short sentences and paragraphs

Accessibility: - Easily findable (e.g., link in footer) - Barrier-free (WCAG compliance) - Multiple formats (web, PDF, paper) - Multilingual when needed

7.6.2 Checklist for Transparent Information

- ☐ Information provided before processing begins
- ☐ All mandatory information according to Art. 13-14 included
- ☐ Understandable and clear language
- ☐ Structured and clear
- ☐ Easily accessible
- ☐ Barrier-free
- ☐ Current and complete
- ☐ Contact options provided

7.7 Proof of Compliance (Accountability)

7.7.1 Documentation

Evidence Documents: - Records of processing activities with legal bases - Privacy notices and information sheets - Consent declarations and their management - Training records for employees - Review protocols for legal bases

7.7.2 Controls

Control	Frequency	Responsible	Documentation
[TODO: Legal Basis Review]	Quarterly	DPO	Review protocol
[TODO: Privacy Notices]	When changes occur	Legal/DPO	Version history
[TODO: Transparency Audit]	Annually	DPO	Audit report
[TODO: Training Status]	Quarterly	HR	Training matrix

7.8 Links to Other Documents

- **Legal Bases (Art. 6):** Basis for lawfulness
- **Information Obligations (Art. 13-14):** Implementation of transparency
- **Records (Art. 30):** Documentation of legal bases
- **Data Subject Rights (Art. 12-23):** Transparency about rights

7.9 Common Violations and Their Prevention

Violation	Example	Prevention
Missing legal basis	Processing without review	Legal basis check before processing
Intransparent information	Hidden privacy notice	Prominent placement and clear language

Violation	Example	Prevention
Unfair practices	Cookie wall without alternative	Provide real choices
Incomprehensible language	Legal jargon	Understandable formulations

---

Next Steps: 1. Implement legal basis review for all processing 2. Revise privacy notices for comprehensibility 3. Establish fair processing practices 4. Train employees on transparency requirements 5. Document all measures for accountability

ewpage

Chapter 8

Purpose Limitation

Document-ID: 0110
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

8.1 Purpose

This document describes the implementation of the principle of purpose limitation in {{ meta.organization }}. Personal data may only be collected and processed for specified, explicit and legitimate purposes.

8.2 Principle according to Art. 5(1)(b) GDPR

Legal Requirement:
Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

8.2.1 Core Elements

1. **Specified Purposes:** Purposes must be defined before collection
2. **Explicit Purposes:** Purposes must be clearly and precisely formulated
3. **Legitimate Purposes:** Purposes must be lawful and comprehensible
4. **No Incompatible Further Processing:** New purposes must be compatible or have new legal basis

8.3 Purpose Definition

8.3.1 Requirements for Purpose Descriptions

Purposes must be: - Concrete and specific (not "business purposes") - Understandable for data subjects - Defined before data collection - Documented in records of processing activities - Communicated in privacy notices

8.3.2 Examples of Purpose Definitions

Well Defined	Poorly Defined
"Processing customer orders"	"Business purposes"
"Sending monthly newsletter"	"Marketing"
"Fulfilling tax obligations"	"Legal requirements"
"Processing job applications"	"HR administration"

8.4 Purpose Limitation in Our Organization

8.4.1 Processing Purposes

Processing Activity	Defined Purpose	Legal Basis	Data Types
[TODO: Customer Management]	[TODO: Contract fulfillment, customer service]	Art. 6(1)(b)	[TODO: Master data]
[TODO: Newsletter]	[TODO: Sending product information]	Art. 6(1)(a)	[TODO: Email, name]
[TODO: Accounting]	[TODO: Fulfilling tax obligations]	Art. 6(1)(c)	[TODO: Invoice data]
[TODO: Applicant Management]	[TODO: Processing applications]	Art. 6(1)(b)	[TODO: Applicant data]

8.4.2 Process for Purpose Definition

For new processing:

1. **Clearly define purpose**
   - What should be achieved?
   - Why is the data needed?
   - How does processing contribute to the purpose?
2. **Document purpose**
   - In records of processing activities (Art. 30)
   - In privacy notices (Art. 13-14)
   - In internal processing policies
3. **Communicate purpose**
   - Inform data subjects
   - Train employees
   - Instruct processors

8.5 Further Processing for Other Purposes

8.5.1 Compatibility Assessment (Art. 6(4))

When data is to be processed for a new purpose, it must be assessed:

1. **Is the new purpose compatible with the original purpose?**

Criteria for Compatibility (Art. 6(4)): - Link between original and new purpose - Context of data collection - Nature of personal data - Possible consequences for data subjects - Existing safeguards (e.g., encryption, pseudonymization)

2. **If compatible:** Further processing is permissible
3. **If not compatible:** New legal basis or consent required

8.5.2 Compatibility Test

Criterion	Assessment Question	Evaluation
Link	Is there a factual connection?	[TODO]
Context	Does it meet data subject expectations?	[TODO]
Data Type	Is the data suitable for the new purpose?	[TODO]
Consequences	What are the impacts of further processing?	[TODO]
Safeguards	What protective measures are in place?	[TODO]

Result: Compatible / Not compatible

8.5.3 Examples of Purpose Compatibility

Compatible Further Processing: - Customer data for contract fulfillment → Further processing for warranty claims - Employee data for payroll → Further processing for social security notifications - Order data → Further processing for accounting and taxes

Incompatible Further Processing (new legal basis required): - Customer data for contract fulfillment → Further processing for advertising (consent required) - Applicant data → Further processing for other job offers (new consent required) - Health data for treatment → Further processing for research (new legal basis required)

8.6 Exceptions to Purpose Limitation

8.6.1 Further Processing for Specific Purposes (Art. 5(1)(b))

Always permissible (no compatibility assessment required): - Archiving purposes in the public interest - Scientific or historical research purposes - Statistical purposes

Prerequisite: Appropriate safeguards (e.g., pseudonymization, access restrictions)

8.7 Measures to Ensure Purpose Limitation

8.7.1 Organizational Measures

Measure	Description	Responsible	Status
[TODO: Purpose Definition]	Clear purpose definition before data collection	Department	[TODO]
[TODO: Documentation]	Maintain Art. 30 records	DPO	[TODO]
[TODO: Compatibility Assessment]	Process for new purposes	DPO	[TODO]
[TODO: Training]	Employee training on purpose limitation	HR	[TODO]

8.7.2 Technical Measures

- [TODO: Access control by purposes]
- [TODO: Purpose-based database segmentation]
- [TODO: Automated purpose checking for data access]
- [TODO: Logging of purpose changes]

8.8 Controls and Monitoring

8.8.1 Regular Reviews

Control	Frequency	Responsible	Documentation
Purpose Definitions	Quarterly	DPO	Review protocol
Compatibility Assessments	As needed	DPO	Compatibility test
Records of Processing	Quarterly	DPO	Update protocol
Employee Training	Annually	HR	Training records

8.9 Documentation

8.9.1 Evidence Requirements

Document for each processing: - Defined purpose - Legal basis for the purpose - Data types required for the purpose - Storage period in relation to the purpose - For further processing: Compatibility test or new legal basis

8.9.2 Checklist for New Processing

- ☐ Purpose clearly and explicitly defined
- ☐ Purpose is legitimate and lawful
- ☐ Purpose defined before data collection
- ☐ Purpose documented in Art. 30 records
- ☐ Purpose communicated in privacy notice
- ☐ Only data necessary for purpose collected
- ☐ Storage period oriented to purpose
- ☐ Employees informed about purpose

8.10 Links to Other Documents

- **Data Protection Principles (Art. 5):** Purpose limitation as core principle
- **Legal Bases (Art. 6):** Legitimacy of purposes
- **Records (Art. 30):** Documentation of purposes
- **Information Obligations (Art. 13-14):** Communication of purposes
- **Data Minimization (Art. 5(1)(c)):** Purpose-related data collection

8.11 Common Violations and Their Prevention

Violation	Example	Prevention
Unclear purposes	"Business purposes"	Concrete purpose definition
Purpose misuse	Customer data for advertising without consent	Conduct compatibility assessment
Missing documentation	Purpose not in records	Maintain Art. 30 records
Retrospective purpose change	Purpose changed after collection	Define purpose before collection

---

Next Steps: 1. Define clear purposes for all processing activities 2. Document purposes in records of processing activities 3. Implement compatibility assessment for new purposes 4. Train employees on purpose limitation 5. Regularly review compliance with purpose limitation

ewpage

Chapter 9

Data Minimization

Document-ID: 0120
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

9.1 Purpose

This document describes the implementation of the principle of data minimization in {{ meta.organization }}. Only personal data that is actually necessary for the respective purpose may be collected.

9.2 Principle according to Art. 5(1)(c) GDPR

Legal Requirement:
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

9.2.1 Three Criteria

1. **Adequate:** Data must be in reasonable proportion to the purpose
2. **Relevant:** Data must be relevant to the purpose
3. **Limited to Necessary:** Collect only minimally required data

9.3 Necessity Assessment

9.3.1 Assessment Process for Data Collection

Before each data collection, assess:

1. **Is data collection necessary for the purpose?**

- Can the purpose be achieved without this data?
- Are there milder means?
- Is data collection proportionate?

2. **What data is minimally required?**
   - Which data is absolutely necessary?
   - Which data is "nice-to-have" (to avoid)?
   - Can data be anonymized or pseudonymized?
3. **Documentation of Necessity**
   - Justification in records of processing activities
   - Evidence of necessity assessment
   - Regular review

9.3.2 Necessity Matrix

Data Type	Purpose	Necessary?	Justification	Alternative
[TODO: Name]	[TODO: Contract fulfillment]	Yes	[TODO: Identification]	None
[TODO: Date of birth]	[TODO: Newsletter]	No	[TODO: Not required]	Omit
[TODO: Address]	[TODO: Delivery]	Yes	[TODO: Shipping]	Parcel station
[TODO: Phone]	[TODO: Contact]	Partially	[TODO: Alternative email]	Email

9.4 Implementation in Our Organization

9.4.1 Data Collection by Categories

Mandatory vs. voluntary information:

Processing Purpose	Mandatory Information	Voluntary Information	Not Required
[TODO: Order]	[TODO: Name, address, payment]	[TODO: Phone]	[TODO: Date of birth]
[TODO: Newsletter]	[TODO: Email]	[TODO: Name]	[TODO: Address]
[TODO: Customer Account]	[TODO: Email, password]	[TODO: Profile picture]	[TODO: Social media]

Marking in Forms: - Mark mandatory fields with * - Clearly mark voluntary fields - Explain why data is needed

9.4.2 Measures for Data Minimization

Measure	Description	Responsible	Status
[TODO: Necessity Assessment]	Review before new processing	DPO	[TODO]
[TODO: Form Optimization]	Reduction of input fields	IT	[TODO]
[TODO: Anonymization]	Use anonymous data where possible	IT	[TODO]
[TODO: Pseudonymization]	Pseudonyms instead of clear data	IT	[TODO]

9.5 Technical Implementation

9.5.1 Privacy by Design (Art. 25)

Data minimization through design:

- [TODO: Forms with only required fields]
- [TODO: Optional fields clearly marked]
- [TODO: Automatic anonymization after purpose fulfillment]
- [TODO: Pseudonymization of sensitive data]
- [TODO: Aggregation instead of individual data for statistics]

9.5.2 Anonymization and Pseudonymization

Anonymization: - Complete removal of personal reference - No traceability to persons - No GDPR application anymore

Pseudonymization: - Separation of identification and content data - Traceability only with additional information - Still GDPR application, but lower risk

Use Cases:

Purpose	Method	Example
[TODO: Statistics]	Anonymization	Aggregated usage data
[TODO: Analysis]	Pseudonymization	User ID instead of name
[TODO: Research]	Anonymization	Removal of all identifiers
[TODO: Backup]	Pseudonymization	Encrypted personal data

9.6 Avoiding Excessive Data Collection

9.6.1 Common Mistakes

Mistake	Example	Correction
“Nice-to-have” data	Date of birth for newsletter	Collect only email
Excessive profiling	Tracking all activities	Only necessary tracking
Data retention	“Might be useful someday”	Only with specific purpose
Missing differentiation	All data as mandatory	Separate mandatory vs. voluntary

9.6.2 Checklist Against Excessive Data Collection

- ☐ Each data field has documented purpose
- ☐ No "nice-to-have" data fields
- ☐ Mandatory and voluntary fields separated
- ☐ Anonymization/pseudonymization assessed
- ☐ No data retention
- ☐ Regular review of necessity
- ☐ Employees trained on data minimization

9.7 Regular Review

9.7.1 Data Inventory Review

Quarterly review:

1. **What data is collected?**
   - Inventory of all data fields
   - Assignment to processing purposes
2. **Is all data still necessary?**
   - Necessity assessment for existing data
   - Identification of superfluous data
3. **Can data be reduced?**
   - Possibilities for anonymization
   - Possibilities for pseudonymization
   - Deletion of no longer required data

9.7.2 Controls

Control	Frequency	Responsible	Documentation
Necessity Assessment	For new processing	DPO	Review protocol
Data Inventory Review	Quarterly	DPO	Inventory list
Form Review	Annually	IT/DPO	Review report
Anonymization Potential	Annually	IT	Analysis report

9.8 Documentation

9.8.1 Evidence Requirements

Document for each processing: - What data is collected? - Why is each data type necessary? - Were alternatives assessed (anonymization, pseudonymization)? - How is necessity regularly reviewed?

9.8.2 Records of Processing Activities (Art. 30)

Documentation of data minimization: - Categories of personal data - Justification of necessity - Minimization measures - Anonymization/pseudonymization

9.9 Links to Other Documents

- **Data Protection Principles (Art. 5):** Data minimization as core principle
- **Purpose Limitation (Art. 5(1)(b)):** Purpose-related necessity
- **Privacy by Design (Art. 25):** Technical implementation
- **Records (Art. 30):** Documentation of data types
- **Information Obligations (Art. 13-14):** Information about collected data

9.10 Common Violations and Their Prevention

Violation	Example	Prevention
Excessive data collection	All data "just in case"	Necessity assessment
Missing differentiation	All fields as mandatory	Mandatory vs. voluntary
Data retention	Data without specific purpose	Observe purpose limitation
No anonymization	Clear data where not needed	Assess anonymization

---

Next Steps: 1. Conduct necessity assessment for all data collections 2. Optimize forms and reduce data fields 3. Implement anonymization and pseudonymization 4. Train employees on data minimization 5. Establish regular data inventory reviews

ewpage

Chapter 10

Accuracy

Document-ID: 0130
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

10.1 Purpose

This document describes the implementation of the principle of accuracy in {{ meta.organization }}. Personal data must be accurate and up to date.

10.2 Principle according to Art. 5(1)(d) GDPR

Legal Requirement:
Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

10.2.1 Two Components

1. **Factual Accuracy:** Data must correspond to facts
2. **Currency:** Data must be kept up to date

10.3 Measures to Ensure Accuracy

10.3.1 Data Quality Management

Quality Assurance Processes:

Measure	Description	Responsible	Frequency
[TODO: Input Validation]	Check at data entry	IT	Continuous
[TODO: Plausibility Check]	Automatic consistency check	IT	Continuous
[TODO: Data Reconciliation]	Comparison with external sources	Department	[TODO: Monthly]
[TODO: Update Reminder]	Reminder for data update	IT	[TODO: Annually]

10.3.2 Input Validation

Technical Measures at Data Entry: - [TODO: Format validation (email, phone, postal code)] - [TODO: Mandatory field validation] - [TODO: Value range validation] - [TODO: Duplicate check] - [TODO: Consistency check between fields]

10.3.3 Data Updates

Processes for Currency Assurance:

Data Type	Update Process	Frequency	Responsible
[TODO: Customer master data]	[TODO: Update on contact]	As needed	Sales
[TODO: Employee data]	[TODO: Annual review]	Annually	HR
[TODO: Contact data]	[TODO: Validation on use]	On use	IT
[TODO: Contract data]	[TODO: Update on contract change]	On change	Legal

10.4 Right to Rectification (Art. 16 GDPR)

10.4.1 Implementation of Rectification Right

Data subjects have the right to: - Immediate rectification of inaccurate data - Completion of incomplete data - Supplementary statement

Process for Rectification Requests:

1. **Receipt of Request**
   - Identification of data subject
   - Documentation of request
   - Confirmation of receipt
2. **Review of Inaccuracy**
   - Verification of contested data
   - Comparison with evidence

- Decision on rectification

3. **Implementation of Rectification**
   - Correction in all systems
   - Information to recipients (Art. 19)
   - Documentation of rectification
4. **Response to Data Subject**
   - Information about rectification performed
   - Deadline: Without delay, at most 1 month

10.4.2 Rectification Channels

Channel	Description	Processing Time	Responsible
[TODO: Online Portal]	Self-rectification by user	Immediate	IT
[TODO: Email]	Request by email	1 month	DPO
[TODO: Written]	Request by mail	1 month	DPO
[TODO: Phone]	Telephone rectification	Immediate	Customer Service

10.5 Error Correction Procedures

10.5.1 Error Identification

Error Sources: - Input errors during data capture - Outdated data due to time lapse - Faulty data transmission - System errors in data processing - Incomplete data collection

Error Detection: - [TODO: Automatic plausibility check] - [TODO: Report by data subjects] - [TODO: Regular data quality check] - [TODO: Feedback from recipients]

10.5.2 Correction Process

Steps Upon Error Detection:

1. **Error Analysis**
   - Type of error
   - Scope of impact
   - Cause of error
2. **Error Correction**
   - Rectification of erroneous data
   - Correction in all affected systems
   - Documentation of correction
3. **Notification**
   - Information to data subject
   - Communication to recipients (Art. 19)
   - Documentation of notifications
4. **Root Cause Elimination**
   - Analysis of error cause

- Measures for error prevention
- Process improvement

10.6 Notification Obligation (Art. 19 GDPR)

10.6.1 Notification of Recipients

Recipients must be informed of rectification or erasure:

Recipient Type	Notification Obligation	Exception	Documentation
Processors	Yes	Impossible/disproportionate	Notification log
Third Party Recipients	Yes	Impossible/disproportionate	Notification log
Public Authorities	Yes	Impossible/disproportionate	Notification log

Process: 1. Identification of all recipients 2. Notification of rectification/erasure 3. Documentation of notifications 4. Information to data subject about recipients (on request)

10.7 Data Quality Controls

10.7.1 Regular Reviews

Control	Frequency	Responsible	Documentation
Data Quality Audit	Annually	DPO	Audit report
Sample Check	Quarterly	Department	Review protocol
System Validation	On changes	IT	Test protocol
Rectification Statistics	Monthly	DPO	Statistics report

10.7.2 Quality Metrics

KPIs for Data Quality: - Error rate in data entry - Number of rectification requests - Average processing time - Proportion of outdated records - Completeness level of data

10.8 Documentation

10.8.1 Evidence Requirements

Documentation for Accountability: - Processes to ensure accuracy - Rectification procedures and deadlines - Processed rectification requests - Notifications to recipients - Data quality controls and their results

10.8.2 Rectification Register

Date	Data Subject	Type of Rectification	Recipients Notified	Processor
[TODO]	[TODO]	[TODO]	Yes/No	[TODO]

10.9 Links to Other Documents

- **Data Protection Principles (Art. 5):** Accuracy as core principle
- **Right to Rectification (Art. 16):** Implementation of data subject right
- **Notification Obligation (Art. 19):** Notification of recipients
- **Records (Art. 30):** Documentation of data quality
- **TOM (Art. 32):** Technical measures for quality assurance

10.10 Common Violations and Their Prevention

Violation	Example	Prevention
Outdated data	No updates	Regular review
Erroneous input	No validation	Input validation
Delayed rectification	Long processing time	Process optimization
Missing notification	Recipients not informed	Notification process

---

Next Steps: 1. Implement input validation and plausibility checks 2. Establish processes for regular data updates 3. Set up rectification procedures according to Art. 16 4. Implement notification process for recipients 5. Conduct regular data quality controls

ewpage

Chapter 11

Storage Limitation

Document-ID: 0140
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

11.1 Purpose

This document describes the implementation of the principle of storage limitation in {{ meta.organization }}. Personal data may only be stored for as long as necessary for the processing purpose.

11.2 Principle according to Art. 5(1)(e) GDPR

Legal Requirement:
Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

11.2.1 Core Principle

Storage Period = Purpose Fulfillment + Legal Retention Periods

After expiration of storage period, data must be: - Deleted, or - Anonymized, or - Archived (with access restrictions)

11.3 Deletion Concept

11.3.1 Definition of Deletion Periods

Criteria for Deletion Periods: 1. Purpose of processing 2. Legal retention periods 3. Contractual obligations 4. Legitimate interests 5. Limitation periods

11.3.2 Deletion Period Matrix

Processing Purpose	Data Type	Deletion Period	Legal Basis	Exceptions
[TODO: Customer Order]	Order data	After contract fulfillment + 2 years	Warranty	Tax law: 10 years
[TODO: Newsletter]	Email, name	Until withdrawal	Consent	None
[TODO: Application]	Applicant data	6 months after rejection	Legitimate interest	Longer with consent
[TODO: Accounting]	Invoice data	10 years	Tax code, Commercial code	None
[TODO: Employee Data]	Personnel data	10 years after departure	Social security	None

11.4 Legal Retention Periods

11.4.1 Tax Law (Example: Germany)

Document Type	Retention Period	Legal Basis
Books, records, annual statements	10 years	§ 147 AO
Commercial letters, accounting documents	10 years	§ 147 AO
Other documents	6 years	§ 147 AO

11.4.2 Commercial Law (Example: Germany)

Document Type	Retention Period	Legal Basis
Commercial books, inventories, balance sheets	10 years	§ 257 HGB
Commercial letters	6 years	§ 257 HGB
Accounting documents	10 years	§ 257 HGB

11.4.3 Other Legal Periods

- [TODO: Social security law]
- [TODO: Labor law]
- [TODO: Product liability]
- [TODO: Industry-specific regulations]

11.5 Deletion Processes

11.5.1 Routine Deletion

Automated Deletion Processes:

System/Database	Deletion Rhythm	Method	Responsible
[TODO: CRM System]	Monthly	Automated	IT
[TODO: Web Server Logs]	Daily	Automated	IT
[TODO: Backup Systems]	On deletion	Manual	IT
[TODO: Archive]	Annually	Manual	Department

11.5.2 Deletion Procedure

Steps for Deletion:

1. **Identification of Deletable Data**
   - Automatic check of deletion periods
   - Consideration of exceptions
   - Creation of deletion list
2. **Review Before Deletion**
   - No ongoing proceedings
   - No legal retention obligations
   - No contractual obligations
3. **Implementation of Deletion**
   - Deletion in all systems
   - Deletion in backups (or marking)
   - Secure deletion (irrecoverable)
4. **Documentation**
   - Logging of deletion
   - Evidence of deletion
   - Retention of deletion log

11.5.3 Secure Deletion

Technical Deletion Methods: - Overwriting of data carriers - Cryptographic deletion (key destruction) - Physical destruction of data carriers - Secure deletion in cloud systems

11.6 Exceptions to Deletion Obligation

11.6.1 Archiving in Public Interest (Art. 89 GDPR)

Permissible Archiving for: - Archiving purposes in the public interest - Scientific or historical research purposes - Statistical purposes

Prerequisites: - Appropriate safeguards (pseudonymization, access restrictions) - Data minimization - Technical and organizational measures

11.6.2 Retention for Legal Claims

Retention Permissible for: - Ongoing court proceedings - Threatening legal disputes - Limitation periods not yet expired

Measures: - Restriction of processing (Art. 18) - Access restrictions - Documentation of retention reasons

11.7 Right to Erasure (Art. 17 GDPR)

11.7.1 Implementation of Erasure Right

Data subjects have right to erasure when: - Data no longer necessary - Consent withdrawn - Objection lodged (Art. 21) - Data unlawfully processed - Legal obligation to erase

Exceptions to Erasure Right: - Exercise of right to freedom of expression - Compliance with legal obligations - Establishment of legal claims - Archiving purposes in public interest

11.7.2 Erasure Request Process

1. **Receipt of Request**
   - Identification of data subject
   - Documentation of request
   - Confirmation of receipt
2. **Review of Erasure Obligation**
   - Is data still necessary?
   - Are there retention obligations?
   - Do exceptions apply?
3. **Implementation or Rejection**
   - If erasure obligation: Perform deletion
   - If exception: Reasoned rejection
   - Notification of recipients (Art. 19)
4. **Response**
   - Information about erasure or rejection
   - Deadline: Without delay, at most 1 month

11.8 Controls and Monitoring

11.8.1 Regular Reviews

Control	Frequency	Responsible	Documentation
Deletion Period Review	Monthly	IT	Deletion log
Deletion Concept Review	Annually	DPO	Review report
Backup Deletion	Quarterly	IT	Backup log
Erasure Requests	On receipt	DPO	Request register

11.8.2 Deletion Logging

Documentation of Each Deletion: - Date and time - Deleted data types - Number of deleted records - Deletion reason (period, request, etc.) - Executing person - Affected systems

11.9 Documentation

11.9.1 Evidence Requirements

Document for Accountability: - Deletion concept with periods - Deletion processes and procedures - Performed deletions (logs) - Processed erasure requests - Exceptions and their justification

11.9.2 Records of Processing Activities (Art. 30)

Documentation of Storage Period: - Deletion periods for each processing activity - Justification of periods - Legal retention obligations - Deletion procedures

11.10 Links to Other Documents

- **Data Protection Principles (Art. 5):** Storage limitation as core principle
- **Right to Erasure (Art. 17):** Implementation of data subject right
- **Restriction (Art. 18):** Alternative to deletion
- **Notification Obligation (Art. 19):** Notification of recipients
- **Records (Art. 30):** Documentation of deletion periods

11.11 Common Violations and Their Prevention

Violation	Example	Prevention
Unlimited storage	"Keep just in case"	Define deletion periods
Missing deletion processes	No automated deletion	Implement deletion routines
Ignoring erasure requests	Delayed processing	Establish process
Incomplete deletion	Only deleted in one system	Check all systems

---

Next Steps: 1. Define deletion periods for all processing activities 2. Implement automated deletion processes 3. Establish procedures for erasure requests 4. Document deletion concept and logs 5. Train employees on deletion obligations

ewpage

Chapter 12

Integrity and Confidentiality

Document-ID: 0150
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

12.1 Purpose

This document describes the implementation of the principle of integrity and confidentiality in {{ meta.organization }}. Personal data must be processed securely and protected from unauthorized access.

12.2 Principle according to Art. 5(1)(f) GDPR

Legal Requirement:
Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

12.2.1 Protection Goals

1. **Confidentiality:** Protection against unauthorized access
2. **Integrity:** Protection against unauthorized modification
3. **Availability:** Protection against loss or destruction
4. **Resilience:** Resistance of systems

12.3 Technical and Organizational Measures (TOM)

12.3.1 Overview of Measure Categories (Art. 32 GDPR)

Category	Description	Examples
Access Control	Protection against unauthorized entry	Access controls, alarms, video surveillance
Authentication Control	Protection against unauthorized system use	User authentication, password policies, MFA
Authorization Control	Protection against unauthorized data access	Permission concept, role model, need-to-know
Transmission Control	Protection during data transmission	Encryption, VPN, secure protocols
Input Control	Traceability of inputs	Logging, audit trails, versioning
Processing Control	Security in data processing	DPA, controls, audits
Availability Control	Protection against data loss	Backups, redundancy, disaster recovery
Separation Control	Separation of different purposes	Multi-tenancy, data segmentation

12.4 Access Control

12.4.1 Physical Security

Measures to protect against unauthorized entry:

Measure	Description	Responsible	Status
[TODO: Access Controls]	Chip cards, keys, codes	Facility Management	[TODO]
[TODO: Visitor Registration]	Registration and escort	Reception	[TODO]
[TODO: Video Surveillance]	Monitoring of sensitive areas	Security	[TODO]
[TODO: Alarm Systems]	Intrusion detection systems	Security	[TODO]
[TODO: Server Room Security]	Special protection for servers	IT	[TODO]

12.5 Authentication Control

12.5.1 Authentication and Authorization

Measures for system access control:

Measure	Description	Implementation	Status
[TODO: User Authentication]	Unique user accounts	Active Directory	[TODO]

Measure	Description	Implementation	Status
[TODO: Password Policy]	Complexity, length, expiration	Group policies	[TODO]
[TODO: Multi-Factor Authentication]	Additional authentication factor	MFA system	[TODO]
[TODO: Single Sign-On]	Central authentication	SSO solution	[TODO]
[TODO: Automatic Lockout]	After inactivity	System setting	[TODO]

12.5.2 Password Policy

Requirements: - Minimum length: [TODO: e.g., 12 characters] - Complexity: [TODO: Upper/lowercase, numbers, special characters] - Expiration: [TODO: e.g., 90 days] - History: [TODO: e.g., last 5 passwords not reusable] - Lockout: [TODO: After 5 failed attempts]

12.6 Authorization Control

12.6.1 Permission Concept

Principles: - Need-to-know: Only necessary access - Least Privilege: Minimal permissions - Role-Based Access Control (RBAC): Role-based access - Regular Review: Quarterly recertification

12.6.2 Permission Matrix

Role	System/Data	Access	Justification
[TODO: Administrator]	All systems	Full access	System administration
[TODO: Sales]	CRM	Read/Write	Customer service
[TODO: Accounting]	Financial system	Read/Write	Accounting
[TODO: Support]	Ticket system	Read/Write	Customer service

12.6.3 Access Control Processes

Process	Description	Responsible	Frequency
Permission Grant	Request and approval	IT/Supervisor	As needed
Recertification	Review of existing rights	IT/Supervisor	Quarterly
Revocation on Departure	Immediate lockout	HR/IT	On departure
Privileged Access	Special control	IT Security	Monthly

12.7 Transmission Control

12.7.1 Encryption

Encryption Measures:

Area	Method	Standard	Status
[TODO: Data Transmission]	TLS/SSL	TLS 1.2+	[TODO]
[TODO: Email]	S/MIME or PGP	-	[TODO]
[TODO: Data Carriers]	Disk encryption	AES-256	[TODO]
[TODO: Databases]	Transparent Data Encryption	AES-256	[TODO]
[TODO: Backups]	Encrypted backups	AES-256	[TODO]

12.7.2 Secure Data Transmission

Measures: - [TODO: VPN for remote access] - [TODO: HTTPS for web applications] - [TODO: SFTP for file transfers] - [TODO: Encrypted email for sensitive data] - [TODO: Secure cloud connections]

12.8 Input Control

12.8.1 Logging and Audit Trails

Logging of:

Event	Details	Retention	Access
[TODO: Logins]	Success/failure, timestamp	90 days	IT Security
[TODO: Data Changes]	Who, what, when	1 year	DPO
[TODO: Access to Sensitive Data]	User, timestamp, data	1 year	DPO
[TODO: System Changes]	Administrator, change	2 years	IT
[TODO: Security Events]	Type, timestamp, source	2 years	IT Security

12.8.2 Traceability

Measures: - Unique user identification - Timestamps for all actions - Immutable logs - Regular analysis - Long-term archiving

12.9 Availability Control

12.9.1 Backup and Recovery

Backup Strategy:

Backup Type	Frequency	Retention	Location	Responsible
[TODO: Full Backup]	Weekly	4 weeks	Offsite	IT
[TODO: Incremental]	Daily	7 days	Onsite	IT
[TODO: Archive]	Monthly	1 year	Offsite	IT

Recovery Process: - Regular restore tests - Documented recovery procedures - Recovery Time Objective (RTO): [TODO] - Recovery Point Objective (RPO): [TODO]

12.9.2 Business Continuity

Measures: - [TODO: Redundant systems] - [TODO: Disaster recovery plan] - [TODO: Emergency manual] - [TODO: Regular tests]

12.10 Incident Response

12.10.1 Security Incidents

Process for Security Incidents:

1. **Detection and Reporting**
   - Identification of incident
   - Immediate report to IT Security
   - Initial assessment
2. **Containment**
   - Isolation of affected systems
   - Damage limitation
   - Evidence preservation
3. **Analysis**
   - Root cause analysis
   - Scope of impact
   - Assessment of consequences
4. **Remediation**
   - Elimination of cause
   - Restoration of normal operations
   - Documentation
5. **Post-Incident**
   - Lessons learned
   - Improvement measures
   - Training

12.10.2 Data Breaches (Art. 33-34 GDPR)

For data breaches additionally: - Notification to supervisory authority (within 72 hours) - Notification of data subjects (if high risk) - Documentation in register of data breaches

12.11 Controls and Monitoring

12.11.1 Regular Reviews

Control	Frequency	Responsible	Documentation
Security Audit	Annually	IT Security	Audit report
Penetration Test	Annually	External Provider	Test report
Permission Review	Quarterly	IT	Review protocol
Backup Test	Monthly	IT	Test protocol
Log Analysis	Weekly	IT Security	Analysis report

12.12 Documentation

12.12.1 Evidence Requirements

Documentation of TOM: - Description of all technical and organizational measures - Justification of appropriateness - Evidence of effectiveness (tests, audits) - Updates on changes

12.12.2 Security Concept

Contents: - Protection goals and risk assessment - Technical measures - Organizational measures - Responsibilities - Controls and tests - Incident response plan

12.13 Links to Other Documents

- **Data Protection Principles (Art. 5):** Integrity and confidentiality as core principle
- **Security of Processing (Art. 32):** Detailed requirements for TOM
- **Data Breaches (Art. 33-34):** Notification obligations for security incidents
- **Records (Art. 30):** Documentation of TOM
- **DPIA (Art. 35):** Risk assessment and measures

12.14 Common Violations and Their Prevention

Violation	Example	Prevention
Weak passwords	Simple passwords	Enforce password policy
Missing encryption	Unencrypted transmission	Implement TLS/SSL
Excessive permissions	Everyone has admin rights	Implement permission concept
No backups	Data loss without recovery	Implement backup strategy

---

Next Steps: 1. Implement comprehensive TOM according to Art. 32 2. Establish access control and permission concept 3. Implement encryption for data at rest and in transit 4. Set up backup and recovery processes 5. Establish incident response process

ewpage

Chapter 13

Transparent Information and Communication

Document-ID: 0200
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

13.1 Purpose

This document describes the implementation of requirements for transparent information and communication in {{ meta.organization }}. Data subjects must be able to exercise their rights easily and comprehensibly.

13.2 Principle according to Art. 12 GDPR

Legal Requirements:

The controller must: - Provide transparent, understandable and easily accessible information - Communicate in clear and plain language - Provide information free of charge - Respond to requests without delay, at most within one month - Take appropriate measures for identification

13.3 Transparency Requirements

13.3.1 Understandable Communication

Requirements for Information:

Criterion	Description	Implementation
Precise	Concrete and specific	[TODO: Clear formulations]

Criterion	Description	Implementation
Transparent	Open and comprehensible	[TODO: Complete information]
Understandable	Plain language	[TODO: No jargon]
Easily Accessible	Easy to find	[TODO: Prominent placement]

13.3.2 Language Requirements

Clear and Plain Language: - Avoidance of legal jargon - Short sentences and paragraphs - Explanation of technical terms - Structured presentation - Use of examples

Multilingualism: - [TODO: English as main language] - [TODO: Other languages for international users] - [TODO: Additional languages as needed]

13.4 Communication Channels

13.4.1 Provision of Information

Channels for Privacy Information:

Channel	Purpose	Target Group	Update
[TODO: Website]	Privacy notice	Website visitors	On changes
[TODO: App]	In-app privacy notices	App users	On changes
[TODO: Email]	Direct information	Customers	At first contact
[TODO: Form]	Data collection	Data subjects	At collection
[TODO: Sign]	On-site information	Visitors	Permanent

13.4.2 Contact Options

Channels for Data Subject Requests:

Channel	Description	Processing Time	Responsible
[TODO: Email]	privacy@organization.com	1 month	DPO
[TODO: Online Form]	Contact form on website	1 month	DPO
[TODO: Written]	Postal address	1 month	DPO
[TODO: Phone]	Hotline	Immediate	Customer Service
[TODO: In Person]	On-site appointment	By arrangement	DPO

13.5 Deadlines and Procedures

13.5.1 Processing Deadlines (Art. 12(3))

Basic Deadline: - Without delay, at most within one month of receipt

Extension: - By further two months for complex requests - Justification of extension required - Information to data subject within one month

Factors for Complexity: - Number of requests - Scope of affected data - Technical difficulty - Number of affected systems

13.5.2 Processing Procedure

Standard Process for Data Subject Requests:

1. **Receipt of Request (Day 0)**
   - Registration in request system
   - Acknowledgment to data subject
   - Assignment to processor
2. **Identification (Day 1-3)**
   - Verification of identity
   - If doubts: Request additional information
   - Documentation of identification
3. **Processing (Day 4-25)**
   - Review of request
   - Compilation of information
   - Coordination with departments
   - Preparation of response
4. **Response (Day 26-30)**
   - Transmission of response
   - Documentation of processing
   - Archiving of correspondence

13.5.3 Deadline Control

Milestone	Deadline	Responsible	Escalation
Acknowledgment	2 business days	DPO Team	DPO
Identification	5 business days	DPO Team	DPO
Processing	25 days	Department	DPO
Response	30 days	DPO	Management

13.6 Identification of Data Subject

13.6.1 Identification Process

Measures for Identification:

Method	Description	Use Case	Security Level
[TODO: Customer Account]	Login with credentials	Online requests	High
[TODO: ID Document]	Copy of ID	Written requests	Very high
[TODO: Security Questions]	Personal questions	Phone requests	Medium
[TODO: Email Verification]	Confirmation link	Email requests	Medium

Method	Description	Use Case	Security Level
[TODO: In Person]	On-site identification	Personal requests	Very high

13.6.2 Doubts About Identity (Art. 12(6))

In case of reasonable doubts: - Request additional information for identity confirmation - No processing until identity confirmation - Information to requesting person - Documentation of doubts and measures

13.7 Free of Charge

13.7.1 Principle of No Cost (Art. 12(5))

Information and measures are generally free of charge.

Exceptions (fees permissible): - Manifestly unfounded requests - Excessive requests (especially frequent repetition)

Fee Schedule: - Reasonable fee based on administrative costs - Justification of fee required - Information to data subject before processing

13.7.2 Refusal of Requests

Requests may be refused if: - Manifestly unfounded - Excessive (frequent repetition)

Process for Refusal: 1. Justification of refusal 2. Information about right to lodge complaint with supervisory authority 3. Information about judicial remedies 4. Documentation of refusal

13.8 Documentation

13.8.1 Request Register

Documentation of All Data Subject Requests:

Date	Data Subject	Type of Request	Processing Status	Deadline	Processor
[TODO]	[TODO]	[TODO: Access]	[TODO: In progress]	[TODO: XX.XX.XXXX]	[TODO]

13.8.2 Evidence Requirements

Document for Accountability: - All received requests - Processing steps and times - Identification measures - Responses and refusals - Fees and their justification

13.9 Training and Awareness

13.9.1 Employee Training

Training Content: - Data subject rights and their significance - Processing procedures and deadlines - Identification procedures - Communication standards - Escalation paths

Training Frequency: - New employees: At hiring - All employees: Annually - DPO team: Quarterly updates

13.10 Links to Other Documents

- **Information Obligations (Art. 13-14):** Provision of information
- **Right of Access (Art. 15):** Processing of access requests
- **Rectification (Art. 16):** Processing of rectification requests
- **Erasure (Art. 17):** Processing of erasure requests
- **Other Data Subject Rights (Art. 18-22):** Processing of other requests

13.11 Common Violations and Their Prevention

Violation	Example	Prevention
Deadline Exceeded	Response after 2 months	Implement deadline control
Incomprehensible Language	Legal jargon	Use plain language
Missing Identification	No identity verification	Establish identification process
Charged Access	Fee without justification	Observe principle of no cost

---

Next Steps: 1. Establish communication channels for data subject requests 2. Implement processing procedures with deadline control 3. Define identification procedures 4. Train employees on data subject rights 5. Document all requests in request register

ewpage

Chapter 14

Information Obligations at Collection

Document-ID: 0210
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

14.1 Purpose

This document describes the implementation of information obligations in {{ meta.organization }}. Data subjects must be comprehensively informed when their data is collected.

14.2 Information Obligation for Direct Collection (Art. 13)

14.2.1 Mandatory Information

When collecting personal data from the data subject, the following information must be provided:

Information	Description	Example
Identity of Controller	Name and contact details	[TODO: Company name, address]
Contact Details of DPO	If applicable	[TODO: privacy@organization.com]
Purposes of Processing	What data is used for	[TODO: Contract fulfillment, marketing]
Legal Basis	Art. 6 or Art. 9 GDPR	[TODO: Art. 6(1)(b)]
Legitimate Interests	For Art. 6(1)(f)	[TODO: Direct marketing]
Recipients	Who receives the data	[TODO: Shipping service provider]

Information	Description	Example
Third Country Transfer	If applicable	[TODO: USA, Standard Contractual Clauses]
Storage Period	How long data is stored	[TODO: 10 years]
Data Subject Rights	Access, rectification, erasure, etc.	[TODO: List all rights]
Right to Withdraw	For consent	[TODO: Withdrawable at any time]
Right to Complain	To supervisory authority	[TODO: State commissioner]
Obligation to Provide	Contractually/legally required	[TODO: Yes/No]
Automated Decision	If applicable	[TODO: No profiling]

14.2.2 Timing of Information

Information must be provided: - At the time of collection - Before processing begins - At first contact with data subject

14.3 Information Obligation for Indirect Collection (Art. 14)

14.3.1 Additional Mandatory Information

When collecting from third parties additionally:

Information	Description
Categories of Personal Data	Which data types
Source of Data	Where data comes from
Publicly Accessible Source	If applicable

14.3.2 Timing of Information

Information must be provided: - Within a reasonable period (max. 1 month) - At latest at first communication - At latest when disclosing to third parties

14.4 Exceptions to Information Obligation

14.4.1 Art. 13(4) - Already Informed

No information required when: - Data subject already has the information

14.4.2 Art. 14(5) - Exceptions for Third Party Collection

No information required when:

Exception	Prerequisite
Already Informed	Person already has information

Exception	Prerequisite
Impossible	Disproportionate effort
Legal Obligation	Explicit regulation
Professional Secrecy	Legally protected
Public Interest	Impairment of purposes

In case of impossibility/disproportionate effort: - Appropriate measures to protect rights - Public announcement - Documentation of reasons

14.5 Implementation in Our Organization

14.5.1 Privacy Notices

Privacy notices for different contexts:

Context	Document	Target Group	Update
[TODO: Website]	Website privacy notice	Website visitors	On changes
[TODO: App]	App privacy notice	App users	On changes
[TODO: Customer Account]	Customer account privacy notice	Customers	At registration
[TODO: Newsletter]	Newsletter privacy notice	Subscribers	At signup
[TODO: Application]	Applicant privacy notice	Applicants	At application
[TODO: Employee]	Employee privacy notice	Employees	At hiring

14.5.2 Forms of Provision

How information is provided:

Form	Description	Use Case
[TODO: Online]	Privacy notice on website	Website visitors
[TODO: Email]	Privacy notice by email	First contact
[TODO: Form]	Privacy notice in form	Data collection
[TODO: Sign]	Privacy notice on-site	Video surveillance
[TODO: Written]	Privacy information by mail	Contract conclusion

14.6 Checklist for Privacy Notices

14.6.1 Completeness Check

- ☐ Identity and contact details of controller
- ☐ Contact details of data protection officer

- ☐ Purposes of processing
- ☐ Legal basis of processing
- ☐ Legitimate interests (for Art. 6(1)(f))
- ☐ Recipients or categories of recipients
- ☐ Intention of third country transfer (if applicable)
- ☐ Storage period or criteria
- ☐ Data subject rights (access, rectification, erasure, etc.)
- ☐ Right to withdraw (for consent)
- ☐ Right to lodge complaint with supervisory authority
- ☐ Obligation to provide data
- ☐ Automated decision-making (if applicable)
- ☐ For third party collection: Categories of data and source

14.6.2 Quality Check

- ☐ Understandable language
- ☐ Structured presentation
- ☐ Easily accessible
- ☐ Complete and current
- ☐ Multilingual (if needed)

14.7 Documentation

14.7.1 Evidence Requirements

Document for Accountability: - All privacy notices and their versions - Time of provision - Method of provision - Exceptions and their justification - Updates and changes

14.7.2 Version Control

Version	Date	Changes	Responsible
[TODO: 1.0]	[TODO]	[TODO: Initial creation]	[TODO]
[TODO: 1.1]	[TODO]	[TODO: New processing added]	[TODO]

14.8 Links to Other Documents

- **Transparency (Art. 12):** Modalities of information
- **Data Protection Principles (Art. 5):** Transparency as core principle
- **Legal Bases (Art. 6):** Basis of processing
- **Data Subject Rights (Art. 15-22):** Information about rights
- **Records (Art. 30):** Source for information

14.9 Common Violations and Their Prevention

Violation	Example	Prevention
Incomplete Information	Missing legal basis	Use checklist
Delayed Information	Information after processing	Establish process
Incomprehensible Language	Legal jargon	Use plain language
Hidden Information	Privacy notice not findable	Prominent placement

---

Next Steps: 1. Create complete privacy notices for all contexts 2. Implement processes for timely information 3. Establish version control for privacy notices 4. Train employees on information obligations 5. Regularly review completeness and currency

ewpage

Chapter 15

Right of Access

Document-ID: 0220
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

15.1 Purpose

This document describes the implementation of the right of access in {{ meta.organization }}. Data subjects have the right to obtain information about the processing of their personal data.

15.2 Right of Access according to Art. 15 GDPR

15.2.1 Scope of Access

Data subjects have the right to information about:

Information	Description
Processing Purposes	What data is processed for
Categories of Personal Data	Which data types are processed
Recipients	Who has or will receive the data
Storage Period	How long data is stored
Right to Rectification	Right to rectification
Right to Erasure	Right to erasure
Right to Restriction	Right to restriction
Right to Object	Right to object
Right to Complain	Right to lodge complaint with supervisory authority
Source of Data	Where data comes from (for third party collection)

Information	Description
Automated Decision	Profiling and logic of processing
Third Country Transfer	Safeguards for transfer

15.2.2 Copy of Data (Art. 15(3))

Data subject has right to: - Free copy of processed data - First copy free of charge - Further copies: Reasonable fee possible

15.3 Processing Procedure

15.3.1 Process for Access Requests

Standard Process:

1. **Receipt of Request (Day 0)**
   - Registration in request system
   - Acknowledgment
   - Assignment to processor
2. **Identification (Day 1-5)**
   - Verification of identity
   - If doubts: Request additional information
   - Documentation
3. **Data Collection (Day 6-20)**
   - Identification of all systems with data
   - Compilation of information
   - Coordination with departments
   - Review of third party rights
4. **Preparation of Access (Day 21-25)**
   - Structured preparation
   - Understandable presentation
   - Completeness check
5. **Transmission (Day 26-30)**
   - Secure transmission
   - Documentation
   - Archiving

15.3.2 Deadlines

Processing Deadline: - Without delay, at most 1 month - Extension by 2 months possible for complexity - Justification of extension required

15.4 Format of Access

15.4.1 Structured Presentation

Recommended Structure:

```
1. General Information
   - Controller
   - Data Protection Officer
   - Contact details

2. Processed Data
   - Categories of personal data
   - Specific records (copy)

3. Processing Purposes
   - Purpose 1: [Description]
   - Purpose 2: [Description]

4. Legal Bases
   - Legal basis per purpose

5. Recipients
   - List of recipients or categories

6. Storage Period
   - Duration or criteria

7. Data Subject Rights
   - Rectification, erasure, restriction, objection
   - Complaint to supervisory authority

8. Source of Data
   - Source for third party collection

9. Automated Decisions
   - If applicable: Logic and significance
```

15.4.2 Forms of Transmission

Form	Description	Use Case
[TODO: Email]	PDF document by email	Standard
[TODO: Online Portal]	Access in customer portal	Customer account exists
[TODO: Written]	Paper form by mail	On request
[TODO: Electronic]	Structured format (JSON, XML)	On request

15.5 Special Considerations

15.5.1 Rights of Third Parties (Art. 15(4))

Access must not adversely affect rights of third parties: - Trade secrets - Rights of other persons - Intellectual property

Measures: - Redaction of sensitive information - Anonymization of third party data - Justification for refusal

15.5.2 Frequent Requests

For manifestly unfounded or excessive requests: - Reasonable fee possible - Refusal possible - Justification required

15.6 Documentation

15.6.1 Access Register

Date	Data Subject	Scope	Form of Transmission	Deadline	Processor
[TODO]	[TODO]	[TODO: Complete]	[TODO: Email]	[TODO: XX.XX.XXXX]	[TODO]

15.6.2 Evidence Requirements

Documentation for Accountability: - All access requests - Processing steps and times - Transmitted information - Refusals and justifications - Fees and their justification

15.7 Links to Other Documents

- **Transparency (Art. 12):** Modalities of access
- **Information Obligations (Art. 13-14):** Proactive information
- **Other Data Subject Rights (Art. 16-22):** Complementary rights
- **Records (Art. 30):** Source for access information

15.8 Common Violations and Their Prevention

Violation	Example	Prevention
Incomplete Access	Not all systems checked	Complete data collection
Deadline Exceeded	Response after 2 months	Deadline control
Incomprehensible Access	Technical raw data	Structured preparation
Missing Identification	No verification	Identification process

---

Next Steps: 1. Establish process for access requests 2. Define format and structure of access 3. Implement deadline control 4. Train employees on providing access 5. Document all requests in access register

ewpage

Chapter 16

Rectification and Erasure

Document-ID: 0230
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

16.1 Purpose

This document describes the implementation of the right to rectification and erasure in {{ meta.organization }}. Data subjects have the right to rectification of inaccurate data and erasure of data no longer necessary.

16.2 Right to Rectification (Art. 16)

16.2.1 Scope of Rectification Right

Data subjects have the right to: - Immediate rectification of inaccurate data - Completion of incomplete data - Supplementary statement

16.2.2 Rectification Process

Standard Process:

1. **Receipt of Request (Day 0)**
   - Registration
   - Acknowledgment
   - Assignment
2. **Review (Day 1-10)**
   - Identification of data subject
   - Review of inaccuracy
   - Comparison with evidence

3. **Implementation (Day 11-25)**
   - Rectification in all systems
   - Notification of recipients (Art. 19)
   - Documentation
4. **Response (Day 26-30)**
   - Information about rectification performed
   - List of notified recipients

16.2.3 Rectification Matrix

System	Responsible	Rectification Procedure	Documentation
[TODO: CRM]	IT	Manual change	Change log
[TODO: ERP]	IT	Workflow-driven	Audit trail
[TODO: Database]	IT	SQL update	Change protocol
[TODO: Backup]	IT	Marking	Backup log

16.3 Right to Erasure (Art. 17)

16.3.1 Grounds for Erasure

Erasure is required when:

Ground	Description	Example
No Longer Necessary	Purpose fulfilled	Applicant data after rejection
Withdrawal of Consent	Consent withdrawn	Newsletter unsubscribe
Objection	Objection lodged (Art. 21)	Marketing objection
Unlawful Processing	Without legal basis	Data without consent
Legal Obligation	Legal erasure obligation	Data protection violation
Children	Information society services	Social media under 16

16.3.2 Exceptions to Right of Erasure

Erasure not required for:

Exception	Description
Freedom of Expression	Exercise of right to freedom of expression
Legal Obligation	Compliance with legal obligations
Public Interest	Tasks in the public interest
Healthcare	Healthcare, occupational medicine
Archiving Purposes	Archiving in the public interest
Legal Claims	Establishment, exercise or defense

16.3.3 Erasure Process

Standard Process:

1. **Receipt of Request (Day 0)**
   - Registration
   - Acknowledgment
   - Assignment
2. **Review (Day 1-10)**
   - Identification of data subject
   - Review of erasure grounds
   - Review of exceptions
   - Review of legal retention periods
3. **Decision (Day 11-15)**
   - Erasure or reasoned refusal
   - If refusal: Review of restriction (Art. 18)
4. **Implementation (Day 16-25)**
   - Erasure in all systems
   - Notification of recipients (Art. 19)
   - Documentation
5. **Response (Day 26-30)**
   - Information about erasure or refusal
   - If refusal: Justification and remedies

16.3.4 Erasure Procedures

Technical Erasure:

System	Erasure Method	Responsible	Documentation
[TODO: Production Systems]	Immediate erasure	IT	Erasure log
[TODO: Backups]	Marking/overwriting	IT	Backup log
[TODO: Archives]	Physical destruction	IT	Destruction log
[TODO: Cloud]	API-driven erasure	IT	API log

16.4 Notification Obligation (Art. 19)

16.4.1 Notification of Recipients

Recipients must be informed of rectification or erasure:

Process: 1. Identification of all recipients 2. Notification of rectification/erasure 3. Documentation of notifications 4. Information to data subject about recipients (on request)

Exceptions: - Impossible - Disproportionate effort

16.4.2 Recipient Matrix

Recipient Type	Notification Obligation	Method	Documentation
[TODO: Processors]	Yes	Email	Notification log
[TODO: Third Party Recipients]	Yes	Email/written	Notification log

Recipient Type	Notification Obligation	Method	Documentation
[TODO: Public Authorities]	Yes	Written	Notification log

16.5 Documentation

16.5.1 Rectification and Erasure Register

Date	Data Subject	Type	Reason	Performed	Recipients Notified	Processor
[TODO]	[TODO]	Rectification	Inaccurate	Yes	Yes	[TODO]
[TODO]	[TODO]	Erasure	No longer necessary	Yes	Yes	[TODO]
[TODO]	[TODO]	Erasure	Refused (retention period)	No	N/A	[TODO]

16.5.2 Evidence Requirements

Documentation for Accountability: - All rectification and erasure requests - Performed rectifications and erasures - Refusals and their justification - Notifications to recipients - Exceptions and their justification

16.6 Deadlines

Processing Deadline: - Without delay, at most 1 month - Extension by 2 months possible for complexity - Justification of extension required

16.7 Links to Other Documents

- **Transparency (Art. 12):** Modalities of processing
- **Accuracy (Art. 5(1)(d)):** Principle of accuracy
- **Storage Limitation (Art. 5(1)(e)):** Principle of erasure
- **Notification Obligation (Art. 19):** Notification of recipients
- **Restriction (Art. 18):** Alternative to erasure

16.8 Common Violations and Their Prevention

Violation	Example	Prevention
Incomplete Rectification	Only in one system	Check all systems
Delayed Erasure	Erasure after 3 months	Deadline control

Violation	Example	Prevention
Missing Notification	Recipients not informed	Notification process
Unjustified Refusal	Refusal without review	Careful review

Next Steps: 1. Establish processes for rectification and erasure requests 2. Implement erasure procedures for all systems 3. Define notification process for recipients 4. Train employees on rectification and erasure rights 5. Document all requests in register

ewpage

Chapter 17

Restriction and Objection

Document-ID: 0240
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

17.1 Purpose

This document describes the implementation of the right to restriction of processing and the right to object in {{ meta.organization }}.

17.2 Right to Restriction (Art. 18)

17.2.1 Grounds for Restriction

Restriction is required when:

Ground	Description	Duration
Accuracy Contested	Data subject contests accuracy	Until verification
Unlawful Processing	Processing unlawful, but no erasure desired	Until clarification
No Longer Necessary	Data no longer necessary, but needed for legal claims	Until clarification
Objection Lodged	Objection according to Art. 21(1)	Until balancing of interests

17.2.2 Meaning of Restriction

During restriction: - Data may only be stored - No further processing (except storage)

Exceptions (processing permissible with consent): - Establishment of legal claims - Protection of rights of other persons - Important reasons of public interest

17.2.3 Technical Implementation

Methods for Restriction:

Method	Description	Use Case
[TODO: Marking]	Mark record as "restricted"	Standard
[TODO: Access Lock]	Technical access restriction	Sensitive data
[TODO: Separation]	Move to separate system	Long-term restriction
[TODO: Pseudonymization]	Separation of identification data	Additional protection

17.2.4 Restriction Process

Standard Process:

1. **Receipt of Request (Day 0)**
   - Registration
   - Acknowledgment
   - Assignment
2. **Review (Day 1-10)**
   - Identification of data subject
   - Review of restriction grounds
   - Identification of affected data
3. **Implementation (Day 11-25)**
   - Technical restriction in all systems
   - Notification of recipients (Art. 19)
   - Documentation
4. **Response (Day 26-30)**
   - Information about restriction performed
   - Information about lifting of restriction

17.2.5 Lifting of Restriction

Restriction is lifted when: - Reason for restriction no longer applies - Data subject consents - Restriction reason clarified

Before lifting: - Information to data subject required - Documentation of lifting

17.3 Right to Object (Art. 21)

17.3.1 Objection to Processing (Art. 21(1))

Right to object for: - Processing based on public interest (Art. 6(1)(e)) - Processing based on legitimate interests (Art. 6(1)(f))

Consequence of Objection: - Processing must be stopped - Unless: Compelling legitimate grounds override

17.3.2 Balancing of Interests

Assessment After Objection:

Criterion	Assessment Question	Evaluation
Compelling Grounds	Are there compelling legitimate grounds?	[TODO]
Legal Claims	Are legal claims affected?	[TODO]
Interests of Person	What interests does the data subject have?	[TODO]
Balancing	Do controller's grounds override?	[TODO]

Result: - Compelling grounds override: Processing permissible - No compelling grounds: Stop processing

17.3.3 Objection to Direct Marketing (Art. 21(2))

Special Features: - Absolute right to object - No balancing of interests required - Processing must be stopped immediately

Implementation: - Entry in suppression list - No further advertising - Information to all marketing channels

17.3.4 Objection to Profiling (Art. 21(3))

Right to object for: - Profiling in connection with direct marketing - Profiling based on legitimate interests

17.3.5 Objection Process

Standard Process:

1. **Receipt of Objection (Day 0)**
   - Registration
   - Acknowledgment
   - Immediate stop for direct marketing
2. **Review (Day 1-15)**
   - Identification of data subject
   - Review of legal basis
   - For Art. 6(1)(f): Balancing of interests
3. **Decision (Day 16-20)**
   - Stop processing or
   - Reasoned refusal (compelling grounds)
4. **Implementation (Day 21-25)**
   - Stop in all systems
   - Notification of recipients
   - Documentation
5. **Response (Day 26-30)**
   - Information about stop or refusal
   - If refusal: Justification and remedies

17.4 Notification Obligation (Art. 19)

17.4.1 Notification of Recipients

Recipients must be informed of restriction or objection: - Processors - Third party recipients - Public authorities

Exceptions: - Impossible - Disproportionate effort

17.5 Documentation

17.5.1 Restriction and Objection Register

Date	Data Subject	Type	Reason	Status	Lifting	Processor
[TODO]	[TODO]	Restriction	Accuracy contested	Active	[TODO]	[TODO]
[TODO]	[TODO]	Objection	Direct marketing	Implemented	N/A	[TODO]
[TODO]	[TODO]	Objection	Legitimate interest	Refused	N/A	[TODO]

17.5.2 Evidence Requirements

Documentation for Accountability: - All restriction and objection requests - Performed restrictions - Balancing of interests for objections - Refusals and their justification - Notifications to recipients - Lifting of restrictions

17.6 Links to Other Documents

- **Transparency (Art. 12):** Modalities of processing
- **Legitimate Interests (Art. 6(1)(f)):** Balancing of interests
- **Notification Obligation (Art. 19):** Notification of recipients
- **Erasure (Art. 17):** Alternative to restriction

17.7 Common Violations and Their Prevention

Violation	Example	Prevention
No Restriction	Continued processing despite request	Immediate implementation
Missing Balancing	Refusal without review	Careful balancing
Delayed Implementation	Advertising after objection	Immediate stop
No Notification	Recipients not informed	Notification process

Next Steps: 1. Establish processes for restriction and objection requests 2. Implement technical restriction mechanisms 3. Define balancing of interests process 4. Train employees on restriction and objection rights 5. Document all requests in register

ewpage

Chapter 18

Data Portability

Document-ID: 0250
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

18.1 Purpose

This document describes the implementation of the right to data portability in {{ meta.organization }}. Data subjects have the right to receive their data in a structured, commonly used and machine-readable format.

18.2 Right to Data Portability (Art. 20)

18.2.1 Prerequisites

Data portability applies only when:

Prerequisite	Description
Legal Basis	Consent (Art. 6(1)(a)) or contract (Art. 6(1)(b))
Provision	Data was provided by data subject
Automated Processing	Processing is automated

Not applicable for: - Processing based on other legal bases (lit. c, d, e, f) - Non-automated processing - Data not provided by data subject

18.2.2 Scope of Data Portability

Affected Data:

Data Type	Portable?	Justification
Provided by Person	Yes	Directly entered or uploaded
Generated by Observation	Yes	Usage data, location data
Derived/calculated Data	No	Algorithms, analyses, profiles
Third Party Data	No	Third party rights affected

18.2.3 Two Variants

1. Transfer to Data Subject: - Provision in structured format - Common format (CSV, JSON, XML) - Machine-readable

2. Direct Transfer to Another Controller: - Where technically feasible - Direct transmission - No obligation if interface missing

18.3 Technical Implementation

18.3.1 Data Formats

Supported Formats:

Format	Description	Use Case
[TODO: JSON]	JavaScript Object Notation	Standard for structured data
[TODO: CSV]	Comma-Separated Values	Tabular data
[TODO: XML]	Extensible Markup Language	Hierarchical data
[TODO: PDF]	Portable Document Format	Readable presentation (additional)

18.3.2 Data Structure

Example JSON Structure:

```
{
  "export_date": "2024-01-15",
  "data_subject": {
    "id": "12345",
    "name": "John Doe",
    "email": "john@example.com"
  },
  "personal_data": {
    "profile": {
      "created": "2020-01-01",
      "last_updated": "2024-01-10",
      "fields": {
        "name": "John Doe",
        "email": "john@example.com",
        "phone": "+1234567890"
      }
```

```
    },
    "orders": [
      {
        "order_id": "ORD-001",
        "date": "2023-12-01",
        "items": [...]
      }
    ],
    "usage_data": {
      "logins": [...],
      "page_views": [...]
    }
  }
}
```

18.3.3 Interfaces

Technical Transfer Options:

Method	Description	Implementation
[TODO: Download Portal]	Self-service portal	Web interface
[TODO: API]	Programmatic interface	REST API
[TODO: Email]	Send as attachment	Encrypted
[TODO: Direct Transfer]	To another controller	API-to-API

18.4 Transfer Process

18.4.1 Process for Data Portability Requests

Standard Process:

1. **Receipt of Request (Day 0)**
   - Registration
   - Acknowledgment
   - Clarification: To person or another controller?
2. **Review (Day 1-10)**
   - Identification of data subject
   - Review of prerequisites
   - Identification of portable data
3. **Data Export (Day 11-20)**
   - Compilation of data
   - Conversion to desired format
   - Quality check
4. **Transfer (Day 21-25)**
   - Provision for download or
   - Direct transfer to another controller
   - Documentation
5. **Response (Day 26-30)**

- Information about provision
- Access link or confirmation of transfer

18.4.2 Direct Transfer

Process for Direct Transfer:

1. **Identification of Recipient**
   - Name and contact details
   - Technical interface
2. **Review of Technical Feasibility**
   - Availability of interfaces
   - Compatibility of formats
3. **Implementation of Transfer**
   - Secure transmission
   - Confirmation of receipt
   - Documentation

If technically not feasible: - Provision to data subject - Information about missing interface

18.5 Exceptions and Limitations

18.5.1 Rights and Freedoms of Others (Art. 20(4))

Data portability must not adversely affect: - Rights and freedoms of other persons - Trade secrets - Intellectual property

Measures: - Anonymization of third party data - Exclusion of protected information - Justification for limitation

18.5.2 No Erasure Obligation

Data portability does not mean: - Automatic erasure at controller - Termination of processing - Separate erasure request required

18.6 Documentation

18.6.1 Data Portability Register

Date	Data Subject	Format	Recipient	Scope	Status	Processor
[TODO]	[TODO]	JSON	Data subject	Complete	Provided	[TODO]
[TODO]	[TODO]	CSV	Another controller	Complete	Transferred	[TODO]
[TODO]	[TODO]	JSON	Data subject	Partial (third party rights)	Provided	[TODO]

18.6.2 Evidence Requirements

Documentation for Accountability: - All data portability requests - Provided data and formats - Direct transfers - Limitations and their justification - Technical feasibility assessments

18.7 Deadlines

Processing Deadline: - Without delay, at most 1 month - Extension by 2 months possible for complexity - Justification of extension required

18.8 Links to Other Documents

- **Transparency (Art. 12):** Modalities of transfer
- **Legal Bases (Art. 6):** Prerequisites for portability
- **Information Obligations (Art. 13-14):** Information about right
- **Right of Access (Art. 15):** Complementary right

18.9 Common Violations and Their Prevention

Violation	Example	Prevention
Unstructured Format	PDF scan	Machine-readable format
Incomplete Data	Only master data	All portable data
Missing Interface	No direct transfer	Provide API
Delayed Provision	Provision after 3 months	Deadline control

Next Steps: 1. Establish process for data portability requests 2. Implement export in structured formats 3. Develop interfaces for direct transfer 4. Train employees on data portability 5. Document all requests in register

ewpage

Chapter 19

Controller: Obligations and Accountability

Document-ID: 0300
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

19.1 Purpose

This document describes the controller's obligations according to Art. 24 GDPR and the implementation of accountability at {{ meta.organization }}. It documents how we ensure that processing of personal data complies with GDPR.

19.2 Accountability (Art. 24(1))

The controller is responsible for compliance with data protection principles and must be able to demonstrate compliance (accountability).

19.2.1 Demonstration of Compliance

Documentation for demonstration:

Document	Purpose	Update Frequency	Responsible
Records of Processing Activities	Art. 30 Compliance	Ongoing	[TODO: Role]
Data Protection Impact Assessments	Art. 35 Compliance	As needed	[TODO: Role]

Document	Purpose	Update Frequency	Responsible
Processor Agreements	Art. 28 Compliance	Upon contract	[TODO: Role]
TOM Documentation	Art. 32 Compliance	Annually	[TODO: Role]
Training Records	Art. 39 Compliance	Ongoing	[TODO: Role]
Data Breach Register	Art. 33 Compliance	Upon incidents	[TODO: Role]

19.3 Technical and Organizational Measures (TOM)

19.3.1 Risk-Based Approach

Measures consider: - **Nature of processing:** [TODO: Describe processing types] - **Scope of processing:** [TODO: Volume, number of data subjects] - **Context of processing:** [TODO: Context, technology] - **Purposes of processing:** [TODO: Processing purposes] - **Likelihood and severity of risk:** [TODO: Risk assessment]

19.3.2 Implemented Measures

19.3.2.1 Technical Measures

Measure	Description	Implementation Status	Responsible
Access Controls	[TODO: Description]	Implemented/Planned	[TODO: Role]
Encryption	[TODO: Description]	Implemented/Planned	[TODO: Role]
Pseudonymization	[TODO: Description]	Implemented/Planned	[TODO: Role]
Logging and Monitoring	[TODO: Description]	Implemented/Planned	[TODO: Role]
Backup and Recovery	[TODO: Description]	Implemented/Planned	[TODO: Role]

19.3.2.2 Organizational Measures

Measure	Description	Implementation Status	Responsible
Data Protection Policies	[TODO: Description]	Implemented/Planned	[TODO: Role]
Training Program	[TODO: Description]	Implemented/Planned	[TODO: Role]

Measure	Description	Implementation Status	Responsible
Incident Response Plan	[TODO: Description]	Implemented/Planned	[TODO: Role]
Access Management	[TODO: Description]	Implemented/Planned	[TODO: Role]
Confidentiality Commitments	[TODO: Description]	Implemented/Planned	[TODO: Role]

19.4 Data Protection by Design (Art. 25(1))

19.4.1 Privacy by Design

Principles: - Data protection as default setting - Data minimization from the start - Pseudonymization where possible - Transparency in processing - User-friendly data protection features

Implementation in Projects:

Project Phase	Data Protection Measures	Responsible
Requirements Analysis	[TODO: Measures]	[TODO: Role]
Design	[TODO: Measures]	[TODO: Role]
Implementation	[TODO: Measures]	[TODO: Role]
Testing	[TODO: Measures]	[TODO: Role]
Deployment	[TODO: Measures]	[TODO: Role]

19.5 Data Protection by Default (Art. 25(2))

19.5.1 Privacy by Default

Default Settings: - Only necessary data processed by default - Minimal storage duration as default - Restricted access as default - Opt-in instead of opt-out for non-necessary processing

Examples:

System/Process	Default Setting	Justification
[TODO: System]	[TODO: Setting]	[TODO: Justification]

19.6 Codes of Conduct and Certification

19.6.1 Codes of Conduct (Art. 40)

Status: [TODO: Participation in codes of conduct? Yes/No]
Code of Conduct: [TODO: Name, Reference]

19.6.2 Certification (Art. 42)

Status: [TODO: Data protection certification available? Yes/No]
Certification: [TODO: Type of certification, Validity]

19.7 Review and Update of Measures

19.7.1 Regular Review

Review Cycles: - **Annual Review:** Complete assessment of all TOM - **Quarterly Review:** Critical systems and high-risk processing - **Ad-hoc Review:** Upon security incidents, new threats, system changes

19.7.2 Update Process

1. **Identification:** Recognize new risks or vulnerabilities
2. **Assessment:** Check appropriateness of existing measures
3. **Planning:** Plan additional or improved measures
4. **Implementation:** Implement measures
5. **Documentation:** Document changes
6. **Verification:** Validate effectiveness of measures

19.8 Documentation and Demonstration

19.8.1 Mandatory Documents

- **Records of Processing Activities (Art. 30)**
- **Data Protection Impact Assessments (Art. 35)**
- **Processor Agreements (Art. 28)**
- **TOM Documentation (Art. 32)**
- **Consent Records (Art. 7)**
- **Information Records (Art. 13, 14)**

19.8.2 Retention Periods

Document	Retention Period	Legal Basis
Processing Records	During operation + 3 years	Art. 30
DPIA	During operation + 3 years	Art. 35
DPA	Contract duration + 3 years	Art. 28
Breach Documentation	3 years	Art. 33

19.9 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
TOM Implementation	[TODO]	[TODO]	[TODO]	[TODO]
TOM Review	[TODO]	[TODO]	[TODO]	[TODO]

Task	Responsible	Accountable	Consulted	Informed
Documentation	[TODO]	[TODO]	[TODO]	[TODO]
Demonstration	[TODO]	[TODO]	[TODO]	[TODO]

19.10 Links to Other Documents

- **Data Protection Principles (Art. 5):** Basis for all measures
- **Security of Processing (Art. 32):** Detailed technical measures
- **Data Protection Impact Assessment (Art. 35):** Risk assessment
- **Processing by Processor (Art. 28):** Responsibilities with processors

---

Next Steps: 1. Document all implemented technical and organizational measures 2. Create a review plan for regular TOM audits 3. Implement Privacy by Design and Privacy by Default in all projects 4. Ensure all evidence documents are current and available 5. Define clear responsibilities for accountability

ewpage

Chapter 20

Processing by Processor

Document-ID: 0310
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

20.1 Purpose

This document regulates processing by processor at {{ meta.organization }} according to Art. 28 GDPR. It defines requirements for processors, contract design, and control mechanisms.

20.2 Processor Register

20.2.1 Active Processors

Processor	Service	Processed Data	DPA Date	Next Review
[TODO: Name]	[TODO: Service]	[TODO: Data Categories]	[TODO: Date]	[TODO: Date]

20.2.2 Categories of Processors

- **IT Service Providers:** [TODO: e.g., Cloud providers, Hosting]
- **HR Service Providers:** [TODO: e.g., Payroll, Recruiting]
- **Marketing Service Providers:** [TODO: e.g., Email marketing, CRM]
- **Support Service Providers:** [TODO: e.g., Helpdesk, Call center]
- **Others:** [TODO: Other categories]

20.3 Requirements for Processors (Art. 28(1))

20.3.1 Selection Criteria

The processor must provide sufficient guarantees to implement appropriate technical and organizational measures.

Assessment Criteria:

Criterion	Description	Assessment Method
Expertise	Data protection expertise	Certificates, References
Reliability	Proven compliance	Audits, Reports
Resources	Sufficient capacities	Documentation, Evidence
TOM	Appropriate security measures	TOM Documentation
Certifications	ISO 27001, SOC 2, etc.	Certificates

20.3.2 Selection Process

1. **Needs Analysis:** Define requirements
2. **Market Analysis:** Identify potential providers
3. **Pre-selection:** Based on selection criteria
4. **Due Diligence:** Detailed review
5. **Contract Negotiation:** DPA conclusion
6. **Approval:** By Data Protection Officer
7. **Onboarding:** Integration and training

20.4 Data Processing Agreement (DPA)

20.4.1 Mandatory Content per Art. 28(3)

The agreement must regulate the following:

20.4.1.1 1. Subject Matter and Duration

- **Subject Matter:** [TODO: Type of processing]
- **Duration:** [TODO: Contract term]
- **Nature and Purpose of Processing:** [TODO: Description]

20.4.1.2 2. Type of Personal Data

- **Data Categories:** [TODO: e.g., Contact data, Contract data]
- **Categories of Data Subjects:** [TODO: e.g., Customers, Employees]

20.4.1.3 3. Obligations and Rights of Controller

- Right to issue instructions
- Right to control
- Right to information
- Right to deletion

20.4.1.4 4. Obligations of Processor

According to Art. 28(3)(a)-(h):

Obligation	Description	Implementation
a) Instructions	Process only on documented instructions	[TODO: Process]
b) Confidentiality	Commitment to confidentiality	[TODO: Evidence]
c) Security	Measures according to Art. 32	[TODO: TOM Documentation]
d) Sub-processors	Authorization and conditions	[TODO: Process]
e) Data Subject Rights	Support with requests	[TODO: Process]
f) Support	With compliance obligations	[TODO: Agreement]
g) Deletion/Return	After contract end	[TODO: Process]
h) Demonstration	Make information available	[TODO: Reporting]

20.4.2 Contract Template

Standard DPA Template: [TODO: Link to template]
Approval Process: [TODO: Describe approval process]

20.5 Sub-Processors (Art. 28(2), (4))

20.5.1 Authorization Procedure

Authorization Type: [TODO: General or specific authorization]

20.5.1.1 General Authorization

- List of authorized sub-processors maintained
- Information obligation upon changes
- Controller's right to object

20.5.1.2 Specific Authorization

- Individual case authorization required
- Review before engagement
- Documentation of authorization

20.5.2 Sub-Processor Register

Sub-Processor	Main Processor	Service	Authorization Date
[TODO: Name]	[TODO: Name]	[TODO: Service]	[TODO: Date]

20.6 Control and Monitoring

20.6.1 Control Rights (Art. 28(3)(h))

Control Measures: - On-site audits - Document review - Certificate review - Questionnaire assessments - Penetration tests

20.6.2 Control Plan

Processor	Control Type	Frequency	Next Control	Responsible
[TODO: Name]	[TODO: Type]	[TODO: Frequency]	[TODO: Date]	[TODO: Role]

20.6.3 Audit Checklist

- ☐ DPA complete and current
- ☐ TOM documentation available and appropriate
- ☐ Sub-processors authorized
- ☐ Certifications valid
- ☐ Incident response process defined
- ☐ Training records available
- ☐ Data deletion/return regulated
- ☐ Insurance coverage sufficient

20.7 Instructions

20.7.1 Issuing Instructions

Authorized Persons: - [TODO: Role/Name] - [TODO: Role/Name]

Form of Instructions: - Written (email, document) - Documented and traceable - With date and signature

20.7.2 Instruction Register

Date	Processor	Instruction	Issued By	Status
[TODO]	[TODO: Name]	[TODO: Content]	[TODO: Person]	Implemented/Open

20.8 Data Breaches

20.8.1 Processor's Notification Obligation

The processor must inform the controller without undue delay about data breaches.

Notification Process: 1. Immediate notification to: [TODO: Contact] 2. Information: Type of breach, affected data, measures 3. Deadline: Within [TODO: e.g., 24 hours]

20.8.2 Incident Response Coordination

- Joint incident response plans
- Regular tests and exercises
- Clear communication channels
- Documentation of incidents

20.9 Contract End

20.9.1 Deletion or Return (Art. 28(3)(g))

After Contract End:

Data Type	Measure	Deadline	Evidence
[TODO: Data Type]	Deletion/Return	[TODO: Deadline]	[TODO: Evidence]

Deletion Certificate: [TODO: Describe certification procedure]

20.9.2 Offboarding Process

1. Contract end notification
2. Data return or deletion
3. Revoke access rights
4. Obtain deletion certificate
5. Complete documentation

20.10 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
DPA Conclusion	[TODO]	[TODO]	[TODO]	[TODO]
Control	[TODO]	[TODO]	[TODO]	[TODO]
Issuing Instructions	[TODO]	[TODO]	[TODO]	[TODO]
Incident Management	[TODO]	[TODO]	[TODO]	[TODO]

20.11 Links to Other Documents

- **Controller Obligations (Art. 24):** Overall responsibility
- **Security of Processing (Art. 32):** TOM requirements
- **Data Breaches (Art. 33):** Notification obligations
- **Records of Processing Activities (Art. 30):** Documentation

---

Next Steps: 1. Create a complete register of all processors 2. Review all existing contracts for GDPR compliance 3. Implement a control plan for regular audits 4. Define instruction processes and authorizations 5. Establish an instruction register

ewpage

Chapter 21

Records of Processing Activities

Document-ID: 0320
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

21.1 Purpose

This document is the records of processing activities according to Art. 30 GDPR for {{ meta.organization }}. It systematically documents all processing of personal data and serves as evidence of compliance.

21.2 Obligation to Maintain Records

Applicability: [TODO: Check exception for < 250 employees per Art. 30(5)]

21.2.1 Exceptions (Art. 30(5))

The obligation does not apply to enterprises with fewer than 250 employees, unless: - The processing is likely to result in a risk to the rights and freedoms of data subjects - The processing is not occasional - The processing includes special categories (Art. 9) or criminal data (Art. 10)

Status for our organization: [TODO: Obligation applies / Exception does not apply]

21.3 Records for Controllers (Art. 30(1))

21.3.1 Processing Activity 1: [TODO: Name of Processing]

21.3.1.1 a) Name and Contact Details

- **Controller:** [TODO: Name, Address, Contact]

- **Representative (if applicable):** [TODO: Name, Address, Contact]
- **Data Protection Officer:** [TODO: Name, Contact]

21.3.1.2 b) Purposes of Processing

- **Main Purpose:** [TODO: e.g., Customer management]
- **Further Purposes:** [TODO: e.g., Marketing, Analysis]

21.3.1.3 c) Categories of Data Subjects

- [TODO: e.g., Customers]
- [TODO: e.g., Prospects]
- [TODO: e.g., Supplier contacts]

21.3.1.4 d) Categories of Personal Data

- **Master Data:** [TODO: e.g., Name, Address, Date of birth]
- **Contact Data:** [TODO: e.g., Email, Phone]
- **Contract Data:** [TODO: e.g., Customer number, Orders]
- **Payment Data:** [TODO: e.g., Bank details]
- **Special Categories (Art. 9):** [TODO: if applicable]

21.3.1.5 e) Categories of Recipients

- **Internal Recipients:** [TODO: e.g., Sales, Accounting]
- **External Recipients:** [TODO: e.g., Payment service providers]
- **Processors:** [TODO: e.g., Cloud providers]
- **Third Countries:** [TODO: if applicable]

21.3.1.6 f) Third Country Transfers

- **Third Country:** [TODO: Country]
- **Legal Basis:** [TODO: Art. 45/46/49]
- **Safeguards:** [TODO: e.g., Standard Contractual Clauses, BCR]
- **Documentation:** [TODO: Reference to document]

21.3.1.7 g) Erasure Deadlines

- **Standard Case:** [TODO: e.g., 3 years after contract end]
- **Legal Retention Obligations:** [TODO: e.g., 10 years commercial law]
- **Erasure Concept:** [TODO: Reference to document]

21.3.1.8 h) Technical and Organizational Measures (Art. 32)

- **Access Controls:** [TODO: Description]
- **Access Management:** [TODO: Description]
- **Encryption:** [TODO: Description]
- **Pseudonymization:** [TODO: Description]
- **Further Measures:** [TODO: Reference to TOM documentation]

21.3.2 Processing Activity 2: [TODO: Name of Processing]

[TODO: Repeat structure for each processing activity]

21.4 Records for Processors (Art. 30(2))

If {{ meta.organization }} acts as processor:

21.4.1 Processing Activity 1: [TODO: Name]

21.4.1.1 a) Name and Contact Details

- **Processor:** [TODO: Name, Address, Contact]
- **Controller(s):** [TODO: Name, Address, Contact]
- **Representative (if applicable):** [TODO: Name, Address, Contact]
- **Data Protection Officer:** [TODO: Name, Contact]

21.4.1.2 b) Categories of Processing

- [TODO: e.g., Hosting, Payroll, Email marketing]

21.4.1.3 c) Third Country Transfers

- **Third Country:** [TODO: Country]
- **Legal Basis:** [TODO: Art. 45/46/49]
- **Safeguards:** [TODO: e.g., Standard Contractual Clauses]

21.4.1.4 d) Technical and Organizational Measures (Art. 32)

- [TODO: Reference to TOM documentation]

21.5 Overview of All Processing Activities

ID	Processing	Purpose	Legal Basis	Data Subjects	Data Categories	Erasure Deadline
P001	[TODO]	[TODO]	Art. 6(1) lit. [TODO]	[TODO]	[TODO]	[TODO]
P002	[TODO]	[TODO]	Art. 6(1) lit. [TODO]	[TODO]	[TODO]	[TODO]

21.6 Maintenance and Updates

21.6.1 Update Process

Triggers for Updates: - New processing activity - Change to existing processing - Termination of processing - Change of processors - Change of third country transfers

Process: 1. Identify change 2. Update records 3. Inform Data Protection Officer 4. File documentation 5. Update version

21.6.2 Responsibilities

Task	Responsible	Frequency
Records Maintenance	[TODO: Data Protection Coordinator]	Ongoing
Review	[TODO: Data Protection Officer]	Quarterly
Approval	[TODO: Management]	Upon significant changes

21.7 Provision to Supervisory Authority

The records are made available to the supervisory authority upon request.

Format: [TODO: e.g., PDF, Excel]
Provision Deadline: Without undue delay upon request
Responsible: [TODO: Data Protection Officer]

21.8 Links to Other Documents

- **Data Protection Impact Assessment (Art. 35):** For high-risk processing
- **Processor Agreements (Art. 28):** Details on processors
- **TOM Documentation (Art. 32):** Detailed security measures
- **Erasure Concept:** Detailed erasure deadlines and processes

---

Next Steps: 1. Systematically record all processing activities 2. Document all mandatory information per Art. 30 3. Implement an update process 4. Train employees to report new processing 5. Review records regularly for completeness

ewpage

Chapter 22

Data Breaches and Notification Obligation

Document-ID: 0330
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

22.1 Purpose

This document regulates handling of data breaches at {{ meta.organization }} according to Art. 33-34 GDPR. It defines notification obligations, deadlines, and processes for managing data protection incidents.

22.2 Definition of Data Breach (Art. 4(12))

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

22.2.1 Categories of Data Breaches

Category	Description	Examples
Confidentiality Breach	Unauthorized disclosure or access	Data leak, hacking, accidental disclosure
Integrity Breach	Unauthorized alteration	Manipulation, data corruption
Availability Breach	Loss or destruction	Ransomware, hardware failure, accidental deletion

22.3 Notification to Supervisory Authority (Art. 33)

22.3.1 Principle (Art. 33(1))

The controller notifies a personal data breach to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

22.3.2 Risk Assessment

Criteria for Risk Assessment:

Criterion	Low Risk	High Risk
Type of Data	General contact data	Special categories (Art. 9), Financial data
Scope	Few data subjects	Many data subjects
Severity	Minor impact	Severe impact
Protective Measures	Encrypted, pseudonymized	Unencrypted, plaintext
Data Subjects	Employees (internal)	Customers, Children, vulnerable groups

Decision Tree: 1. Is there a data breach? → Yes/No 2. Is there a risk to rights and freedoms? → Yes/No 3. If Yes: Notification required 4. If high risk: Additionally notify data subjects

22.3.3 Mandatory Content of Notification (Art. 33(3))

The notification must contain at least the following information:

22.3.3.1 a) Nature of Breach

- Description of the data breach
- Categories and approximate number of data subjects concerned
- Categories and approximate number of data records concerned

22.3.3.2 b) Contact Point

- Name and contact details of the Data Protection Officer or other contact point

22.3.3.3 c) Description of Consequences

- Description of the likely consequences of the data breach

22.3.3.4 d) Measures Taken

- Description of measures taken or proposed to address and mitigate the breach

22.3.4 Notification Deadline

72-Hour Deadline from Awareness

Time	Action
T+0 (Discovery)	Activate incident response, initial assessment
T+24h	Risk assessment completed, notification obligation clarified
T+48h	Notification prepared
T+72h	Notification submitted to supervisory authority

If 72-Hour Deadline Exceeded: - Justification for delay required (Art. 33(1))

22.3.5 Competent Supervisory Authority

Supervisory Authority: [TODO: Name of competent authority]
Address: [TODO: Address]
Notification Portal: [TODO: URL to online notification form]
Contact: [TODO: Email, Phone]

22.4 Communication to Data Subjects (Art. 34)

22.4.1 Notification Obligation (Art. 34(1))

When the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller communicates the breach to the data subject without undue delay.

22.4.2 Criteria for High Risk

- **Special categories of personal data (Art. 9)**
- **Financial data, access credentials**
- **Large number of data subjects**
- **Vulnerable groups (children, patients)**
- **Severe consequences (identity theft, financial losses)**

22.4.3 Content of Communication (Art. 34(2))

The communication must contain:

- Nature of the data breach
- Name and contact details of the Data Protection Officer
- Likely consequences of the data breach
- Measures taken or proposed to address and mitigate the breach
- Recommendations for data subjects (e.g., change password)

22.4.4 Exceptions from Communication (Art. 34(3))

No communication required if:

a) Protective Measures: Data was encrypted or otherwise protected
b) Subsequent Measures: Measures taken that eliminate high risk
c) Disproportionate Effort: Public communication instead

22.5 Incident Response Process

22.5.1 Phase 1: Detection and Assessment

Timeframe: 0-4 hours

1. Detect and report incident
2. Activate incident response team
3. Conduct initial assessment
4. Confirm data breach

Responsible: [TODO: IT Security, Data Protection Officer]

22.5.2 Phase 2: Containment

Timeframe: 4-12 hours

1. Immediate measures for damage control
2. Isolate affected systems
3. Prevent further data loss
4. Forensic preservation

Responsible: [TODO: IT Security]

22.5.3 Phase 3: Analysis and Risk Assessment

Timeframe: 12-24 hours

1. Determine scope of breach
2. Identify affected data and persons
3. Conduct risk assessment
4. Check notification obligation

Responsible: [TODO: Data Protection Officer, IT Security]

22.5.4 Phase 4: Notification and Communication

Timeframe: 24-72 hours

1. Notification to supervisory authority (if required)
2. Communication to data subjects (if required)
3. Internal communication
4. External communication (if required)

Responsible: [TODO: Data Protection Officer, Management]

22.5.5 Phase 5: Recovery

Timeframe: 72 hours - weeks

1. Restore systems
2. Close security gaps
3. Implement preventive measures
4. Enhance monitoring

Responsible: [TODO: IT Security]

22.5.6 Phase 6: Post-Incident Review

Timeframe: After completion

1. Document incident
2. Conduct lessons learned
3. Adapt processes
4. Update training

Responsible: [TODO: Data Protection Officer, IT Security]

22.6 Documentation Obligation (Art. 33(5))

The controller documents all data breaches, including all facts, effects, and remedial action taken.

22.6.1 Breach Register

Date	Type of Breach	Affected Data	Number of Data Subjects	Risk	Notified	Communicated	Status
[TODO]	[TODO]	[TODO]	[TODO]	Low/High	Yes/No	Yes/No	Open/Closed

22.6.2 Retention Period

Documentation: At least 3 years after incident closure

22.7 Communication Plans

22.7.1 Internal Communication

Escalation Chain: 1. Discoverer → IT Security 2. IT Security → Data Protection Officer 3. Data Protection Officer → Management 4. Management → Supervisory Board (for severe incidents)

22.7.2 External Communication

Stakeholders: - Supervisory authority - Data subjects - Media (for public interest) - Business partners (if affected) - Insurance

Communication Responsible: [TODO: Role]

22.8 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
Incident Detection	[TODO]	[TODO]	[TODO]	[TODO]
Risk Assessment	[TODO]	[TODO]	[TODO]	[TODO]
Notification to Authority	[TODO]	[TODO]	[TODO]	[TODO]

Task	Responsible	Accountable	Consulted	Informed
Communication to Data Subjects	[TODO]	[TODO]	[TODO]	[TODO]
Documentation	[TODO]	[TODO]	[TODO]	[TODO]

22.9 Links to Other Documents

- **Security of Processing (Art. 32):** Preventive measures
- **Processing by Processor (Art. 28):** Processor notification obligation
- **Data Protection Impact Assessment (Art. 35):** Risk assessment
- **Incident Response Plan:** Detailed technical processes

Next Steps: 1. Implement an incident response process 2. Define escalation paths and responsibilities 3. Create templates for notifications and communications 4. Conduct regular incident response exercises 5. Establish a breach register

ewpage

Chapter 23

Data Protection Officer

Document-ID: 0340
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

23.1 Purpose

This document regulates the role, tasks, and position of the Data Protection Officer at {{ meta.organization }} according to Art. 37-39 GDPR.

23.2 Designation Obligation (Art. 37)

23.2.1 Assessment of Designation Obligation

The controller designates a Data Protection Officer if:

23.2.1.1 a) Public Authority or Body (Art. 37(1)(a))

Status: [TODO: Yes/No]
Justification: [TODO: Description]

23.2.1.2 b) Core Activities Consist of Regular and Systematic Monitoring (Art. 37(1)(b))

Criteria: - Core activity of the organization - Large-scale processing - Regular and systematic - Monitoring of data subjects

Status: [TODO: Yes/No]
Justification: [TODO: e.g., Online tracking, Profiling, Behavior monitoring]

23.2.1.3 c) Core Activities Consist of Large-Scale Processing of Special Categories (Art. 37(1)(c))

Special Categories (Art. 9): - Health data - Genetic/biometric data - Racial/ethnic origin - Political opinions - Religious beliefs - Trade union membership - Sex life/sexual orientation

Status: [TODO: Yes/No]
Justification: [TODO: Description of processing]

23.2.1.4 d) National Regulations

Germany (§ 38 BDSG): Designation obligation from 20 persons regularly engaged in automated processing

Status: [TODO: Number of persons, Designation obligation Yes/No]

23.2.2 Result of Assessment

Designation Obligation: [TODO: Yes/No]
Legal Basis: [TODO: Art. 37(1)(a)/(b)/(c) or national regulation]
Voluntary Designation: [TODO: If no obligation but voluntarily designated]

23.3 Designation of Data Protection Officer

23.3.1 Data Protection Officer

Name: [TODO: Name]
Type: [TODO: Internal/External]
Contact: - Email: [TODO: dataprotection@organization.com] - Phone: [TODO: Phone number] - Address: [TODO: Postal address]

Designation Date: [TODO: Date]
Publication: [TODO: Published internally (intranet) and externally (website)]

23.3.2 Publication of Contact Details (Art. 37(7))

The contact details of the Data Protection Officer are published and communicated to the supervisory authority.

Publication Locations: - Website: [TODO: URL] - Intranet: [TODO: URL] - Privacy Policy: [TODO: URL] - Notice Board: [TODO: Locations]

Communication to Supervisory Authority: [TODO: Date of communication]

23.4 Qualification and Expertise (Art. 37(5))

23.4.1 Required Qualifications

The Data Protection Officer is designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

Expertise in the following areas:

Area	Qualification	Evidence
Data Protection Law	[TODO: e.g., Certification, Studies]	[TODO: Certificate]
IT Security	[TODO: Knowledge]	[TODO: Evidence]
Industry Knowledge	[TODO: Experience in the industry]	[TODO: References]
Business Operations	[TODO: Understanding of organization]	[TODO: Experience]

Certifications: - [TODO: e.g., TÜV-certified Data Protection Officer] - [TODO: e.g., GDD Certification] - [TODO: e.g., CIPP/E (Certified Information Privacy Professional)]

23.4.2 Continuing Education

Training Program: - Regular participation in data protection seminars - Professional literature and newsletters - Participation in conferences - Exchange with other Data Protection Officers

Budget: [TODO: Annual training budget]

23.5 Position of Data Protection Officer (Art. 38)

23.5.1 Proper Involvement (Art. 38(1))

The controller ensures that the Data Protection Officer is properly and in a timely manner involved in all issues relating to the protection of personal data.

Involvement in: - Strategic decisions - New projects and systems - Contract negotiations with processors - Data protection impact assessments - Incident response

23.5.2 Support and Resources (Art. 38(2))

Provided Resources:

Resource	Description	Status
Personnel	[TODO: e.g., Data protection team]	[TODO: Number of persons]
Budget	[TODO: Annual budget]	[TODO: Amount]
Facilities	[TODO: Office, Meeting rooms]	[TODO: Available]
IT Systems	[TODO: Software, Tools]	[TODO: Available]
Training	[TODO: Training budget]	[TODO: Amount]
Access to Information	[TODO: Access to systems, documents]	[TODO: Granted]

23.5.3 Independence (Art. 38(3))

The Data Protection Officer does not receive any instructions regarding the exercise of their tasks.

Ensuring Independence: - Direct reporting line to management - No instructions regarding data protection matters - No conflicts of interest - Protection against dismissal

Reporting Line: [TODO: e.g., directly to management/board]

23.5.4 Confidentiality and Secrecy (Art. 38(5))

The Data Protection Officer is bound by secrecy or confidentiality in the performance of their tasks.

Confidentiality Commitment: [TODO: Date of signature]

23.5.5 Dismissal and Disadvantage (Art. 38(3))

The Data Protection Officer may not be dismissed or penalized for performing their tasks.

Protection Against Dismissal: [TODO: Contractually regulated]

23.6 Tasks of Data Protection Officer (Art. 39)

23.6.1 a) Information and Advice (Art. 39(1)(a))

Target Groups: - Controller and processor - Employees who carry out processing

Topics: - Obligations under GDPR - National data protection provisions - Data protection principles - Data subject rights

Implementation: - Regular training - Project consultation - Provision of information materials - Data protection newsletter

23.6.2 b) Monitoring Compliance (Art. 39(1)(b))

Monitoring Activities: - Review of processing activities - Audits and controls - Review of records of processing activities - Monitoring implementation of data protection policies

Monitoring Plan: [TODO: Quarterly audits, annual compliance review]

23.6.3 c) Advice on Data Protection Impact Assessment (Art. 39(1)(c))

Role in DPIA: - Advice on necessity of DPIA - Support in conducting - Review of DPIA results - Recommendations on measures

23.6.4 d) Cooperation with Supervisory Authority (Art. 39(1)(d))

Tasks: - Contact point for supervisory authority - Answering inquiries - Coordination of inspections - Notification of data breaches

Contact with Supervisory Authority: [TODO: Regular exchange]

23.6.5 e) Contact Point for Supervisory Authority (Art. 39(1)(e))

The Data Protection Officer is the contact point for the supervisory authority on issues relating to processing.

Availability: [TODO: Contact details, Availability hours]

23.6.6 Further Tasks

Additional tasks at {{ meta.organization }}: - [TODO: e.g., Handling data subject requests] - [TODO: e.g., Maintaining records of processing activities] - [TODO: e.g., Contract management for processors] - [TODO: e.g., Data protection communication]

23.7 Avoiding Conflicts of Interest (Art. 38(6))

The Data Protection Officer may fulfill other tasks, provided these do not result in a conflict of interest.

Incompatible Functions: - Management - IT Management (operational responsibility) - HR Management (operational responsibility) - Marketing Management (operational responsibility)

Current Function: [TODO: Description, Check for conflicts of interest]

23.8 Reporting

23.8.1 Reports to Management

Report	Frequency	Content
Quarterly Reports	Quarterly	Compliance status, Incidents, Measures
Annual Report	Annually	Overall overview, Developments, Recommendations
Ad-hoc Reports	As needed	Severe incidents, Urgent measures

23.8.2 Participation in Committees

- **Management Meetings:** [TODO: Frequency]
- **IT Security Board:** [TODO: Frequency]
- **Compliance Committee:** [TODO: Frequency]

23.9 Responsibilities

Task	Data Protection Officer	Management	Departments
Advice	Responsible	Consulted	Consulted
Monitoring	Responsible	Informed	Informed
Training	Responsible	Supports	Participants
DPIA	Advises	Approves	Conducts
Notifications	Responsible	Informed	Reports

23.10 Links to Other Documents

- **Roles and Responsibilities (Art. 4):** Overall overview
- **Controller Obligations (Art. 24):** Cooperation
- **Data Protection Impact Assessment (Art. 35):** Advisory role
- **Data Breaches (Art. 33):** Notification responsibility

Next Steps: 1. Check designation obligation for your organization 2. Designate a qualified Data Protection Officer 3. Publish contact details internally and externally 4. Provide sufficient resources 5. Define clear tasks and responsibilities

ewpage

Chapter 24

Codes of Conduct and Certification

Document-ID: 0350
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

24.1 Purpose

This document describes {{ meta.organization }}'s participation in codes of conduct and data protection certifications according to Art. 40-43 GDPR. These serve as evidence of compliance and can support accountability.

24.2 Codes of Conduct (Art. 40-41)

24.2.1 Purpose of Codes of Conduct (Art. 40(1))

Codes of conduct contribute to the proper application of GDPR, particularly taking into account the specific features of various processing sectors and the specific needs of micro, small and medium-sized enterprises.

24.2.2 Benefits of Participation

- **Compliance Evidence:** Demonstration of GDPR conformity
- **Industry Standards:** Orientation to best practices
- **Trust Building:** Towards customers and partners
- **Legal Certainty:** Clarity in implementation
- **Competitive Advantage:** Market differentiation

24.2.3 Available Codes of Conduct

24.2.3.1 Industry-Specific Codes of Conduct

Code of Conduct	Issuer	Industry	Status	Approval
[TODO: Name]	[TODO: Association]	[TODO: Industry]	Approved/In Development	[TODO: Supervisory Authority]

24.2.3.2 Cross-Functional Codes of Conduct

Code of Conduct	Topic	Issuer	Status
[TODO: Name]	[TODO: e.g., Cloud Computing]	[TODO: Association]	Approved/In Development

24.2.4 Participation in Codes of Conduct

Current Participation:

Code of Conduct	Accession Date	Monitoring Body	Next Review
[TODO: Name]	[TODO: Date]	[TODO: Body]	[TODO: Date]

Status: [TODO: Participation Yes/No]

24.2.5 Monitoring of Compliance (Art. 41)

Monitoring Body: [TODO: Name of accredited body]
Contact: [TODO: Contact details]
Review Frequency: [TODO: e.g., annually]

Monitoring Measures: - Regular audits - Complaint handling - Sanctions for non-compliance - Reporting to supervisory authority

24.3 Certification (Art. 42-43)

24.3.1 Purpose of Certification (Art. 42(1))

Certification mechanisms and data protection seals and marks serve to demonstrate that processing operations by controllers or processors comply with GDPR.

24.3.2 Benefits of Certification

- **Compliance Evidence:** Independent confirmation of GDPR conformity
- **Trust Building:** Transparency towards data subjects
- **Competitive Advantage:** Market differentiation
- **Simplification:** In processor selection
- **International Recognition:** Cross-border validity

24.3.3 Available Certifications

24.3.3.1 Data Protection Certifications

Certification	Certification Body	Scope	Validity Period
EuroPriSe	[TODO: Body]	Products, Services	2 years
ISO/IEC 27701	[TODO: Body]	PIMS (Privacy Information Management System)	3 years
TÜV Data Protection Certificate	TÜV	Organization, Processes	3 years
TISAX	ENX Association	Automotive Industry	3 years

24.3.3.2 Security Certifications (Supporting)

Certification	Certification Body	Scope	Validity Period
ISO/IEC 27001	[TODO: Body]	Information Security Management System	3 years
SOC 2 Type II	[TODO: Body]	Service Organization Controls	1 year
BSI C5	BSI	Cloud Services	2 years

24.3.4 Obtained Certifications

Current Certifications:

Certification	Certificate Number	Issue Date	Valid Until	Certification Body
[TODO: Name]	[TODO: Number]	[TODO: Date]	[TODO: Date]	[TODO: Body]

Status: [TODO: Certified Yes/No]

24.3.5 Certification Process

24.3.5.1 Phase 1: Preparation

1. **Certification Selection:** Assess relevance and benefit
2. **Gap Analysis:** Compare current state with requirements
3. **Action Plan:** Close gaps
4. **Documentation:** Prepare evidence

Duration: [TODO: e.g., 3-6 months]
Responsible: [TODO: Data Protection Officer, Project Team]

24.3.5.2 Phase 2: Audit

1. **Application:** To certification body
2. **Document Review:** Pre-audit review
3. **On-Site Audit:** Verification of implementation
4. **Remediation:** If required

Duration: [TODO: e.g., 1-2 months]
Responsible: [TODO: Data Protection Officer]

24.3.5.3 Phase 3: Certification

1. **Certificate Issuance:** Upon successful audit
2. **Publication:** Communicate certificate
3. **Surveillance Audits:** Regular reviews
4. **Recertification:** Before expiry

Duration: Ongoing
Responsible: [TODO: Data Protection Officer]

24.3.6 Validity Period and Recertification (Art. 42(7))

Certifications are issued for a maximum period of three years and may be renewed if requirements continue to be met.

Recertification Plan:

Certification	Expiry Date	Recertification Planned	Responsible
[TODO: Name]	[TODO: Date]	[TODO: Date]	[TODO: Role]

24.3.7 Monitoring and Withdrawal (Art. 42(8), Art. 43(4))

Monitoring Measures: - Annual surveillance audits - Spot checks - Complaint handling - Continuous improvement

Withdrawal Reasons: - Non-compliance with certification criteria - Severe data breaches - Refusal of monitoring - Deception in certification

24.4 Use of Seals and Marks

24.4.1 Communication of Certification

Usage Locations: - Website: [TODO: URL] - Privacy Policy: [TODO: URL] - Business Documents: [TODO: e.g., Offers, Contracts] - Marketing Materials: [TODO: e.g., Brochures]

Usage Guidelines: - Correct representation of seal - Indication of validity period - Reference to certification body - No misleading use

24.4.2 Transparency Towards Data Subjects

Data subjects are informed about certification: - In the privacy policy - Upon contract conclusion - Upon request

24.5 Cost-Benefit Analysis

24.5.1 Costs

Cost Type	One-Time	Annual
Certification Fees	[TODO: Amount]	[TODO: Amount]
Consulting/Preparation	[TODO: Amount]	-
Internal Resources	[TODO: Person-days]	[TODO: Person-days]
Surveillance Audits	-	[TODO: Amount]
Recertification	-	[TODO: Amount (every 3 years)]

24.5.2 Benefits

- **Compliance Evidence:** Reduction of liability risk
- **Trust Building:** Customer acquisition and retention
- **Process Improvement:** Optimization of data protection processes
- **Competitive Advantage:** Market differentiation
- **International Business:** Facilitation of third country transfers

ROI Assessment: [TODO: Assessment of return on investment]

24.6 Planning and Roadmap

24.6.1 Short-Term (0-12 months)

☐ Conduct gap analysis
☐ Select certification
☐ Create action plan
☐ Prepare documentation

24.6.2 Medium-Term (1-2 years)

☐ Conduct certification audit
☐ Obtain certificate

☐ First surveillance audit
☐ Communicate certification

24.6.3 Long-Term (2-3 years)

☐ Regular surveillance audits
☐ Continuous improvement
☐ Plan recertification
☐ Evaluate further certifications

24.7 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
Certification Selection	[TODO]	[TODO]	[TODO]	[TODO]
Gap Analysis	[TODO]	[TODO]	[TODO]	[TODO]
Audit Preparation	[TODO]	[TODO]	[TODO]	[TODO]
Audit Execution	[TODO]	[TODO]	[TODO]	[TODO]
Monitoring	[TODO]	[TODO]	[TODO]	[TODO]

24.8 Links to Other Documents

- **Controller Obligations (Art. 24):** Accountability
- **Processing by Processor (Art. 28):** Certification as selection criterion
- **Data Protection Impact Assessment (Art. 35):** Certification as measure
- **Data Transfers (Art. 46):** Certification as safeguard

Next Steps: 1. Evaluate relevant codes of conduct for your industry 2. Check available data protection certifications 3. Conduct a gap analysis 4. Create a certification plan 5. Communicate obtained certifications transparently

ewpage

Chapter 25

Data Protection Impact Assessment (DPIA)

Document-ID: 0400
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

25.1 Purpose

This document describes the Data Protection Impact Assessment (DPIA) process at {{ meta.organization }} according to Art. 35 GDPR. A DPIA is required when processing is likely to result in a high risk to the rights and freedoms of natural persons.

25.2 Requirement for DPIA (Art. 35(1))

25.2.1 Principle

A DPIA is required when a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, considering the nature, scope, context and purposes of the processing.

25.2.2 Mandatory Cases (Art. 35(3))

A DPIA is required in particular for:

25.2.2.1 a) Systematic and Extensive Evaluation of Personal Aspects (Art. 35(3)(a))

Examples: - Profiling with automated decisions having legal effect - Scoring procedures (creditworthiness, health risk) - Behavior-based advertising with comprehensive tracking

Status for our organization: [TODO: Applicable Yes/No]

25.2.2.2 b) Large-Scale Processing of Special Categories (Art. 35(3)(b))

Special Categories (Art. 9): - Health data - Genetic/biometric data - Racial/ethnic origin - Political opinions - Religious beliefs - Trade union membership - Sex life/sexual orientation

Status for our organization: [TODO: Applicable Yes/No]

25.2.2.3 c) Systematic Large-Scale Monitoring of Publicly Accessible Areas (Art. 35(3)(c))

Examples: - Video surveillance with facial recognition - Tracking of movement profiles - Comprehensive location data collection

Status for our organization: [TODO: Applicable Yes/No]

25.2.3 Supervisory Authority Blacklist (Art. 35(4))

The supervisory authority establishes a list of processing operations for which a DPIA must be conducted.

Relevant entries for our organization: - [TODO: Check list of competent supervisory authority] - [TODO: Document applicable entries]

25.2.4 Supervisory Authority Whitelist (Art. 35(5))

The supervisory authority may establish a list of processing operations for which no DPIA is required.

Relevant entries for our organization: - [TODO: Check list of competent supervisory authority] - [TODO: Document applicable entries]

25.2.5 Additional Criteria (WP29 Guidelines)

Additional indicators for high risk:

Criterion	Description	Applicable
Evaluation or Scoring	Profiling, prediction of behavior	Yes/No
Automated Decisions	With legal or similar effect	Yes/No
Systematic Monitoring	Continuous observation	Yes/No
Sensitive Data	Special categories (Art. 9)	Yes/No
Large-Scale Processing	Many data subjects or large data volumes	Yes/No
Matching or Combining	Datasets from different sources	Yes/No
Vulnerable Data Subjects	Children, employees, patients	Yes/No
Innovative Use	New technologies or applications	Yes/No
Denial of Rights	Access to service or contract	Yes/No

Rule of Thumb: If two or more criteria apply, a DPIA is recommended.

25.3 DPIA Register

25.3.1 Overview of Conducted DPIAs

DPIA-ID	Processing	Conduct Date	Risk	Status	Next Review
DPIA-001	[TODO: Name]	[TODO: Date]	High/Medium/Low	Completed/Ongoing	[TODO: Date]

25.4 DPIA Process

25.4.1 Phase 1: Threshold Analysis

Objective: Determine if a DPIA is required

Steps: 1. Describe processing 2. Check criteria (Art. 35(3), Blacklist, WP29 criteria) 3. Consult Data Protection Officer 4. Document decision

Responsible: [TODO: Department, Data Protection Officer]
Duration: [TODO: e.g., 1-2 weeks]

25.4.2 Phase 2: DPIA Execution

Objective: Systematic assessment of risks

25.4.2.1 Step 1: Description of Processing (Art. 35(7)(a))

To be documented: - Purposes of processing - Categories of personal data - Categories of data subjects - Recipients of data - Storage duration - Functional description of processing - Technologies used - Data flows (diagrams)

25.4.2.2 Step 2: Assessment of Necessity and Proportionality (Art. 35(7)(b))

To be checked: - Is processing necessary to achieve purpose? - Are means appropriate? - Are data protection principles complied with? - Are there less invasive alternatives?

Lawfulness: - Legal basis (Art. 6) - Legitimate interests (if Art. 6(1)(f)) - Balancing of interests

25.4.2.3 Step 3: Risk Assessment (Art. 35(7)(c))

Risk Identification:

Risk	Description	Affected Rights	Likelihood	Severity
[TODO]	[TODO]	[TODO: e.g., Right to privacy]	Low/Medium/High	Low/Medium/High

Risk Assessment Matrix:

Severity / Likelihood	Low	Medium	High
High	Medium	High	Very High

Severity / Likelihood	Low	Medium	High
Medium	Low	Medium	High
Low	Very Low	Low	Medium

Affected Rights and Freedoms: - Right to privacy - Right to data protection - Right to non-discrimination - Right to freedom of expression - Other fundamental rights

25.4.2.4 Step 4: Measures for Risk Mitigation (Art. 35(7)(d))

Technical Measures:

Measure	Description	Risk Mitigation	Status
Encryption	[TODO]	[TODO: Reduces risk from X to Y]	Implemented/Planned
Pseudonymization	[TODO]	[TODO]	Implemented/Planned
Access Controls	[TODO]	[TODO]	Implemented/Planned

Organizational Measures:

Measure	Description	Risk Mitigation	Status
Training	[TODO]	[TODO]	Implemented/Planned
Policies	[TODO]	[TODO]	Implemented/Planned
Audits	[TODO]	[TODO]	Implemented/Planned

Residual Risk After Measures:

Risk	Original Risk	Measures	Residual Risk	Acceptable
[TODO]	[TODO: High]	[TODO: Measures]	[TODO: Medium]	Yes/No

25.4.3 Phase 3: Consultation of Data Protection Officer (Art. 35(2))

Obligation: The Data Protection Officer is consulted during the DPIA.

Consultation: - **Date:** [TODO: Date] - **Opinion:** [TODO: Summary of recommendations] - **Consideration:** [TODO: How recommendations were implemented]

25.4.4 Phase 4: Seeking Views of Data Subjects (Art. 35(9))

Where appropriate: Seek views of data subjects or their representatives.

Conducted: [TODO: Yes/No]
Method: [TODO: e.g., Survey, Focus group]
Results: [TODO: Summary]

25.4.5 Phase 5: Documentation and Approval

Create DPIA Report: - Document all steps - Summarize risk assessment - List measures - Assess residual risk

Approval: - **Responsible:** [TODO: Management] - **Date:** [TODO: Date] - **Decision:** Approved / Approved with conditions / Rejected

25.5 Prior Consultation with Supervisory Authority (Art. 36)

25.5.1 Consultation Obligation (Art. 36(1))

If the DPIA indicates that processing would result in a high risk if the controller does not take measures to mitigate the risk, the controller consults the supervisory authority prior to processing.

Criteria for Consultation: - Residual risk after measures is high - No further measures possible to mitigate risk - Uncertainty about appropriateness of measures

Consultation Required: [TODO: Yes/No]

25.5.2 Consultation Process

Information to be Provided (Art. 36(3)): - Responsibilities - Purposes and means of processing - Measures to protect rights and freedoms - Contact details of Data Protection Officer - DPIA report - Other relevant information

Supervisory Authority Deadline: 8 weeks (extendable to 14 weeks for complex processing)

Consultation Documentation: - **Request Date:** [TODO: Date] - **Supervisory Authority Opinion:** [TODO: Summary] - **Implementation of Recommendations:** [TODO: Measures]

25.6 Review and Update

25.6.1 Review Obligation (Art. 35(11))

The DPIA is reviewed when: - Changes in risk of processing - Changes in processing activity - New technologies are used - New insights about risks emerge

Review Frequency: [TODO: e.g., annually or upon changes]

25.6.2 Update Process

1. Identify changes
2. Update risk assessment
3. Adapt measures
4. Consult Data Protection Officer
5. Update documentation
6. Obtain approval

25.7 DPIA Template

Standard Template: [TODO: Link to DPIA template]
Industry-Specific Templates: [TODO: If available]

25.8 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
Threshold Analysis	[TODO]	[TODO]	[TODO]	[TODO]
DPIA Execution	[TODO]	[TODO]	[TODO]	[TODO]
Risk Assessment	[TODO]	[TODO]	[TODO]	[TODO]
Measure Planning	[TODO]	[TODO]	[TODO]	[TODO]
Approval	[TODO]	[TODO]	[TODO]	[TODO]

25.9 Links to Other Documents

- **Controller Obligations (Art. 24):** Accountability
- **Security of Processing (Art. 32):** Technical measures
- **Records of Processing Activities (Art. 30):** Documentation
- **Data Protection Officer (Art. 39):** Advisory role

Next Steps: 1. Identify all processing requiring DPIA 2. Conduct systematic DPIAs 3. Document risks and measures 4. Consult Data Protection Officer 5. Review DPIAs regularly

ewpage

Chapter 26

DPIA Template

Document-ID: 0410
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

26.1 DPIA Identification

DPIA-ID: [TODO: e.g., DPIA-2024-001]
Processing: [TODO: Name of processing]
Controller: [TODO: Name, Department]
Created on: [TODO: Date]
Created by: [TODO: Name, Role]
Status: Draft / Under Review / Approved

26.2 1. Description of Processing

26.2.1 1.1 Purposes of Processing

Main Purpose: [TODO: Describe the main purpose of processing]

Further Purposes: - [TODO: Purpose 1] - [TODO: Purpose 2]

26.2.2 1.2 Categories of Personal Data

Data Category	Examples	Special Category (Art. 9)
[TODO: e.g., Master Data]	[TODO: Name, Address, Date of birth]	No
[TODO: e.g., Contact Data]	[TODO: Email, Phone]	No
[TODO: e.g., Health Data]	[TODO: Diagnoses, Treatments]	Yes

Estimated Data Volume: [TODO: e.g., 10,000 records]

26.2.3 1.3 Categories of Data Subjects

- [TODO: e.g., Customers]
- [TODO: e.g., Employees]
- [TODO: e.g., Patients]

Estimated Number: [TODO: e.g., 5,000 persons]

Vulnerable Groups: [TODO: e.g., Children, Patients - Yes/No]

26.2.4 1.4 Recipients of Data

Internal Recipients: - [TODO: e.g., Sales, Accounting]

External Recipients: - [TODO: e.g., Payment service providers]

Processors: - [TODO: e.g., Cloud providers, IT service providers]

Third Country Transfer: [TODO: Yes/No - if Yes, which countries]

26.2.5 1.5 Storage Duration

Standard Case: [TODO: e.g., 3 years after contract end]
Legal Retention Obligations: [TODO: e.g., 10 years commercial law]
Erasure Concept: [TODO: Reference to document or description]

26.2.6 1.6 Functional Description

[TODO: Describe processing in detail: - How is data collected? - How is data processed? - Which systems are involved? - Which technologies are used? - Are there automated decisions? - Is there profiling?]

26.2.7 1.7 Data Flow Diagram

[TODO: Insert diagram visualizing data flow]

```
[Data Source] → [Processing System] → [Storage] → [Recipient]
```

26.3 2. Necessity and Proportionality

26.3.1 2.1 Legal Basis

Legal Basis: [TODO: Art. 6(1) lit. a/b/c/d/e/f]

Justification: [TODO: Explain why this legal basis is applicable]

For Special Categories (Art. 9): Legal Basis: [TODO: Art. 9(2) lit. a-j]

26.3.2 2.2 Necessity

Is processing necessary to achieve purpose? [TODO: Yes/No - Justification]

Are there less invasive alternatives? [TODO: Yes/No - if Yes, why are they not used?]

26.3.3 2.3 Proportionality

Are means appropriate? [TODO: Assessment of proportionality]

Data Protection Principles (Art. 5):

Principle	Compliance	Justification
Lawfulness, Fairness, Transparency	Yes/No	[TODO]
Purpose Limitation	Yes/No	[TODO]
Data Minimization	Yes/No	[TODO]
Accuracy	Yes/No	[TODO]
Storage Limitation	Yes/No	[TODO]
Integrity and Confidentiality	Yes/No	[TODO]

26.3.4 2.4 Balancing of Interests (for Art. 6(1)(f))

Legitimate Interest of Controller: [TODO: Describe legitimate interest]

Interests of Data Subjects: [TODO: Describe interests and fundamental rights of data subjects]

Balancing: [TODO: Do controller's interests or data subjects' interests prevail?]

26.4 3. Risk Assessment

26.4.1 3.1 Risk Identification

Identified Risks:

26.4.1.1 Risk 1: [TODO: Name of Risk]

Description: [TODO: Detailed description of risk]

Threat: [TODO: e.g., Unauthorized access, Data loss, Manipulation]

Affected Rights and Freedoms: - [TODO: e.g., Right to privacy] - [TODO: e.g., Right to data protection]

Possible Consequences for Data Subjects: - [TODO: e.g., Identity theft] - [TODO: e.g., Financial losses] - [TODO: e.g., Discrimination] - [TODO: e.g., Reputational damage]

Likelihood: [TODO: Low / Medium / High]

Justification of Likelihood: [TODO: Why is likelihood assessed this way?]

Severity of Impact: [TODO: Low / Medium / High]

Justification of Severity: [TODO: Why is severity assessed this way?]

Risk Level: [TODO: Calculate from Likelihood × Severity]

26.4.1.2 Risk 2: [TODO: Name of Risk]

[TODO: Repeat structure for additional risks]

26.4.2 3.2 Risk Assessment Matrix

Risk	Likelihood	Severity	Risk Level
Risk 1	[TODO]	[TODO]	[TODO]
Risk 2	[TODO]	[TODO]	[TODO]

Overall Risk: [TODO: Low / Medium / High / Very High]

26.5 4. Measures for Risk Mitigation

26.5.1 4.1 Technical Measures

26.5.1.1 Measure 1: [TODO: Name of Measure]

Description: [TODO: Detailed description]

Addressed Risk: [TODO: Risk 1, Risk 2, …]

Effectiveness: [TODO: High / Medium / Low]

Implementation Status: [TODO: Implemented / In Progress / Planned]

Responsible: [TODO: Role/Name]

Deadline: [TODO: Date]

26.5.1.2 Measure 2: [TODO: Name of Measure]

[TODO: Repeat structure for additional measures]

26.5.2 4.2 Organizational Measures

26.5.2.1 Measure 1: [TODO: Name of Measure]

Description: [TODO: Detailed description]

Addressed Risk: [TODO: Risk 1, Risk 2, …]

Effectiveness: [TODO: High / Medium / Low]

Implementation Status: [TODO: Implemented / In Progress / Planned]

Responsible: [TODO: Role/Name]

Deadline: [TODO: Date]

26.5.3 4.3 Data Protection by Design

Implemented Principles: - [ ] Data minimization from the start - [ ] Pseudonymization where possible - [ ] Encryption as standard - [ ] Transparency in processing - [ ] User-friendly data protection features

Description: [TODO: How were Privacy by Design principles implemented?]

26.5.4 4.4 Data Protection by Default

Implemented Principles: - [ ] Only necessary data processed by default - [ ] Minimal storage duration as default - [ ] Restricted access as default - [ ] Opt-in instead of opt-out

Description: [TODO: How were Privacy by Default principles implemented?]

26.6 5. Residual Risk Assessment

26.6.1 5.1 Risks After Measures

Risk	Original Risk Level	Measures	Residual Risk	Acceptable
Risk 1	[TODO: High]	[TODO: Measures 1, 2]	[TODO: Medium]	Yes/No
Risk 2	[TODO: Medium]	[TODO: Measure 3]	[TODO: Low]	Yes/No

26.6.2 5.2 Overall Assessment

Residual Risk After Measures: [TODO: Low / Medium / High]

Is residual risk acceptable? [TODO: Yes / No]

Justification: [TODO: Why is residual risk acceptable or not acceptable?]

26.7 6. Consultation of Data Protection Officer

Data Protection Officer: [TODO: Name]

Consultation Date: [TODO: Date]

Opinion: [TODO: Summary of Data Protection Officer's recommendations]

Consideration of Recommendations: [TODO: How were recommendations implemented?]

Signature Data Protection Officer: _____

26.8 7. Seeking Views of Data Subjects

Were views of data subjects sought? [TODO: Yes / No]

If Yes:

Method: [TODO: e.g., Survey, Focus group, Consultation]

Date: [TODO: Date]

Results: [TODO: Summary of views and concerns]

Consideration: [TODO: How were views considered?]

26.9 8. Prior Consultation with Supervisory Authority

Is consultation with supervisory authority required? [TODO: Yes / No]

Justification: [TODO: Why is/isn't consultation required?]

If Yes:

Request Date: [TODO: Date]

Supervisory Authority Opinion: [TODO: Summary of opinion]

Implementation of Recommendations: [TODO: How were recommendations implemented?]

26.10 9. Approval

Controller: [TODO: Name, Role]

Date: [TODO: Date]

Decision: [ ] Approved [ ] Approved with Conditions [ ] Rejected

Conditions (if applicable): [TODO: List of conditions]

Signature: _____

26.11 10. Review and Update

Next Review Planned: [TODO: Date]

Review Triggers: - [ ] Annual review - [ ] Change in processing - [ ] New technologies - [ ] Security incident - [ ] New insights about risks

26.11.1 Change History

Version	Date	Change	Changed By
1.0	[TODO]	Initial version	[TODO]
1.1	[TODO]	[TODO: Description]	[TODO]

26.12 Appendices

- ☐ Data flow diagrams
- ☐ TOM documentation
- ☐ Processor agreements
- ☐ Consent forms
- ☐ Other relevant documents

Note: This DPIA is a living document and must be updated upon changes in processing or new insights about risks.

ewpage

Chapter 27

Data Transfers to Third Countries

Document-ID: 0500
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

27.1 Purpose

This document regulates the transfer of personal data to third countries (outside EU/EEA) at {{ meta.organization }} according to Art. 44-50 GDPR. It ensures that an adequate level of protection is guaranteed even for international data transfers.

27.2 Principle (Art. 44)

A transfer of personal data to a third country may only take place if: - The conditions of Art. 45-49 are complied with - The other provisions of GDPR are complied with - Including data subject rights and remedies

27.3 Register of Third Country Transfers

27.3.1 Overview

ID	Recipient	Third Country	Purpose	Legal Basis	Safeguards	Volume
T001	[TODO: Name]	[TODO: Country]	[TODO: Purpose]	Art. 45/46/49	[TODO]	[TODO: Number of data subjects]

27.4 Adequacy Decision (Art. 45)

27.4.1 Countries with Adequacy Decision

The European Commission may decide that a third country provides an adequate level of protection.

Current Adequacy Decisions (as of 2024):

Country/Region	Decision	Valid Since	Specifics
Andorra	2010/625/EU	19.10.2010	-
Argentina	2003/490/EC	30.06.2003	-
Canada	2002/2/EC	20.12.2001	Commercial organizations only
Faroe Islands	2010/146/EU	05.03.2010	-
Guernsey	2003/821/EC	21.11.2003	-
Israel	2011/61/EU	31.01.2011	-
Isle of Man	2004/411/EC	28.04.2004	-
Japan	2019/419	23.01.2019	-
Jersey	2008/393/EC	08.05.2008	-
New Zealand	2013/65/EU	19.12.2012	-
Republic of Korea	2021/2216	17.12.2021	-
Switzerland	2000/518/EC	26.07.2000	-
United Kingdom	2021/1772	28.06.2021	Post-Brexit
Uruguay	2012/484/EU	21.08.2012	-

USA - EU-U.S. Data Privacy Framework: - **Status:** [TODO: Check current status] - **Certification Required:** Yes - **Verification:** [TODO: Check list of certified companies]

27.4.2 Transfers Based on Adequacy Decision

Recipient	Country	Adequacy Decision	Additional Checks
[TODO: Name]	[TODO: Country]	[TODO: Decision]	[TODO: e.g., Privacy Shield certification]

Documentation: [TODO: Reference to evidence]

27.5 Appropriate Safeguards (Art. 46)

Without an adequacy decision, a transfer is only permissible if appropriate safeguards have been provided and enforceable rights and effective remedies for data subjects are available.

27.5.1 Standard Contractual Clauses (Art. 46(2)(c))

Available Standard Contractual Clauses (SCC):

27.5.1.1 New SCCs (2021)

- **Module 1:** Controller to Controller
- **Module 2:** Controller to Processor
- **Module 3:** Processor to Processor
- **Module 4:** Processor to Controller

Used SCCs:

Transfer	Module	Conclusion Date	Contracting Party	Documentation
[TODO: Description]	[TODO: Module]	[TODO: Date]	[TODO: Name]	[TODO: Link]

Mandatory Content of SCCs: - Description of transfer - List of sub-processors (for Module 2/3) - Technical and organizational measures - Docking clause (optional)

27.5.2 Binding Corporate Rules (Art. 46(2)(b))

Status: [TODO: BCRs in place? Yes/No]

If Yes: - **Approval Date:** [TODO: Date] - **Approving Supervisory Authority:** [TODO: Authority] - **Scope:** [TODO: Group companies] - **Documentation:** [TODO: Link to BCRs]

27.5.3 Codes of Conduct and Certification (Art. 46(2)(e), (f))

Codes of Conduct with Enforcement Mechanism: - **Status:** [TODO: In place? Yes/No] - **Code of Conduct:** [TODO: Name]

Certification with Enforcement Mechanism: - **Status:** [TODO: In place? Yes/No] - **Certification:** [TODO: Name]

27.5.4 Other Safeguards (Art. 46(3))

Ad-hoc Contractual Clauses (with supervisory authority approval): - **Status:** [TODO: In place? Yes/No] - **Approval Date:** [TODO: Date]

27.6 Transfer Impact Assessment (TIA)

27.6.1 Requirement

Following the Schrems-II judgment (CJEU C-311/18), the controller must assess whether the level of protection in the third country is equivalent to that in the EU.

TIA Required for: - All transfers based on Art. 46 (safeguards) - Particularly for transfers to USA and other countries with government access possibilities

27.6.2 TIA Process

27.6.2.1 Step 1: Map Data Transfer

- What data is transferred?

- To whom is data transferred?
- To which country is data transferred?
- Which legal basis is used?

27.6.2.2 Step 2: Assess Legal Situation in Third Country

To be assessed: - Data protection laws in third country - Government access possibilities (e.g., FISA 702, EO 12333) - Legal remedies for data subjects - Practical enforceability of rights

Documentation: [TODO: Summary of legal situation in destination country]

27.6.2.3 Step 3: Evaluate Supplementary Measures

Technical Measures: - End-to-end encryption - Pseudonymization - Anonymization - Encryption in transit and at rest

Organizational Measures: - Contractual commitments - Transparency towards data subjects - Training of recipient - Audits and controls

Legal Measures: - Challenge government requests - Notification upon government requests - Transparency reports

27.6.2.4 Step 4: Decision

Is an adequate level of protection ensured? [TODO: Yes / No]

If No: - Stop transfer - Seek alternative solutions (e.g., EU providers) - Check derogation per Art. 49

27.6.3 TIA Documentation

Transfer	TIA Conducted	Date	Result	Supplementary Measures	Next Review
[TODO]	Yes/No	[TODO]	Adequate/Not adequate	[TODO]	[TODO]

27.7 Derogations (Art. 49)

Without an adequacy decision or appropriate safeguards, a transfer is only permissible in exceptional cases.

27.7.1 Derogation Grounds (Art. 49(1))

27.7.1.1 a) Consent

Requirements: - Data subject informed about possible risks - Consent is freely given, specific, informed and unambiguous

Use: [TODO: Yes/No - if Yes, document consents]

27.7.1.2 b) Contract Performance

Requirements: - Transfer necessary for performance of contract - Or for pre-contractual measures at data subject's request

Use: [TODO: Yes/No - if Yes, document cases]

27.7.1.3 c) Public Interest

Requirements: - Transfer necessary for important reasons of public interest

Use: [TODO: Yes/No - if Yes, document cases]

27.7.1.4 d) Legal Claims

Requirements: - Transfer necessary for establishment, exercise or defense of legal claims

Use: [TODO: Yes/No - if Yes, document cases]

27.7.1.5 e) Vital Interests

Requirements: - Transfer necessary to protect vital interests - Data subject physically or legally incapable of giving consent

Use: [TODO: Yes/No - if Yes, document cases]

27.7.1.6 f) Public Register

Requirements: - Transfer from register intended to provide information to public

Use: [TODO: Yes/No - if Yes, document cases]

27.7.2 Derogation for Occasional Transfers (Art. 49(1) subpara. 2)

Requirements: - Transfer is not repetitive - Concerns only limited number of persons - Necessary for compelling legitimate interests - Interests override data subject's interests - Controller assessed all circumstances - Appropriate safeguards provided

Use: [TODO: Yes/No - if Yes, document cases]

Documentation Obligation: Transfer must be notified to supervisory authority

27.8 Information Obligations

27.8.1 Information to Data Subjects

Data subjects must be informed about third country transfers: - In privacy policy (Art. 13, 14) - Upon access requests (Art. 15)

To be informed about: - Recipients or categories of recipients in third countries - Third country - Legal basis of transfer - Appropriate safeguards (with reference to copy or location) - For derogations: Compelling legitimate interests

27.8.2 Transparency

Publication: - List of third country transfers on website - Information on safeguards used - Contact for inquiries

27.9 Monitoring and Review

27.9.1 Regular Review

Review Frequency: [TODO: e.g., annually]

To be checked: - Are all third country transfers recorded? - Are legal bases still current? - Are safeguards still effective? - Have legal situation or risks changed? - Are TIAs current?

27.9.2 Change Management

Triggers for Review: - New third country transfer - Change in legal situation in third country - New court judgments (e.g., CJEU) - Revocation of adequacy decisions - Security incidents

27.10 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
Identification of Third Country Transfers	[TODO]	[TODO]	[TODO]	[TODO]
TIA Execution	[TODO]	[TODO]	[TODO]	[TODO]
SCC Conclusion	[TODO]	[TODO]	[TODO]	[TODO]
Monitoring	[TODO]	[TODO]	[TODO]	[TODO]

27.11 Links to Other Documents

- **Records of Processing Activities (Art. 30):** Documentation of transfers
- **Data Protection Impact Assessment (Art. 35):** TIA as part of DPIA
- **Processing by Processor (Art. 28):** SCCs with processors in third countries
- **Information Obligations (Art. 13-14):** Transparency towards data subjects

---

Next Steps: 1. Identify all third country transfers 2. Check adequacy decisions 3. Implement appropriate safeguards (SCCs, BCRs) 4. Conduct Transfer Impact Assessments 5. Inform data subjects transparently

ewpage

Chapter 28

Standard Contractual Clauses (SCC)

Document-ID: 0510
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Internal
Last Update: {{ meta.date }}

28.1 Purpose

This document describes the use of Standard Contractual Clauses (SCC) at {{ meta.organization }} for the transfer of personal data to third countries according to Art. 46(2)(c) GDPR.

28.2 New Standard Contractual Clauses (2021)

28.2.1 Implementing Decision (EU) 2021/914

Adoption: 4 June 2021
Applicable from: 27 June 2021
Transition Period for Old SCCs: Until 27 December 2022

Advantages of New SCCs: - Modular structure for different transfer scenarios - Consideration of Schrems-II judgment - Flexibility for complex processing chains - Docking clause for additional parties

28.3 SCC Modules

28.3.1 Module 1: Controller to Controller

Use Case: Controller in EU transfers data to controller in third country

Examples: - Transfer of customer data to foreign business partner - Data exchange between group companies (both as controllers) - Transfer to foreign authorities (where permissible)

Use at {{ meta.organization }}:

Transfer	Recipient	Country	Conclusion Date	Documentation
[TODO: Description]	[TODO: Name]	[TODO: Country]	[TODO: Date]	[TODO: Link]

28.3.2 Module 2: Controller to Processor

Use Case: Controller in EU engages processor in third country

Examples: - Cloud hosting outside EU/EEA - Outsourcing of IT services - Call centers in third countries - Payroll by foreign service provider

Use at {{ meta.organization }}:

Processor	Service	Country	Conclusion Date	Documentation
[TODO: Name]	[TODO: Service]	[TODO: Country]	[TODO: Date]	[TODO: Link]

28.3.3 Module 3: Processor to Processor

Use Case: Processor engages sub-processor in third country

Examples: - Cloud provider uses sub-hosting provider - IT service provider outsources parts to sub-provider

Use at {{ meta.organization }}:

Main Processor	Sub-Processor	Country	Conclusion Date	Documentation
[TODO: Name]	[TODO: Name]	[TODO: Country]	[TODO: Date]	[TODO: Link]

28.3.4 Module 4: Processor to Controller

Use Case: Processor transfers data to controller in third country

Examples: - Processor transfers data to group parent in third country - Return transfer of data after contract end

Use at {{ meta.organization }}:

Processor	Recipient	Country	Conclusion Date	Documentation
[TODO: Name]	[TODO: Name]	[TODO: Country]	[TODO: Date]	[TODO: Link]

28.4 Mandatory Annexes of SCCs

28.4.1 Annex I: Parties and Data Transfer

28.4.1.1 Part A: List of Parties

Data Exporter (EU): - Name: [TODO: {{ meta.organization }}] - Address: [TODO: Address] - Contact: [TODO: Name, Email, Phone] - Role: Controller / Processor - Signature: _____

Data Importer (Third Country): - Name: [TODO: Name of recipient] - Address: [TODO: Address] - Contact: [TODO: Name, Email, Phone] - Role: Controller / Processor - Signature: _____

28.4.1.2 Part B: Description of Transfer

Categories of Data Subjects: - [TODO: e.g., Customers, Employees, Suppliers]

Categories of Personal Data: - [TODO: e.g., Master data, Contact data, Contract data] - **Special Categories (Art. 9):** [TODO: if applicable]

Sensitive Data (if applicable): - [TODO: Description]

Frequency of Transfer: - [TODO: e.g., continuous, monthly, as needed]

Nature of Transfer: - [TODO: e.g., Email, API, Cloud storage]

Purpose(s) of Data Transfer: - [TODO: e.g., Contract performance, IT services]

Storage Period with Importer: - [TODO: e.g., Contract duration + 3 years]

For Transfers to Sub-Processors: - [TODO: Description of processing by sub-processors]

28.4.1.3 Part C: Competent Supervisory Authority

Exporter's Supervisory Authority: - Name: [TODO: e.g., State Commissioner for Data Protection] - Address: [TODO: Address] - Email: [TODO: Email] - Website: [TODO: URL]

28.4.2 Annex II: Technical and Organizational Measures (TOM)

Description of data importer's technical and organizational measures:

28.4.2.1 1. Access Controls

Physical Access Controls: - [TODO: e.g., Access control system, Visitor management]

Logical Access Controls: - [TODO: e.g., User authentication, Multi-factor authentication]

28.4.2.2 2. Access Management

Authorization Concept: - [TODO: e.g., Role-based access control (RBAC)]

Least Privilege Principle: - [TODO: Description]

28.4.2.3 3. Encryption

Encryption in Transit: - [TODO: e.g., TLS 1.3]

Encryption at Rest: - [TODO: e.g., AES-256]

Key Management: - [TODO: Description]

28.4.2.4 4. Pseudonymization

Procedures: - [TODO: Description, if applicable]

28.4.2.5 5. Logging and Monitoring

Logging: - [TODO: e.g., Access logs, Change logs]

Log Retention Period: - [TODO: e.g., 90 days]

Monitoring: - [TODO: e.g., SIEM, Intrusion detection]

28.4.2.6 6. Incident Response

Incident Response Plan: - [TODO: Reference to document]

Notification Obligation: - [TODO: Immediate notification to exporter]

28.4.2.7 7. Backup and Recovery

Backup Strategy: - [TODO: e.g., Daily backups, 30 days retention]

Recovery Time Objective (RTO): - [TODO: e.g., 24 hours]

Recovery Point Objective (RPO): - [TODO: e.g., 1 hour]

28.4.2.8 8. Data Deletion

Deletion Procedures: - [TODO: e.g., Secure deletion per NIST 800-88]

Deletion Certificate: - [TODO: Description]

28.4.2.9 9. Training and Awareness

Training Program: - [TODO: e.g., Annual data protection training]

Confidentiality Commitment: - [TODO: All employees committed]

28.4.2.10 10. Audits and Certifications

Internal Audits: - [TODO: e.g., Annually]

External Audits: - [TODO: e.g., ISO 27001, SOC 2]

Certifications: - [TODO: List of certifications]

28.4.3 Annex III: List of Sub-Processors (Module 2 and 3 only)

Authorization Procedure: [ ] General Authorization [ ] Specific Authorization

List of Authorized Sub-Processors:

Name	Address	Country	Processing Activity	Safeguards
[TODO]	[TODO]	[TODO]	[TODO]	[TODO: e.g., SCCs]

Information Obligation Upon Changes: - Objection Period: [TODO: e.g., 30 days] - Notification Method: [TODO: e.g., Email]

28.5 Optional Clauses

28.5.1 Docking Clause (Clause 7)

Activated: [TODO: Yes/No]

Purpose: Allows additional parties to accede to SCCs

Acceded Parties:

Name	Role	Accession Date	Documentation
[TODO]	[TODO]	[TODO]	[TODO]

28.5.2 Local Laws and Practices (Clause 14)

Importer's Obligation: - Notification upon government requests - Challenge disproportionate requests - Annual review of legal situation

Documentation of Government Requests:

Date	Authority	Type of Request	Measures	Notification to Exporter
[TODO]	[TODO]	[TODO]	[TODO]	[TODO: Date]

28.6 Transfer Impact Assessment (TIA)

28.6.1 Requirement

According to Schrems-II judgment, a TIA must be conducted in addition to SCCs.

TIA Conducted: [TODO: Yes/No]
Date: [TODO: Date]
Result: [TODO: Adequate level of protection ensured Yes/No]

28.6.2 Supplementary Measures

Technical Measures: - [TODO: e.g., End-to-end encryption] - [TODO: e.g., Pseudonymization]

Organizational Measures: - [TODO: e.g., Contractual commitments] - [TODO: e.g., Transparency reports]

Legal Measures: - [TODO: e.g., Challenge government requests]

Documentation: [TODO: Reference to TIA report]

28.7 Contract Management

28.7.1 Conclusion Process

1. **Module Selection:** Choose appropriate SCC template
2. **Complete Annexes:** Fill all mandatory annexes completely
3. **Conduct TIA:** Transfer Impact Assessment
4. **Supplementary Measures:** Implement if required
5. **Consult Data Protection Officer:** Obtain opinion
6. **Contract Signature:** Both parties sign
7. **Documentation:** File and register contract

28.7.2 Monitoring

Review Frequency: [TODO: e.g., annually]

To be checked: - Importer's compliance with SCCs - Currency of TOM - Changes in legal situation in third country - Sub-processor list current - Government requests documented

Audit Rights: - Right to on-site audits - Right to document review - Right to certificate review

28.7.3 Contract End

Upon Contract End: - Return or deletion of data - Obtain deletion certificate - Complete documentation

28.8 Responsibilities

Task	Responsible	Accountable	Consulted	Informed
Module Selection	[TODO]	[TODO]	[TODO]	[TODO]
Complete Annexes	[TODO]	[TODO]	[TODO]	[TODO]
Conduct TIA	[TODO]	[TODO]	[TODO]	[TODO]
Contract Conclusion	[TODO]	[TODO]	[TODO]	[TODO]
Monitoring	[TODO]	[TODO]	[TODO]	[TODO]

28.9 Links to Other Documents

- **Data Transfers to Third Countries (Art. 44-50):** Overarching document

- **Processing by Processor (Art. 28):** For Module 2 and 3
- **TOM Documentation (Art. 32):** Detailed security measures
- **Transfer Impact Assessment:** Risk assessment

Next Steps: 1. Identify all third country transfers requiring SCCs 2. Select appropriate SCC module 3. Complete all annexes fully 4. Conduct a Transfer Impact Assessment 5. Conclude SCCs with all data importers

ewpage

Chapter 29

Data Breach Response Plan (Template)

Document-ID: 0600
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Draft
Classification: Confidential
Last Update: {{ meta.date }}

29.1 Purpose

This response plan defines the steps for managing data breaches at {{ meta.organization }}. It ensures that data breaches are quickly detected, assessed, and handled according to GDPR Art. 33-34.

29.2 Scope

This plan applies to all data breaches affecting personal data processed by {{ meta.organization }}.

29.3 Breach Response Team

29.3.1 Core Team

Role	Name	Contact	Responsibilities
Incident Commander	[TODO]	[TODO: Phone, Email]	Overall responsibility, decisions
Data Protection Officer	[TODO]	[TODO: Phone, Email]	Legal assessment, notification obligation

Role	Name	Contact	Responsibilities
IT Security Lead	[TODO]	[TODO: Phone, Email]	Technical analysis, containment
Legal Counsel	[TODO]	[TODO: Phone, Email]	Legal advice
Communication Lead	[TODO]	[TODO: Phone, Email]	Internal/external communication

29.3.2 Extended Stakeholders

Role	Name	Contact	When to involve
Management	[TODO]	[TODO]	For high risk
HR	[TODO]	[TODO]	For employee data
Compliance	[TODO]	[TODO]	For regulatory questions
PR/Marketing	[TODO]	[TODO]	For public communication

29.4 Breach Response Process

29.4.1 Phase 1: Detection and Reporting (0-2 hours)

29.4.1.1 1.1 Detect Breach

Detection Sources: - Monitoring systems and alerts - Employee reports - External reports (customers, partners) - Audit findings - Media reports

29.4.1.2 1.2 Initial Report

Who reports: - Any employee who discovers a potential data breach

To whom: - IT Security: [TODO: Email/Phone] - Data Protection Officer: [TODO: Email/Phone]

Report Form:

```
INITIAL BREACH REPORT

Reporter: [Name, Department, Contact]
Date/Time of Discovery: [YYYY-MM-DD HH:MM]
Discovery Method: [Monitoring / Employee / External / Audit / Other]

Brief Description:
[What happened?]

Affected Systems:
[Which systems are affected?]

Affected Data (initial assessment):
[What type of data?]
```

```
Number of Data Subjects (estimate):
[Approximate number]

Immediate Actions Taken:
[What has been done already?]
```

29.4.1.3 1.3 Activate Breach Response Team

Incident Commander: - Activates core team - Schedules initial meeting (within 2 hours) - Creates Breach-ID: `BREACH-[YYYY]-[NNN]`

29.4.2 Phase 2: Assessment and Containment (2-12 hours)

29.4.2.1 2.1 Initial Assessment

Checklist: - [ ] Is there actually a data breach? - [ ] Which category: Confidentiality / Integrity / Availability? - [ ] What data is affected? - [ ] How many persons are affected? - [ ] Are special categories (Art. 9) affected? - [ ] How did the breach occur? - [ ] Is the breach still active?

Documentation: - Document all findings in breach register - Secure screenshots and logs - Forensic preservation if needed

29.4.2.2 2.2 Immediate Containment

Technical Measures: - [ ] Isolate affected systems - [ ] Block access - [ ] Reset passwords - [ ] Close security gaps - [ ] Prevent further data loss

Responsible: IT Security Lead

Timeframe: Within 4 hours

29.4.2.3 2.3 Scope Determination

To clarify: - Exact number of affected persons - Exact data categories - Period of breach - Cause of breach - Potential impacts

Methods: - Log analysis - Database queries - System forensics - Interviews with involved parties

29.4.3 Phase 3: Risk Assessment (12-24 hours)

29.4.3.1 3.1 Assess Risk to Data Subjects

Assessment Criteria:

Criterion	Assessment	Points
Type of Data		
- General contact data	Low	1
- Financial data, credentials	Medium	2
- Special categories (Art. 9)	High	3
Number of Data Subjects		
- < 100 persons	Low	1
- 100-1,000 persons	Medium	2

Criterion	Assessment	Points
- > 1,000 persons	High	3
Protective Measures		
- Encrypted, pseudonymized	Low	1
- Partially protected	Medium	2
- Unencrypted, plaintext	High	3
Data Subjects		
- Employees (internal)	Low	1
- Customers, partners	Medium	2
- Children, vulnerable groups	High	3

Overall Risk: - 4-6 points: Low risk - 7-9 points: Medium risk (notification required) - 10-12 points: High risk (notification + communication required)

29.4.3.2 3.2 Check Notification Obligation

Decision Tree:

```
Data breach confirmed?
  No → Document, no further action required
  Yes → Risk to rights and freedoms?
      No (< 7 points) → Only document
      Yes (  7 points) → Notification to supervisory authority required
          High risk (  10 points)?
              No → Only notification
              Yes → Notification + Communication to data subjects
```

Responsible: Data Protection Officer

29.4.4 Phase 4: Notification and Communication (24-72 hours)

29.4.4.1 4.1 Notification to Supervisory Authority (if required)

Deadline: 72 hours from awareness

Competent Authority: - Name: [TODO: e.g., Data Protection Authority] - Notification Portal: [TODO: URL] - Contact: [TODO: Email, Phone]

Prepare Notification: - Use Template 0610 (Breach Notification Template) - Compile all required information - Have Data Protection Officer review - Obtain management approval

Responsible: Data Protection Officer

29.4.4.2 4.2 Communication to Data Subjects (if required)

Prerequisite: High risk (10 points)

Exceptions (no communication): - Data was encrypted/pseudonymized - Subsequent measures eliminate high risk - Disproportionate effort (then public communication)

Prepare Communication: - Use Template 0620 (Breach Communication Template) - Clear, understandable language - Concrete action recommendations - Contact options

Communication Channels: - Email (preferred) - Letter (if no email) - Public announcement (if disproportionate effort)

Responsible: Communications Lead, Data Protection Officer

29.4.4.3 4.3 Internal Communication

To inform: - Management - Affected departments - Works council (for employee data) - All employees (if needed)

Communication Plan: - Initial information: Within 24 hours - Regular updates: Daily during active phase - Final report: After incident closure

29.4.5 Phase 5: Recovery (72 hours - weeks)

29.4.5.1 5.1 Restore Systems

Checklist: - [ ] Security gaps closed - [ ] Systems patched/updated - [ ] Access controls reviewed - [ ] Monitoring enhanced - [ ] Backup strategy reviewed

Responsible: IT Security Lead

29.4.5.2 5.2 Preventive Measures

To implement: - Technical improvements - Process adjustments - Training - Enhanced monitoring

29.4.6 Phase 6: Post-Incident Review (After completion)

29.4.6.1 6.1 Post-Breach Review

Use Template 0640 (Post-Breach Review Template)

To be conducted within: 2 weeks after incident closure

Participants: - Breach Response Team - Affected departments - Management

Topics: - What went well? - What went poorly? - Lessons learned - Improvement measures

29.4.6.2 6.2 Complete Documentation

Checklist: - [ ] Breach register updated - [ ] All notifications archived - [ ] Timeline documented - [ ] Costs recorded - [ ] Measures documented

Retention Period: At least 3 years

29.5 Communication Guidelines

29.5.1 Internal Communication

Principles: - Transparent but confidential - Fact-based - Regular updates - Clear responsibilities

29.5.2 External Communication

Principles: - Only through authorized spokespersons - Coordinated with Legal and Data Protection Officer - No speculation - Focus on measures and support

Media Inquiries: - All inquiries to Communications Lead - No spontaneous statements - Preparation of Q&A

29.6 Escalation

29.6.1 Escalation Levels

Level 1: Routine - Low risk - < 100 data subjects - No special categories - Core team sufficient

Level 2: Elevated - Medium risk - 100-1,000 data subjects - Notification obligation - Inform management

Level 3: Critical - High risk - > 1,000 data subjects - Special categories - Communication obligation - Actively involve management - Consider external advisors

Level 4: Crisis - Very high risk - Massive impact - Public interest - Activate crisis management - External PR support - Inform supervisory board

29.7 Contacts and Resources

29.7.1 Internal Contacts

Role	Name	Phone	Email	Availability
Incident Commander	[TODO]	[TODO]	[TODO]	24/7
Data Protection Officer	[TODO]	[TODO]	[TODO]	24/7
IT Security Lead	[TODO]	[TODO]	[TODO]	24/7
Legal Counsel	[TODO]	[TODO]	[TODO]	Business hours
Communications Lead	[TODO]	[TODO]	[TODO]	Business hours

29.7.2 External Contacts

Organization	Contact	Phone	Email	Purpose
Supervisory Authority	[TODO]	[TODO]	[TODO]	Notification
Forensics Provider	[TODO]	[TODO]	[TODO]	Analysis
External Lawyer	[TODO]	[TODO]	[TODO]	Advice
PR Agency	[TODO]	[TODO]	[TODO]	Crisis communication
Cyber Insurance	[TODO]	[TODO]	[TODO]	Claim reporting

29.7.3 Tools and Systems

Tool	Purpose	Access
[TODO: SIEM]	Monitoring, log analysis	[TODO: URL]

Tool	Purpose	Access
[TODO: Ticketing System]	Incident tracking	[TODO: URL]
[TODO: Breach Register]	Documentation	[TODO: URL/File]
[TODO: Communication Platform]	Team coordination	[TODO: URL]

29.8 Appendices

- **Template 0610:** Breach Notification Template (Supervisory Authority)
- **Template 0620:** Breach Communication Template (Data Subjects)
- **Template 0630:** Breach Register Template
- **Template 0640:** Post-Breach Review Template

Next Steps: 1. Adapt this plan to your organization 2. Define all roles and contacts 3. Conduct breach response exercises (at least annually) 4. Keep the plan current 5. Ensure all team members know the plan

ewpage

Chapter 30

Breach Notification Template (Supervisory Authority)

Document-ID: 0610
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Classification: Confidential
Last Update: {{ meta.date }}

30.1 Notification of a Data Breach pursuant to Art. 33 GDPR

To: [TODO: Name of competent supervisory authority]
Date: [TODO: YYYY-MM-DD]
Breach-ID: [TODO: BREACH-YYYY-NNN]

30.1.1 1. Controller

Organization: {{ meta.organization }}
Address: [TODO: Full address]
Contact Person: [TODO: Name, Function]
Phone: [TODO: Phone number]
Email: [TODO: Email address]

30.1.2 2. Data Protection Officer

Name: [TODO: Name of Data Protection Officer]
Phone: [TODO: Phone number]
Email: [TODO: Email address]

30.2 A. Nature of the Breach (Art. 33(3)(a))

30.2.1 Description of the Data Breach

Date and Time of Breach:
[TODO: YYYY-MM-DD HH:MM - YYYY-MM-DD HH:MM]

Date and Time of Awareness:
[TODO: YYYY-MM-DD HH:MM]

Type of Breach:
[ ] Confidentiality breach (unauthorized disclosure or access)
[ ] Integrity breach (unauthorized alteration)
[ ] Availability breach (loss or destruction)

Detailed Description:
[TODO: Describe in detail what happened, how the breach occurred, which systems are affected]

Example:

```
On [Date] at [Time], it was discovered that due to a misconfiguration of the
web server, personal data of customers was publicly accessible for a period
of [Period]. The data was accessible via an unprotected API interface.
```

30.2.2 Categories of Personal Data Affected

Data Category	Description	Special Category (Art. 9)
[TODO: e.g., Master Data]	[TODO: Name, Address, Date of birth]	[ ] Yes [X] No
[TODO: e.g., Contact Data]	[TODO: Email, Phone]	[ ] Yes [X] No
[TODO: e.g., Financial Data]	[TODO: Account number, Credit card]	[ ] Yes [X] No

Special categories of personal data affected (Art. 9):
[ ] Yes [ ] No

If Yes, which:
[ ] Health data
[ ] Genetic data
[ ] Biometric data
[ ] Data revealing racial/ethnic origin
[ ] Political opinions
[ ] Religious/philosophical beliefs
[ ] Trade union membership
[ ] Sex life/sexual orientation

30.2.3 Categories of Data Subjects

Number of data subjects affected (approximate): [TODO: e.g., 1,234 persons]

Categories:
[ ] Customers
[ ] Employees
[ ] Suppliers/Partners
[ ] Patients
[ ] Children
[ ] Other: [TODO]

Vulnerable groups affected:
[ ] Yes [ ] No

If Yes, which: [TODO: e.g., Children, Patients, Disabled persons]

30.2.4 Number of Data Records Affected

Approximate number: [TODO: e.g., 5,000 records]

30.3 B. Contact Point (Art. 33(3)(b))

Name and contact details of the Data Protection Officer:

Name: [TODO: Name]
Phone: [TODO: Phone number]
Email: [TODO: Email address]
Availability: [TODO: e.g., Mon-Fri 9am-5pm, Emergency 24/7]

Alternative Contact Point:

Name: [TODO: Name, Function]
Phone: [TODO: Phone number]
Email: [TODO: Email address]

30.4 C. Likely Consequences (Art. 33(3)(c))

30.4.1 Description of Likely Consequences

For data subjects:

[TODO: Describe the possible impacts on the rights and freedoms of data subjects]

Examples: - Identity theft - Financial loss - Reputational damage - Discrimination - Loss of confidentiality - Psychological distress

Risk Assessment:
[ ] Low risk
[ ] Medium risk
[ ] High risk
[ ] Very high risk

Justification of Risk Assessment:
[TODO: Explain why the risk was assessed this way, considering type of data, number of data subjects, protective measures, etc.]

30.5 D. Measures Taken (Art. 33(3)(d))

30.5.1 Measures to Address the Data Breach

Immediate Measures (already taken):

1. [TODO: e.g., Isolated affected systems]
   - Time: [TODO: YYYY-MM-DD HH:MM]
   - Responsible: [TODO: Name/Role]
2. [TODO: e.g., Closed security gap]
   - Time: [TODO: YYYY-MM-DD HH:MM]
   - Responsible: [TODO: Name/Role]
3. [TODO: e.g., Reset passwords]
   - Time: [TODO: YYYY-MM-DD HH:MM]
   - Responsible: [TODO: Name/Role]

30.5.2 Measures to Mitigate Adverse Effects

Already implemented:

1. [TODO: e.g., Notified data subjects]
   - Time: [TODO: YYYY-MM-DD]
   - Method: [TODO: Email/Letter/Phone]
2. [TODO: e.g., Enhanced monitoring]
   - Time: [TODO: YYYY-MM-DD]
   - Description: [TODO]

Planned Measures:

1. [TODO: e.g., Implementation of additional security measures]
   - Planned time: [TODO: YYYY-MM-DD]
   - Responsible: [TODO: Name/Role]
2. [TODO: e.g., Employee training]
   - Planned time: [TODO: YYYY-MM-DD]
   - Responsible: [TODO: Name/Role]

30.6 E. Communication to Data Subjects (Art. 34)

Were data subjects notified?
[ ] Yes [ ] No [ ] Planned

If Yes: - Time: [TODO: YYYY-MM-DD] - Method: [TODO: Email/Letter/Public announcement] - Number of notified persons: [TODO]

If No, justification:
[ ] No high risk to rights and freedoms
[ ] Data was encrypted/pseudonymized
[ ] Subsequent measures eliminate high risk
[ ] Disproportionate effort (public announcement planned)

Explanation:
[TODO: Justify why no communication occurred or why the chosen method is appropriate]

30.7 F. Cross-Border Processing

Is there cross-border processing?
[ ] Yes [ ] No

If Yes: - Main establishment: [TODO: Country] - Other affected Member States: [TODO: Countries] - Lead supervisory authority: [TODO: Name]

30.8 G. Processor Involved

Is a processor involved?
[ ] Yes [ ] No

If Yes:

Processor	Role	Notified	Time
[TODO: Name]	[TODO: e.g., Cloud provider]	[ ] Yes [ ] No	[TODO: YYYY-MM-DD]

30.9 H. Additional Information

Previous data breaches:
[ ] Yes [ ] No

If Yes, number in last 12 months: [TODO]

Insurance:
[ ] Cyber insurance available
[ ] Insurance notified on: [TODO: YYYY-MM-DD]

External Support:
[ ] Forensics provider involved
[ ] Lawyer consulted
[ ] Other: [TODO]

Media Coverage:
[ ] Yes [ ] No [ ] Expected

Criminal Complaint Filed:
[ ] Yes [ ] No [ ] Planned

If Yes: - Authority: [TODO: e.g., Police, Prosecutor] - Case number: [TODO] - Date: [TODO: YYYY-MM-DD]

30.10 I. Attachments

[ ] Timeline of events
[ ] Technical report
[ ] Forensic analysis
[ ] Communication to data subjects (sample)
[ ] Other: [TODO]

30.11 J. Declaration

I hereby confirm that the above information is complete and truthful to the best of my knowledge and belief.

Place, Date: [TODO: Place, YYYY-MM-DD]

Name: [TODO: Name of Controller/Data Protection Officer]

Function: [TODO: Function]

Signature: _____

30.12 K. Submission Notes

Submit to:
[TODO: Name of supervisory authority]
[TODO: Address]
[TODO: Email]
[TODO: Online portal URL]

Deadline: 72 hours from awareness (Art. 33(1))

If deadline exceeded:
Include justification for delay (Art. 33(1))

Subsequent submission of information:
If not all information is immediately available, it can be submitted in phases (Art. 33(4))

Internal Notes:

Created by: [TODO: Name]
Reviewed by: [TODO: Data Protection Officer]
Approved by: [TODO: Management]
Submitted on: [TODO: YYYY-MM-DD HH:MM]
Authority case number: [TODO: Enter after receipt]

ewpage

Chapter 31

Breach Communication Template (Data Subjects)

Document-ID: 0620
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Classification: Confidential
Last Update: {{ meta.date }}

31.1 Email Template

Subject: Important Information About Your Data at {{ meta.organization }}

Dear [Salutation] [Name],

We are informing you about an incident affecting your personal data that we process.

31.1.1 What happened?

[TODO: Describe in clear, understandable language what happened. Avoid technical jargon.]

Example:

```
On [Date], we discovered that due to a technical error, personal data of
customers was temporarily accessible to unauthorized parties. The error was
fixed on [Date].
```

31.1.2 Which of your data is affected?

[TODO: List the affected data categories]

Example: - Your name - Your email address - Your phone number - [Additional data]

Not affected: [TODO: e.g., Passwords, payment data]

31.1.3 What impact could this have on you?

[TODO: Explain honestly and transparently the possible consequences]

Example:

```
There is a risk that third parties could use your contact data for
unwanted advertising or phishing attempts.
```

31.1.4 What have we done?

[TODO: Describe the measures taken]

Example: 1. We immediately fixed the error 2. We strengthened our security measures 3. We informed the competent data protection authority 4. We initiated a comprehensive investigation

31.1.5 What should you do now?

[TODO: Provide concrete, actionable recommendations]

Recommendations:

1. **Be vigilant for suspicious emails or calls**
   - Do not open attachments from unknown senders
   - Do not click on suspicious links
   - Do not disclose personal information
2. **[If passwords affected] Change your password**
   - Use a strong, unique password
   - Also change passwords for other services if you use the same password
3. **[If financial data affected] Check your account statements**
   - Watch for unusual transactions
   - Contact your bank immediately if you notice anything suspicious
4. **[If credentials affected] Enable two-factor authentication**
   - This provides additional protection for your account

31.1.6 Your contact options

If you have questions or need support, we are happy to help:

Data Protection Officer:
[TODO: Name]
Email: [TODO: Email address]
Phone: [TODO: Phone number]
Availability: [TODO: e.g., Mon-Fri 9am-5pm]

Customer Service:
Email: [TODO: Email address]
Phone: [TODO: Phone number]
Availability: [TODO: e.g., Mon-Fri 8am-6pm]

31.1.7 Your rights

You have the right to: - Obtain information about your data - Request correction of incorrect data - Request deletion of your data - File a complaint with the data protection authority

Competent Supervisory Authority:
[TODO: Name of authority]
Website: [TODO: URL]
Email: [TODO: Email address]

31.1.8 Further information

Further information about this incident can be found on our website:
[TODO: URL to FAQ or information page]

We take the protection of your data very seriously and regret this incident. We have taken comprehensive measures to ensure that such an incident does not happen again.

Sincerely,

[TODO: Name]
[TODO: Function]
{{ meta.organization }}

Appendix: [Optional: Detailed technical information, FAQ]

ewpage

Chapter 32

Breach Register (Record of Data Breaches)

Document-ID: 0630
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Classification: Confidential
Last Update: {{ meta.date }}

32.1 Purpose

This register documents all data breaches at {{ meta.organization }} according to Art. 33(5) GDPR. It serves accountability and enables the supervisory authority to verify compliance with notification obligations.

32.2 Responsibilities

Register Owner: [TODO: Name, Function]
Data Protection Officer: [TODO: Name]
Access Authorized: [TODO: Roles/Persons]

32.3 Retention Period

At least 3 years after incident closure

32.4 Breach Register

32.4.1 Breach Entry: [BREACH-YYYY-NNN]

32.4.1.1 1. Basic Information

Field	Value
Breach-ID	[TODO: BREACH-2024-001]
Status	[ ] Open [ ] In Progress [ ] Closed
Discovery Date	[TODO: YYYY-MM-DD HH:MM]
Awareness Date	[TODO: YYYY-MM-DD HH:MM]
Closure Date	[TODO: YYYY-MM-DD]
Discoverer	[TODO: Name, Department]
Incident Commander	[TODO: Name]

32.4.1.2 2. Nature of Breach

Field	Value
Category	[ ] Confidentiality [ ] Integrity [ ] Availability
Brief Description	[TODO: 1-2 sentences]
Detailed Description	[TODO: Comprehensive description]
Cause	[TODO: e.g., Misconfiguration, Hacking, Human error]
Affected Systems	[TODO: List of systems]

32.4.1.3 3. Affected Data and Persons

Field	Value
Data Categories	[TODO: e.g., Name, Email, Address]
Special Categories (Art. 9)	[ ] Yes [ ] No - If Yes: [TODO]
Number of Data Subjects	[TODO: Number]
Categories of Data Subjects	[TODO: e.g., Customers, Employees]
Vulnerable Groups	[ ] Yes [ ] No - If Yes: [TODO]
Number of Data Records	[TODO: Number]

32.4.1.4 4. Risk Assessment

Field	Value
Risk to Data Subjects	[ ] Low [ ] Medium [ ] High [ ] Very High
Risk Points	[TODO: 4-12 points]
Justification	[TODO: Explanation of risk assessment]
Possible Consequences	[TODO: e.g., Identity theft, Financial losses]

32.4.1.5 5. Notification Obligation and Communication

Field	Value
Notification to Authority	[ ] Yes [ ] No
Justification	[TODO: Why Yes/No]
Notified on	[TODO: YYYY-MM-DD HH:MM]
Deadline met (72h)	[ ] Yes [ ] No
Authority Case Number	[TODO: If available]
Communication to Data Subjects	[ ] Yes [ ] No [ ] Not required
Communicated on	[TODO: YYYY-MM-DD]
Number of Notified Persons	[TODO: Number]
Communication Method	[TODO: Email/Letter/Public]

32.4.1.6 6. Measures Taken

Immediate Measures:

Measure	Time	Responsible	Status
[TODO: e.g., Isolated systems]	[TODO: YYYY-MM-DD HH:MM]	[TODO: Name]	[ ] Done
[TODO: e.g., Blocked access]	[TODO: YYYY-MM-DD HH:MM]	[TODO: Name]	[ ] Done

Remedial Measures:

Measure	Time	Responsible	Status
[TODO: e.g., Closed security gap]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Done
[TODO: e.g., Enhanced monitoring]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Done

Preventive Measures:

Measure	Planned for	Responsible	Status
[TODO: e.g., Employee training]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Planned [ ] Implemented
[TODO: e.g., Process adjustment]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Planned [ ] Implemented

32.4.1.7 7. Costs and Impact

Field	Value
Direct Costs	[TODO: EUR/USD]
Indirect Costs	[TODO: EUR/USD]
Insurance Benefit	[TODO: EUR/USD]
Reputational Damage	[ ] Yes [ ] No
Media Coverage	[ ] Yes [ ] No
Data Subject Complaints	[TODO: Number]

32.4.1.8 8. Involved Parties

Role	Name/Organization	Contact
Data Protection Officer	[TODO]	[TODO]
IT Security	[TODO]	[TODO]
Legal	[TODO]	[TODO]
Processor	[TODO]	[TODO]
Forensics Provider	[TODO]	[TODO]
Supervisory Authority	[TODO]	[TODO]

32.4.1.9 9. Documentation

Document	Location	Created on
Initial Report	[TODO: Path/URL]	[TODO: YYYY-MM-DD]
Technical Report	[TODO: Path/URL]	[TODO: YYYY-MM-DD]
Forensic Analysis	[TODO: Path/URL]	[TODO: YYYY-MM-DD]
Authority Notification	[TODO: Path/URL]	[TODO: YYYY-MM-DD]
Data Subject Communication	[TODO: Path/URL]	[TODO: YYYY-MM-DD]
Post-Breach Review	[TODO: Path/URL]	[TODO: YYYY-MM-DD]

32.4.1.10 10. Lessons Learned

What went well: - [TODO: Positive aspects]

What went poorly: - [TODO: Areas for improvement]

Improvement Measures: - [TODO: Concrete measures]

Process Adjustments: - [TODO: Process changes]

32.4.1.11 11. Closure

Field	Value
Closed on	[TODO: YYYY-MM-DD]
Closed by	[TODO: Name, Function]
DPO Approval	[ ] Yes - Date: [TODO]

Field	Value
Management Approval	[ ] Yes - Date: [TODO]

32.5 Statistics and Overview

32.5.1 Annual Overview [YYYY]

Month	Number of Breaches	Notified	Communicated	Status
January	[TODO]	[TODO]	[TODO]	[TODO]
February	[TODO]	[TODO]	[TODO]	[TODO]
March	[TODO]	[TODO]	[TODO]	[TODO]
April	[TODO]	[TODO]	[TODO]	[TODO]
May	[TODO]	[TODO]	[TODO]	[TODO]
June	[TODO]	[TODO]	[TODO]	[TODO]
July	[TODO]	[TODO]	[TODO]	[TODO]
August	[TODO]	[TODO]	[TODO]	[TODO]
September	[TODO]	[TODO]	[TODO]	[TODO]
October	[TODO]	[TODO]	[TODO]	[TODO]
November	[TODO]	[TODO]	[TODO]	[TODO]
December	[TODO]	[TODO]	[TODO]	[TODO]
Total	**[TODO]**	**[TODO]**	**[TODO]**	

32.5.2 Categorization

Category	Number	Percent
Confidentiality Breach	[TODO]	[TODO]%
Integrity Breach	[TODO]	[TODO]%
Availability Breach	[TODO]	[TODO]%

32.5.3 Causes

Cause	Number	Percent
Human Error	[TODO]	[TODO]%
Technical Failure	[TODO]	[TODO]%
External Attacks	[TODO]	[TODO]%
Processor	[TODO]	[TODO]%
Other	[TODO]	[TODO]%

32.5.4 Trends and Insights

[TODO: Analysis of trends, common causes, improvement potential]

32.6 Access Control

32.6.1 Access Log

Date	User	Action	Breach-ID
[TODO]	[TODO]	[TODO: View/Edit/Export]	[TODO]

32.7 Audit Trail

32.7.1 Change History

Date	User	Breach-ID	Change	Justification
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Notes: - This register is confidential and may only be accessible to authorized persons - All entries must be complete and truthful - The register must be available for audits and upon request by the supervisory authority - Regular review and update required

ewpage

Chapter 33

Post-Breach Review Template

Document-ID: 0640
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Classification: Confidential
Last Update: {{ meta.date }}

33.1 Post-Breach Review

Breach-ID: [TODO: BREACH-YYYY-NNN]
Review Date: [TODO: YYYY-MM-DD]
Facilitator: [TODO: Name]

33.1.1 Participants

Name	Role	Department
[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]

33.2 1. Incident Summary

Brief Description:
[TODO: 2-3 sentences describing the incident]

Timeline:
- Start: [TODO: YYYY-MM-DD HH:MM] - Discovery: [TODO: YYYY-MM-DD HH:MM] - Closure: [TODO: YYYY-MM-DD HH:MM] - Total Duration: [TODO: X hours/days]

Impact:
- Number of Data Subjects: [TODO] - Data Categories: [TODO] - Risk Level: [TODO: Low/Medium/High]

33.3 2. Timeline Analysis

Time	Event	Responsible	Duration to Next Step
[TODO: HH:MM]	Incident occurs	-	-
[TODO: HH:MM]	Discovery	[TODO]	[TODO: X min/hrs]
[TODO: HH:MM]	Initial report	[TODO]	[TODO: X min/hrs]
[TODO: HH:MM]	Team activated	[TODO]	[TODO: X min/hrs]
[TODO: HH:MM]	Containment	[TODO]	[TODO: X min/hrs]
[TODO: HH:MM]	Authority notification	[TODO]	[TODO: X hrs]
[TODO: HH:MM]	Data subject communication	[TODO]	[TODO: X hrs]
[TODO: HH:MM]	Incident closed	[TODO]	-

Analysis:
[TODO: Were response times appropriate? Where were delays?]

33.4 3. What Went Well? (Positives)

33.4.1 3.1 Detection and Reporting

Positive Aspects: - [TODO: e.g., Quick detection through monitoring] - [TODO: e.g., Clear reporting channels worked]

33.4.2 3.2 Response and Containment

Positive Aspects: - [TODO: e.g., Team was well prepared] - [TODO: e.g., Technical measures worked quickly]

33.4.3 3.3 Communication

Positive Aspects: - [TODO: e.g., Clear internal communication] - [TODO: e.g., Professional external communication]

33.4.4 3.4 Documentation

Positive Aspects: - [TODO: e.g., Complete documentation] - [TODO: e.g., Breach register up to date]

33.5 4. What Went Poorly? (Areas for Improvement)

33.5.1 4.1 Detection and Reporting

Problems: - [TODO: e.g., Delayed detection] - [TODO: e.g., Unclear reporting channels]

Causes: - [TODO: Why did these problems occur?]

33.5.2 4.2 Response and Containment

Problems: - [TODO: e.g., Delayed response] - [TODO: e.g., Missing tools]

Causes: - [TODO: Why did these problems occur?]

33.5.3 4.3 Communication

Problems: - [TODO: e.g., Delayed notification] - [TODO: e.g., Unclear messages]

Causes: - [TODO: Why did these problems occur?]

33.5.4 4.4 Documentation

Problems: - [TODO: e.g., Incomplete documentation] - [TODO: e.g., Missing templates]

Causes: - [TODO: Why did these problems occur?]

33.6 5. Root Cause Analysis

Primary Cause:
[TODO: What was the main cause of the incident?]

Contributing Factors: - [TODO: Factor 1] - [TODO: Factor 2] - [TODO: Factor 3]

5-Why Analysis:

1. Why did the incident occur?
   [TODO: Answer]
2. Why [Answer from 1]?
   [TODO: Answer]
3. Why [Answer from 2]?
   [TODO: Answer]
4. Why [Answer from 3]?
   [TODO: Answer]
5. Why [Answer from 4]?
   [TODO: Root Cause]

33.7 6. Lessons Learned

33.7.1 6.1 Technical Insights

- [TODO: e.g., Monitoring gaps identified]
- [TODO: e.g., Security configuration insufficient]

33.7.2 6.2 Process Insights

- [TODO: e.g., Response plan needs update]
- [TODO: e.g., Escalation paths unclear]

33.7.3 6.3 Organizational Insights

- [TODO: e.g., Training needs identified]
- [TODO: e.g., Roles need clearer definition]

33.7.4 6.4 Communication Insights

- [TODO: e.g., Templates need improvement]
- [TODO: e.g., Optimize communication channels]

33.8 7. Improvement Measures

33.8.1 7.1 Immediate Actions (within 1 month)

Measure	Responsible	Deadline	Priority	Status
[TODO: e.g., Expand monitoring]	[TODO]	[TODO: YYYY-MM-DD]	High	[ ] Open
[TODO: e.g., Update response plan]	[TODO]	[TODO: YYYY-MM-DD]	High	[ ] Open

33.8.2 7.2 Medium-term Actions (1-3 months)

Measure	Responsible	Deadline	Priority	Status
[TODO: e.g., Conduct training]	[TODO]	[TODO: YYYY-MM-DD]	Medium	[ ] Open
[TODO: e.g., Document processes]	[TODO]	[TODO: YYYY-MM-DD]	Medium	[ ] Open

33.8.3 7.3 Long-term Actions (3-12 months)

Measure	Responsible	Deadline	Priority	Status
[TODO: e.g., Implement new tools]	[TODO]	[TODO: YYYY-MM-DD]	Low	[ ] Open
[TODO: e.g., Adjust organizational structure]	[TODO]	[TODO: YYYY-MM-DD]	Low	[ ] Open

---

33.9 8. Cost-Benefit Analysis

33.9.1 8.1 Incident Costs

Cost Type	Amount (EUR/USD)
Direct costs (forensics, external consultants)	[TODO]
Personnel costs (work time)	[TODO]
Notifications and communications	[TODO]
Reputational damage (estimated)	[TODO]
Total	**[TODO]**

33.9.2 8.2 Improvement Measure Costs

Measure	Estimated Cost (EUR/USD)
[TODO: Measure 1]	[TODO]
[TODO: Measure 2]	[TODO]
Total	**[TODO]**

33.9.3 8.3 Expected Benefits

[TODO: Describe expected benefits of measures, e.g., risk reduction, faster response times]

33.10 9. Response Plan Adjustments

Required Changes to Response Plan:

Section	Change	Justification
[TODO: e.g., Contacts]	[TODO: e.g., Add new contacts]	[TODO]
[TODO: e.g., Escalation]	[TODO: e.g., Adjust thresholds]	[TODO]

33.11 10. Training and Awareness Needs

Identified Training Needs:

Target Group	Topic	Format	Timeframe
[TODO: e.g., IT Team]	[TODO: e.g., Incident Response]	[TODO: Workshop]	[TODO: Q2 2024]
[TODO: e.g., All Staff]	[TODO: e.g., Data Breach Awareness]	[TODO: E-Learning]	[TODO: Q2 2024]

33.12 11. Follow-up and Monitoring

Next Steps:

Action	Responsible	Deadline
Create action plan	[TODO]	[TODO: YYYY-MM-DD]
Monthly review meeting	[TODO]	[TODO: Every 1st Monday]
Progress report to management	[TODO]	[TODO: YYYY-MM-DD]
Follow-up review (3 months)	[TODO]	[TODO: YYYY-MM-DD]

33.13 12. Closure and Approval

Summary:
[TODO: 2-3 sentences summarizing key findings and measures]

Approval:

Role	Name	Date	Signature
Facilitator	[TODO]	[TODO]	_____
Data Protection Officer	[TODO]	[TODO]	_____
Management	[TODO]	[TODO]	_____

Appendices: - [ ] Detailed timeline - [ ] Technical report - [ ] Communication materials - [ ] Action plan (detailed)

ewpage

Chapter 34

Appendix: Records of Processing Activities (Template)

Document-ID: 0700
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Classification: Internal
Last Update: {{ meta.date }}

34.1 Records of Processing Activities

Organization: {{ meta.organization }}
Controller: [TODO: Name, Function]
Data Protection Officer: [TODO: Name, Contact]
As of: {{ meta.date }}

34.2 Processing Activity [No. 1]

34.2.1 1. Name and Contact Details of Controller

Controller:
{{ meta.organization }}
[TODO: Address]
[TODO: Phone]
[TODO: Email]

Representative (if applicable):
[TODO: Name, Address, Contact]

Data Protection Officer:
[TODO: Name]

[TODO: Contact]

34.2.2 2. Purposes of Processing

Main Purpose:
[TODO: e.g., Customer management, HR management, Marketing]

Further Purposes:
- [TODO: Purpose 1] - [TODO: Purpose 2]

34.2.3 3. Categories of Data Subjects

- ☐ Customers
- ☐ Prospects
- ☐ Employees
- ☐ Applicants
- ☐ Suppliers/Partners
- ☐ Website visitors
- ☐ Other: [TODO]

34.2.4 4. Categories of Personal Data

General Data: - [ ] Master data (Name, Address, Date of birth) - [ ] Contact data (Email, Phone) - [ ] Contract data - [ ] Payment data - [ ] Usage data - [ ] Other: [TODO]

Special Categories (Art. 9): - [ ] Health data - [ ] Genetic data - [ ] Biometric data - [ ] Data revealing racial/ethnic origin - [ ] Political opinions - [ ] Religious/philosophical beliefs - [ ] Trade union membership - [ ] Sex life/sexual orientation

34.2.5 5. Categories of Recipients

Internal Recipients:
[TODO: e.g., Sales, Accounting, IT]

External Recipients:
[TODO: e.g., Payment service providers, Shipping providers]

Processors:
[TODO: e.g., Cloud providers, IT service providers]

Third Country Transfer:
[ ] Yes [ ] No

If Yes: - Countries: [TODO] - Safeguards: [TODO: e.g., Standard contractual clauses, Adequacy decision]

34.2.6 6. Time Limits for Erasure

Standard Case:
[TODO: e.g., 3 years after contract end]

Legal Retention Obligations:
[TODO: e.g., 10 years commercial law, 6 years tax law]

Erasure Concept:
[TODO: Description or reference to document]

34.2.7 7. Technical and Organizational Measures (TOM)

Access Control:
[TODO: e.g., Access cards, Visitor registration]

Authentication Control:
[TODO: e.g., Passwords, Two-factor authentication]

Authorization Control:
[TODO: e.g., Authorization concept, Role model]

Disclosure Control:
[TODO: e.g., Encryption, VPN]

Input Control:
[TODO: e.g., Logging, Audit trails]

Job Control:
[TODO: e.g., Processor agreements]

Availability Control:
[TODO: e.g., Backup, Emergency plan]

Separation Control:
[TODO: e.g., Multi-tenancy, Data separation]

34.2.8 8. Legal Basis

Legal Basis:
[ ] Art. 6(1)(a) (Consent)
[ ] Art. 6(1)(b) (Contract performance)
[ ] Art. 6(1)(c) (Legal obligation)
[ ] Art. 6(1)(d) (Protection of vital interests)
[ ] Art. 6(1)(e) (Public interest)
[ ] Art. 6(1)(f) (Legitimate interest)

For Special Categories (Art. 9):
[ ] Art. 9(2)(a) (Explicit consent)
[ ] Art. 9(2)(b) (Employment law)
[ ] Art. 9(2)(c) (Protection of vital interests)
[ ] Art. 9(2)(d) (Foundations, associations)
[ ] Art. 9(2)(e) (Publicly disclosed data)
[ ] Art. 9(2)(f) (Legal claims)
[ ] Art. 9(2)(g) (Substantial public interest)
[ ] Art. 9(2)(h) (Healthcare)
[ ] Art. 9(2)(i) (Public health)
[ ] Art. 9(2)(j) (Archiving, research, statistics)

Explanation:
[TODO: Justification of legal basis]

34.2.9 9. Data Protection Impact Assessment (DPIA)

DPIA Required:
[ ] Yes [ ] No

If Yes:
- DPIA-ID: [TODO] - Conducted on: [TODO: YYYY-MM-DD] - Result: [TODO: Risk acceptable/not acceptable]

34.2.10 10. Additional Information

Data Sources:
[TODO: e.g., Directly from data subject, from third parties]

Automated Decision-Making:
[ ] Yes [ ] No

If Yes:
[TODO: Description of logic, significance, consequences]

Profiling:
[ ] Yes [ ] No

If Yes:
[TODO: Description]

34.3 Processing Activity [No. 2]

[TODO: Repeat structure for additional processing activities]

34.4 Overview of All Processing Activities

No.	Name	Purpose	Data Subjects	Legal Basis	DPIA
1	[TODO]	[TODO]	[TODO]	[TODO]	Yes/No
2	[TODO]	[TODO]	[TODO]	[TODO]	Yes/No
3	[TODO]	[TODO]	[TODO]	[TODO]	Yes/No

34.5 Change History

Version	Date	Change	Changed By
1.0	[TODO]	Initial version	[TODO]
1.1	[TODO]	[TODO: Description]	[TODO]

Notes: - This record must be updated upon changes - The record must be made available to the supervisory authority upon request - Regular review (at least annually) required

ewpage

Chapter 35

Appendix: DPIA Quick Reference

Document-ID: 0710
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Reference
Classification: Internal
Last Update: {{ meta.date }}

35.1 When is a DPIA Required?

35.1.1 Mandatory Cases (Art. 35(3))

A DPIA is **always** required for:

1. **Systematic and extensive evaluation of personal aspects**
   - Automated processing including profiling
   - Basis for decisions with legal effect or significant impact
2. **Large-scale processing of special categories (Art. 9)**
   - Health data, genetic data, biometric data
   - Data concerning criminal convictions and offences
3. **Systematic large-scale monitoring of publicly accessible areas**
   - Video surveillance
   - Tracking and monitoring

35.1.2 Supervisory Authority Blacklist

Additionally required for (examples): - Scoring and rating - Automated decisions with legal effect - Systematic monitoring - Processing sensitive data at large scale - Data matching or combination - Data of vulnerable persons (children, patients, employees) - Innovative technologies (AI, biometrics) - Third country transfer without adequacy decision

35.1.3 Threshold Criteria

Number of Data Subjects: - < 5,000: Usually no DPIA required - 5,000 - 20,000: DPIA recommended - > 20,000: DPIA usually required

Risk Factors (more applicable, more likely DPIA): - [ ] Evaluation or scoring - [ ] Automated decisions - [ ] Systematic monitoring - [ ] Special categories (Art. 9) - [ ] Vulnerable groups - [ ] Large-scale processing - [ ] Data matching - [ ] Innovative technology - [ ] Third country transfer - [ ] Prevention of rights exercise

Rule of thumb: With 2 or more risk factors → Conduct DPIA

35.2 DPIA Process (Quick Overview)

35.2.1 Phase 1: Preparation

1. **Check:** Is DPIA required?
2. **Form team:** Controller, DPO, IT, Business unit
3. **Gather information:** Processing description, data flows, systems

35.2.2 Phase 2: Execution

4. **Description:** Describe processing in detail
5. **Necessity:** Check necessity and proportionality
6. **Identify risks:** Systematic risk analysis
7. **Define measures:** Technical and organizational measures
8. **Assess residual risk:** Is residual risk acceptable?

35.2.3 Phase 3: Consultation

9. **Data Protection Officer:** Obtain opinion
10. **Data subjects (optional):** Seek views
11. **Supervisory authority (if required):** Consult if high residual risk

35.2.4 Phase 4: Documentation

12. **Document DPIA:** Use Template 0410
13. **Approval:** Controller approves
14. **Archiving:** Retain DPIA

35.3 Risk Assessment Matrix

35.3.1 Likelihood

Level	Description	Example
Low	Unlikely	Encrypted data, strong security measures
Medium	Possible	Standard security, known vulnerabilities

Level	Description	Example
High	Likely	Weak security, publicly accessible

35.3.2 Severity of Impact

Level	Description	Example
Low	Minor impact	General contact data, no sensitive data
Medium	Significant impact	Financial data, contract data
High	Severe impact	Health data, identity theft possible

35.3.3 Risk Matrix

	Low Severity	**Medium Severity**	**High Severity**
Low Likelihood	Low Risk	Medium Risk	Medium Risk
Medium Likelihood	Medium Risk	Medium Risk	High Risk
High Likelihood	Medium Risk	High Risk	Very High Risk

Action Recommendation: - **Low Risk:** Standard measures sufficient - **Medium Risk:** Additional measures required - **High Risk:** Comprehensive measures, possibly consult authority - **Very High Risk:** Consultation with authority required

---

35.4 Typical Measures

35.4.1 Technical Measures

- **Encryption:** End-to-end, transport, storage
- **Pseudonymization:** Separation of identification data
- **Anonymization:** Irreversible removal of personal data
- **Access control:** Role-based, Least Privilege
- **Logging:** Traceability, Audit trails
- **Backup:** Regular, tested
- **Monitoring:** Anomaly detection, Intrusion Detection

35.4.2 Organizational Measures

- **Policies:** Data protection policy, Security policy
- **Training:** Regular, target group-specific
- **Contracts:** Processor agreements, NDAs
- **Processes:** Incident response, Erasure concept
- **Documentation:** Processing records, TOMs
- **Audits:** Regular reviews

35.4.3 Privacy by Design/Default

- **Data minimization:** Collect only necessary data
- **Purpose limitation:** Clear purpose definition
- **Storage limitation:** Automatic deletion
- **Transparency:** Clear information for data subjects
- **User-friendliness:** Easy exercise of rights

35.5 Checklist: DPIA Required?

☐ Systematic and extensive evaluation of personal aspects?
☐ Automated decisions with legal effect?
☐ Large-scale processing of special categories (Art. 9)?
☐ Systematic monitoring of publicly accessible areas?
☐ Scoring or rating?
☐ Processing sensitive data at large scale?
☐ Data matching or combination?
☐ Data of vulnerable persons (children, patients)?
☐ Innovative technologies (AI, biometrics)?
☐ Third country transfer without adequacy decision?
☐ More than 20,000 data subjects?
☐ 2 or more risk factors apply?

If 1 or more questions answered Yes: Conduct DPIA!

35.6 Prior Consultation with Supervisory Authority

Required when: - Residual risk remains high despite measures - No adequate measures possible - Uncertainty about adequacy of measures

Process: 1. Complete DPIA fully 2. Document all possible measures 3. Request to supervisory authority with DPIA documentation 4. Authority has 8 weeks (extendable to 14 weeks) 5. Implement authority's opinion

---

35.7 Avoid Common Mistakes

Conduct DPIA too late → Before processing starts!
Superficial risk analysis → Systematic and detailed!
Not involving DPO → Always consult!
No concrete measures → Specific and implementable!
Not updating DPIA → Review upon changes!
No documentation → Document completely!

35.8 Useful Resources

Templates: - Template 0410: DPIA Template - Template 0400: DPIA Fundamentals

External Resources: - WP29 Guidelines on DPIA (wp248rev.01) - Supervisory authority blacklists - DPIA tools from supervisory authorities

Contact: - Data Protection Officer: [TODO: Contact] - Supervisory Authority: [TODO: Contact]

ewpage

Chapter 36

Appendix: Data Processing Agreement (DPA) Template

Document-ID: 0720
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Classification: Confidential
Last Update: {{ meta.date }}

36.1 Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR

between

Controller (Principal):
{{ meta.organization }}
[TODO: Address]
[TODO: Authorized representative]

hereinafter “Principal”

and

Processor (Contractor):
[TODO: Name of Processor]
[TODO: Address]
[TODO: Authorized representative]

hereinafter “Contractor”

36.2 Preamble

The Principal engages the Contractor for services where the Contractor processes personal data on behalf of the Principal. This agreement regulates the rights and obligations of the parties in connection with this processing pursuant to Art. 28 GDPR.

36.3 § 1 Subject Matter and Duration

36.3.1 1.1 Subject Matter

The Contractor processes personal data on behalf of the Principal in the context of the following services:

[TODO: e.g., Cloud hosting, IT support, Payroll processing, Marketing services]

36.3.2 1.2 Duration

This agreement enters into force upon signature and applies for the duration of the main service. It ends automatically upon termination of the main service or can be terminated by either party with [TODO: e.g., 3 months] notice.

36.4 § 2 Type and Purpose of Processing

36.4.1 2.1 Type of Processing

[ ] Collection
[ ] Recording
[ ] Organization
[ ] Structuring
[ ] Storage
[ ] Adaptation
[ ] Alteration
[ ] Retrieval
[ ] Consultation
[ ] Use
[ ] Disclosure by transmission
[ ] Dissemination
[ ] Making available
[ ] Alignment
[ ] Combination
[ ] Restriction
[ ] Erasure
[ ] Destruction

36.4.2 2.2 Purpose of Processing

[TODO: e.g., Provision of cloud storage for customer data, Processing of payroll data]

36.5 § 3 Scope of Processing

36.5.1 3.1 Categories of Data Subjects

[TODO: e.g., Customers, Employees, Suppliers]

36.5.2 3.2 Categories of Personal Data

General Data:
[TODO: e.g., Name, Address, Email, Phone]

Special Categories (Art. 9):
[ ] Yes [ ] No

If Yes: [TODO: e.g., Health data, Biometric data]

36.5.3 3.3 Volume

Estimated number of data subjects: [TODO: e.g., 10,000]
Estimated data volume: [TODO: e.g., 100 GB]

36.6 § 4 Obligations of Contractor

36.6.1 4.1 Instructions

The Contractor processes personal data exclusively according to documented instructions from the Principal. Instructions may be given in writing, electronically, or orally (with written confirmation).

Authorized persons at Principal:
[TODO: Name, Function, Contact]

Instruction recipients at Contractor:
[TODO: Name, Function, Contact]

36.6.2 4.2 Confidentiality

The Contractor ensures that all persons involved in processing have committed to confidentiality or are subject to appropriate statutory confidentiality obligations.

36.6.3 4.3 Technical and Organizational Measures (TOM)

The Contractor implements and maintains appropriate technical and organizational measures according to Annex 1 (TOM).

36.6.4 4.4 Support Obligations

The Contractor supports the Principal with: - Responding to data subject requests - Reporting data breaches - Conducting data protection impact assessments - Prior consultations with supervisory authorities

36.6.5 4.5 Deletion and Return

After termination of services, the Contractor deletes or returns all personal data unless a legal retention obligation exists.

Deadline: [TODO: e.g., 30 days after contract end]

36.7 § 5 Sub-processing

36.7.1 5.1 Authorization

The Contractor may only engage sub-processors with prior written authorization from the Principal.

Already authorized sub-processors:

Name	Service	Location
[TODO]	[TODO]	[TODO]

36.7.2 5.2 Information Obligation

The Contractor informs the Principal of planned changes (addition or replacement) of sub-processors. The Principal may object within [TODO: e.g., 14 days].

36.7.3 5.3 Obligations

The Contractor ensures that sub-processors fulfill the same data protection obligations as set out in this agreement.

36.8 § 6 Rights and Obligations of Principal

36.8.1 6.1 Right to Instruct

The Principal has the right to issue instructions for data processing at any time.

36.8.2 6.2 Control Rights

The Principal or an appointed auditor has the right to: - Obtain information - Conduct inspections - Conduct audits

Notice period: [TODO: e.g., 14 days]

36.8.3 6.3 Responsibility

The Principal remains responsible for compliance with data protection regulations.

36.9 § 7 Data Breaches

36.9.1 7.1 Notification Obligation

The Contractor reports data breaches without undue delay, at the latest within [TODO: e.g., 24 hours] to the Principal.

Contact at Principal:
[TODO: Name, Phone, Email]

36.9.2 7.2 Support

The Contractor supports the Principal in fulfilling notification obligations pursuant to Art. 33-34 GDPR.

36.10 § 8 Liability and Damages

36.10.1 8.1 Liability

Both parties are liable pursuant to Art. 82 GDPR for damages arising from processing.

36.10.2 8.2 Indemnification

The Contractor indemnifies the Principal from third-party claims arising from the Contractor's violations of this agreement.

36.11 § 9 Data Protection Officers

Data Protection Officer of Principal:
[TODO: Name, Contact]

Data Protection Officer of Contractor:
[TODO: Name, Contact]

36.12 § 10 Final Provisions

36.12.1 10.1 Amendments

Amendments and supplements to this agreement require written form.

36.12.2 10.2 Severability Clause

If individual provisions are invalid, the validity of the remaining provisions remains unaffected.

36.12.3 10.3 Applicable Law

The law of [TODO: e.g., Federal Republic of Germany] applies.

36.12.4 10.4 Place of Jurisdiction

Place of jurisdiction is [TODO: e.g., Munich].

36.13 Signatures

Principal:

Place, Date: _____

Name: _____

Signature: _____

Contractor:

Place, Date: _____

Name: _____

Signature: _____

36.14 Annex 1: Technical and Organizational Measures (TOM)

36.14.1 1. Access Control

[TODO: e.g., Access cards, Visitor registration, Security personnel]

36.14.2 2. Authentication Control

[TODO: e.g., Passwords, Two-factor authentication, Biometrics]

36.14.3 3. Authorization Control

[TODO: e.g., Role-based permissions, Least Privilege, Need-to-know]

36.14.4 4. Disclosure Control

[TODO: e.g., Encryption, VPN, Secure transmission protocols]

36.14.5 5. Input Control

[TODO: e.g., Logging, Audit trails, Versioning]

36.14.6 6. Job Control

[TODO: e.g., Clear contracts, Instruction documentation, Controls]

36.14.7 7. Availability Control

[TODO: e.g., Backup, Redundancy, Emergency plan, Disaster recovery]

36.14.8 8. Separation Control

[TODO: e.g., Multi-tenancy, Data separation, Separate environments]

36.14.9 9. Data Protection Management

[TODO: e.g., Data Protection Officer, Policies, Training]

36.14.10 10. Incident Response

[TODO: e.g., Incident response plan, Reporting channels, Escalation]

Note: This template is a template and must be adapted to specific requirements. Legal review is recommended.

ewpage

Chapter 37

Appendix: Terms and Abbreviations

Document-ID: 0730
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Reference
Classification: Public
Last Update: {{ meta.date }}

37.1 Abbreviations

Abbreviation	Meaning	German
GDPR	General Data Protection Regulation	DSGVO (Datenschutz-Grundverordnung)
DSGVO	Datenschutz-Grundverordnung	GDPR (General Data Protection Regulation)
DPO	Data Protection Officer	DSB (Datenschutzbeauftragter)
DSB	Datenschutzbeauftragter	DPO (Data Protection Officer)
DPIA	Data Protection Impact Assessment	DSFA (Datenschutz-Folgenabschätzung)
DSFA	Datenschutz-Folgenabschätzung	DPIA (Data Protection Impact Assessment)
DPA	Data Processing Agreement	AVV (Auftragsverarbeitungsvertrag)
AVV	Auftragsverarbeitungsvertrag	DPA (Data Processing Agreement)
TOMs	Technical and Organizational Measures	TOM (Technische und organisatorische Maßnahmen)
SCC	Standard Contractual Clauses	Standardvertragsklauseln

Abbreviation	Meaning	German
BCR	Binding Corporate Rules	Verbindliche interne Datenschutzvorschriften
PbD	Privacy by Design	Datenschutz durch Technikgestaltung
PbD	Privacy by Default	Datenschutz durch datenschutzfreundliche Voreinstellungen
CJEU	Court of Justice of the European Union	EuGH (Europäischer Gerichtshof)
EDPB	European Data Protection Board	EDSA (Europäischer Datenschutzausschuss)
EDSA	Europäischer Datenschutzausschuss	EDPB (European Data Protection Board)

37.2 Term Definitions (Art. 4 GDPR)

37.2.1 Personal Data (Art. 4(1))

Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly.

Examples: - Name, address, date of birth - Email address, phone number - IP address, cookie ID - Location data, usage data - Photo, video, audio recording

37.2.2 Processing (Art. 4(2))

Any operation performed on personal data, such as: - Collection, recording, organization - Structuring, storage, adaptation, alteration - Retrieval, consultation, use - Disclosure, transmission, dissemination - Alignment, combination, restriction - Erasure, destruction

37.2.3 Restriction of Processing (Art. 4(3))

Marking of stored personal data with the aim of limiting their processing in the future.

37.2.4 Profiling (Art. 4(4))

Any form of automated processing to evaluate personal aspects, in particular to analyze or predict: - Work performance - Economic situation - Health - Personal preferences - Interests - Reliability - Behavior - Location - Movements

37.2.5 Pseudonymization (Art. 4(5))

Processing of personal data in such a manner that the data can no longer be attributed to a specific person without the use of additional information.

Example: Replacement of names with pseudonyms (IDs), with the mapping table stored separately.

37.2.6 Filing System (Art. 4(6))

Any structured set of personal data accessible according to specific criteria.

37.2.7 Controller (Art. 4(7))

The natural or legal person who, alone or jointly with others, determines the purposes and means of processing.

Example: Company processing customer data

37.2.8 Processor (Art. 4(8))

A natural or legal person who processes personal data on behalf of the controller.

Examples: - Cloud providers - IT service providers - Payroll service providers - Marketing agencies

37.2.9 Recipient (Art. 4(9))

A natural or legal person to whom personal data are disclosed.

37.2.10 Third Party (Art. 4(10))

A natural or legal person other than the data subject, controller, processor, and persons authorized to process data under the direct authority of the controller or processor.

37.2.11 Consent (Art. 4(11))

Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of their personal data.

Requirements: - Freely given - Informed - Specific - Unambiguous - Revocable

37.2.12 Personal Data Breach (Art. 4(12))

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Categories: - Confidentiality breach - Integrity breach - Availability breach

37.2.13 Genetic Data (Art. 4(13))

Personal data relating to the inherited or acquired genetic characteristics of a natural person.

37.2.14 Biometric Data (Art. 4(14))

Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow their unique identification.

Examples: - Fingerprints - Facial recognition - Iris scan - Voice recognition

37.2.15 Data Concerning Health (Art. 4(15))

Personal data related to the physical or mental health of a natural person, including information about their health status.

Examples: - Diagnoses - Treatments - Medications - Laboratory values - Medical history

37.2.16 Main Establishment (Art. 4(16))

For a controller with establishments in more than one Member State, the place of its central administration in the Union.

37.2.17 Representative (Art. 4(17))

A natural or legal person established in the Union who is designated in writing by a controller or processor not established in the Union.

37.2.18 Enterprise (Art. 4(18))

A natural or legal person engaged in an economic activity.

37.2.19 Group of Undertakings (Art. 4(19))

A controlling undertaking and its controlled undertakings.

37.2.20 Binding Corporate Rules (Art. 4(20))

Personal data protection policies adhered to by a controller or processor for transfers of personal data.

37.2.21 Supervisory Authority (Art. 4(21))

An independent public authority established by a Member State to monitor the application of GDPR.

Germany: Federal and State Data Protection Commissioners

37.2.22 Supervisory Authority Concerned (Art. 4(22))

A supervisory authority affected by processing because: - The controller or processor is established in its Member State - Data subjects in its Member State are substantially affected - A complaint has been lodged with it

37.2.23 Cross-border Processing (Art. 4(23))

Processing that: - Takes place in the context of activities of establishments of a controller or processor in more than one Member State, or - Substantially affects data subjects in more than one Member State

37.2.24 Relevant and Reasoned Objection (Art. 4(24))

An objection by a supervisory authority concerned to a draft decision as to whether there is an infringement of GDPR.

37.2.25 Information Society Service (Art. 4(25))

A service as defined in Article 1(1)(b) of Directive (EU) 2015/1535.

Examples: - Online shops - Social networks - Cloud services - Streaming services

37.2.26 International Organisation (Art. 4(26))

An organization and its subordinate bodies governed by public international law, or any other body set up by an agreement between two or more countries.

37.3 Additional Important Terms

37.3.1 Special Categories of Personal Data (Art. 9)

Sensitive data requiring special protection: - Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Genetic data - Biometric data for unique identification - Health data - Data concerning sex life or sexual orientation

37.3.2 Anonymization

Irreversible removal of personal reference so that data can no longer be attributed to a person.

Difference from Pseudonymization: Anonymization is irreversible, pseudonymization is reversible.

37.3.3 Privacy by Design

Implementation of data protection principles already during the development of systems and processes.

37.3.4 Privacy by Default

Default settings that maximize data protection (e.g., only necessary data is processed).

37.3.5 Third Country

A country outside the European Union and the European Economic Area.

37.3.6 Adequacy Decision

Decision by the EU Commission that a third country provides an adequate level of data protection.

Examples: Switzerland, United Kingdom (post-Brexit), Japan

37.3.7 Standard Contractual Clauses (SCC)

Contractual clauses approved by the EU Commission for data transfers to third countries.

37.3.8 Accountability

Obligation of the controller to demonstrate compliance with GDPR.

37.3.9 Data Protection Impact Assessment (DPIA)

Systematic assessment of the risks of processing for the rights and freedoms of data subjects.

37.3.10 Records of Processing Activities

Documentation of all processing activities of a controller or processor (Art. 30).

37.3.11 Data Subject Rights

Rights of natural persons vis-à-vis the controller: - Right of access (Art. 15) - Right to rectification (Art. 16) - Right to erasure (Art. 17) - Right to restriction (Art. 18) - Right to data portability (Art. 20) - Right to object (Art. 21) - Right to withdraw consent (Art. 7)

37.4 Legal Bases (Art. 6(1))

Letter	Legal Basis	Description
a	Consent	Data subject has given consent
b	Contract	Necessary for performance of a contract
c	Legal obligation	Necessary for compliance with legal obligation
d	Vital interests	Necessary to protect vital interests
e	Public interest	Necessary for task in public interest
f	Legitimate interests	Necessary for legitimate interests

37.5 Sanctions and Fines

37.5.1 Fine Categories

Category 1 (up to EUR 10 million or 2% of annual turnover): - Violations of processor obligations (Art. 28-29) - Violations of certification bodies (Art. 42-43)

Category 2 (up to EUR 20 million or 4% of annual turnover): - Violations of principles (Art. 5) - Violations of legal bases (Art. 6) - Violations of data subject rights (Art. 12-22) - Violations of data transfers (Art. 44-49)

Note: These definitions are based on GDPR and serve as a reference. For legal questions, a data protection expert or lawyer should be consulted.

ewpage