[Logo der Organisation]

[Name der Organisation]

**PROJEKTPLAN**  
**für die Umsetzung des Informationssicherheits-Managementsystems und für die Einhaltung der europäischen Datenschutz-Grundverordnung**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Datum der Version: |  |
| Erstellt durch: |  |
| Genehmigt durch: |  |
| Vertraulichkeitsstufe: |  |

**Änderungs-Historie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Erstellt durch** | **Beschreibung der Änderung** |
| TT.MM.JJJJ | 0.1 | EUGDPRAcademy | Erster Entwurf des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Anwender 3](#_Toc504979205)

[2. Referenzdokumente 3](#_Toc504979206)

[3. ISMS Einführungsprojekt 3](#_Toc504979207)

[3.1. Ziel des Projekts 3](#_Toc504979208)

[3.2. Ergebnisse des Projekts 3](#_Toc504979209)

[3.3. Fristen 6](#_Toc504979210)

[3.4. Projekt-Organisation 6](#_Toc504979211)

[3.4.1. Projekt-Sponsor 6](#_Toc504979212)

[3.4.2. Projektmanager 6](#_Toc504979213)

[3.4.3. Projektteam 6](#_Toc504979214)

[3.5. Hauptrisiken im Projekt 7](#_Toc504979215)

[3.6. Werkzeuge für Projekt-Umsetzung, Berichtswesen 7](#_Toc504979216)

[4. Verwaltung von Aufzeichnungen zu diesem Dokument 7](#_Toc504979217)

[5. Gültigkeit und Dokumenten-Handhabung 8](#_Toc504979218)

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Projektplans ist die eindeutige Beschreibung der Zielsetzung für das Informationssicherheits-Managementsystem (ISMS) und des europäischen Datenschutz-Grundverordnung (DSGVO) Einführungsprojektes, der benötigten Dokumente, der Fristen und der Rollen und Verantwortlichkeiten im Projekt.

Dieser Projektplan wird für alle Aktivitäten im Rahmen des ISMS/EU DSGVO Einrichtungsprojektes angewendet.

Anwender dieses Dokumentes sind Mitglieder des [Unternehmensleitung] und Mitglieder des Projekt-Teams.

# Referenzdokumente

* ISO/IEC 27001 Norm
* EU DSGVO 2016/679 (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EC)
* [Beschluss oder ähnliches Dokument in dem der Projektstart angeordnet wird]
* [Methodik für Projekt-Management]

# ISMS Einführungsprojekt

## Ziel des Projekts

Die Einführung des Informationssicherheits-Managementsystems gemäß der ISO 27001 Norm und die Einhaltung der EU DSGVO bis spätestens [Datum].

## Ergebnisse des Projekts

Um eine möglichst wirksame Projektplanung zu gewährleisten, sollte das Unternehmen den DSGVO-Bereitschaftsfragebogen verwenden, um zu bestimmen, welche Bereiche bezüglich der Einhaltung der DSGVO die meiste Arbeit erfordern.

Im Verlauf des ISMS/DSGVO Einrichtungs-Projektes werden folgende Dokumente (dies ist keine vollständige Liste aller Dokumente) erstellt:

* **Verfahren zur Lenkung von Dokumenten und Aufzeichnungen** – Regelwerk für die Erstellung, Genehmigung, Verteilung und Aktualisierung von Dokumenten und Aufzeichnungen
* **Verfahren zur Identifikation der Anforderungen** – Vorgehensweise für die Identifikation amtlicher, gesetzlicher, vertraglicher und anderer Verpflichtungen
* **Anwendungsbereich des Informationssicherheits-Managementsystems** – ein Dokument zur genauen Definition von Werten (Assets), Standorten, Technologien, etc. innerhalb des Anwendungsbereiches
* **Informationssicherheitspolitik** – ein zentrales Dokument für die Leitungs-Ebene zur Steuerung des Informationssicherheits-Managements
* **Politik des Schutzes personenbezogener Daten** diese Politik bezieht sich auf die Bestimmung der Grundprinzipien des Schutzes personenbezogener Daten, als auch auf den Nachweis, dass sich das Unternehmen diesen Prinzipien verpflichtet
* **Politik des Schutzes von Arbeitnehmerdaten –** diese Politik legt dar unter welchen Bedingungen das Unternehmen personenbezogene Daten seiner Arbeitnehmer bearbeitet;
* **Datenschutzerklärung –** eine Erklärung, die darlegt unter welchen Bedingungen ein Unternehmen die personenbezogenen Daten seiner Klienten/ Website-Besucher bearbeitet;
* **Verzeichnis der Datenschutzerklärungen** – ein Dokument, in dem Sie alle veröffentlichten Erklärungen aufführen müssen;
* **Politik der Datenspeicherung –** Politik, die den Zeitrahmen darlegt, in dem das Unternehmen personenbezogene Daten aufbewahren darf;
* **Arbeitsbeschreibung des Datenschutzbeauftragten –** ein Dokument, in dem die Verantwortlichkeiten des Datenschutzbeauftragten beschrieben sind;
* **Richtlinien für das Datenverzeichnis und für die Zuordnung von Verarbeitungstätigkeiten –** ein Dokument, welches erklärt, wie alle Datenverarbeitungstätigkeiten aufgeführt werden;
* **Verzeichnis von Verarbeitungstätigkeiten –** ein Dokument, das vom Unternehmen genutzt werden sollte, um die Übereinstimmung mit den Anforderungen von Artikel 30 der DSGVO nachzuweisen;
* **Einverständniserklärung betroffener Personen -**  ein Dokument, das vom Unternehmen genutzt wird, um das Einverständnis betroffener Personen zu erlangen personenbezogene Daten für einen bestimmten Zweck zu verarbeiten;
* **Widerrufung der Einverständniserklärung betroffener Personen –** ein Dokument, das von betroffenen Personen genutzt wird, um ihr Einverständnis zu widerrufen;
* **Elterliche Einverständniserklärung –** ein Dokument, das vom Unternehmen genutzt wird, um das Einverständnis von Eltern/Erziehungsberechtigten/Vertretern eines Minderjährigen zu erlangen, personenbezogene Daten für einen bestimmten Zweck zu verarbeiten;
* **Widerrufung der elterlichen Einverständniserklärung** – ein Dokument, das von Eltern/Erziehungsberechtigten/Vertretern eines Minderjährigen genutzt wird, um ihr Einverständnis zu widerrufen, personenbezogene Daten für einen bestimmten Zweck verarbeiten zu dürfen;
* **Prozedur des Auskunftsersuchens betroffener Personen –** ein Dokument, das einen Prozess erstellt anhand dem das Unternehmen auf Ersuchen betroffener Personen antwortet;
* **Methodik zur Risikoeinschätzung und Risikobehandlung** – Beschreibung der Methodik zum Umgang mit Informationsrisiken
* **Verzeichnis zur Risikoeinschätzung** – Ergebnis der Einschätzung von Werten, Bedrohungen und Schwachstellen
* **Verzeichnis zur Risikobehandlung** – Ein Verzeichnis in dem für jedes inakzeptable Risiko die entsprechenden Maßnahmen ausgewählt sind
* **Bericht Risikoeinschätzung und Risikobehandlung** – Dieses Dokument umfasst alle wichtigen Dokumente die während des Prozesses der Risikoeinschätzung und Risikobehandlung erstellt wurden
* **Methodik der Datenschutz-Folgenabschätzung** – ein Dokument, in dem beschrieben wird, wie die Notwendigkeit und Verhältnismäßigkeit einer bestimmten Verarbeitungstätigkeit abgeschätzt wird und in dem Maßnahmen bereitgestellt werden, die möglichen Risiken für die Rechte und Freiheiten betroffener Personen zu mindern;
* **Verzeichnis der DSFA –** ein Dokument, das vom Unternehmen genutzt wird, um den DSFA-Prozess zu dokumentieren. Es umfasst den Schwellenfragebogen und den Datenschutz- Folgenabschätzungsfragebogen
* **Erklärung zur Anwendbarkeit** – Ein Dokument das die Zielsetzung und Anwendbarkeit jeder Maßnahme nach Anhang A der ISO 27001 feststellt
* **Plan zur Risikobehandlung** – Umsetzungsdokument mit Beschreibung der umzusetzenden Maßnahmen, der Verantwortlichen für die Umsetzung, der Fristen und der Ressourcen
* **Bring Your Own Device (BYOD) Politik** – beschreibt die Regeln für Nutzung von Handys und anderer firmenfremder Geräte zu Geschäftszwecken;
* **Politik mobiler Geräte und Telearbeit** – beschreibt die Sicherheitsregeln für den Gebrauch von Laptops, Handys und anderer Geräte außerhalb des Firmengeländes;
* **IT Sicherheitspolitik** – beschreibt die Grundsicherheitsvorschriften für alle Arbeitnehmer;
* **Politik der Klassifizierung von Informationen** – definiert, wie Daten in Bezug zu Vertraulichkeit zu klassifizieren sind und wie Daten entsprechend geschützt werden;
* **Politik der Zugangskontrollen** – definiert auf welche Weise das Management Zugangsrechte bestimmten Nutzern des Informationssystems genehmigt;
* **Verschlüsselungspolitik** – definiert, wie kryptografische Kontrollen und Schlüssel zu benutzen sind, um die Vertraulichkeit und Integrität der Daten zu schützen;
* **Politik der Anonymisierung und Pseudonymisierung** – definiert wie diese Techniken angewendet werden, um die personenbezogene Datenverarbeitung zu schützen;
* **Politik des aufgeräumten Arbeitsplatzes** – definiert wie Informationen am Arbeitsplatz und auf Computerbildschirmen geschützt werden;
* **Sicherheitsprozeduren für die IT-Abteilung** – beschreibt Sicherheitsregeln, die in der IT-Infrastruktur befolgt werden müssen;
* **Prozedur für die grenzüberschreitende Datenübertragung –** ein Dokument, in dem die Bedingungen festgelegt sind, unter denen die grenzüberschreitende Datenübertragung ausgeführt werden darf;
* **Standardvertragsklauseln –** Modellklauseln, herausgegeben von der EU Kommission um angemessene Schutzmaßnahmen bereitzustellen hinsichtlich des Schutzes der Privatsphäre und der Grundrechte und Freiheiten des Einzelnen und der Ausübung der dazugehörigen Rechte;
* **Fragebogen über die Übereinstimmung des Auftragsverarbeiters mit DSGVO –** ein Fragebogen zur Bewertung der Übereinstimmung des Zulieferers mit der EU DSGVO;
* **Zuliefererdatenverarbeitungsvereinbarung –** ein Vertragsdokument, das die Grenzen und Bedingungen festlegt, unter denen der Zulieferer (Auftragsverarbeiter) personenbezogene Daten für das Unternehmen (Verantwortliche) verarbeiten darf;
* **Reaktion auf eine Datenschutzverletzung und Meldeverfahren –** ein Verfahren, das, im Falle einer Datenschutzverletzung, die Verpflichtungen des Unternehmens festlegt;
* **Verzeichnis der Datenschutzverletzungen** – internes Register der Datenschutzverletzungen des Unternehmens;
* **Meldungsformular der Datenschutzverletzung an die Aufsichtsbehörde** – Dokument, das im Falle einer Datenschutzverletzung genutzt wird;
* **Disaster-Recovery-Plan** – definiert, wie die Infrastruktur und Daten nach einem Störfall wiederherzustellen sind;
* **Verfahren für interne Audits** – beschreibt wie Auditoren ausgewählt werden, wie Audit Programme erstellt werden, wie Audits durchgeführt werden und wie Audit-Ergebnisse protokolliert werden
* **Verfahren zu Korrektur** – beschreibt das Verfahren zur Umsetzung von Korrektur- und Vorbeugungs-Maßnahmen
* **Protokoll zur Managementbewertung** – ein Formblatt für die Protokollierung des Management-Meetings zur Bewertung der Angemessenheit des ISMS

Weitere Dokumente die während der ISMS/EU DSGVO-Einrichtung erstellt werden müssen, werden im Plan zur Risikobehandlung spezifiziert.

## Fristen

Im Folgenden werden die Fristen für die Freigabe der einzelnen Dokumente im Verlauf der ISMS/EU DSGVO Einführung aufgeführt:

|  |  |
| --- | --- |
| ***Dokument*** | ***Fristen für Dokument-Freigabe*** |
| \* |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Abschließende Vorstellung der Projektergebnisse ist für den [Datum] geplant.

## Projekt-Organisation

### Projekt-Sponsor

Jedem Projekt ist ein „Sponsor“ zugeteilt, der nicht aktiv am Projekt teilnimmt. Der Projekt-Sponsor muss regelmäßig vom Projektmanager über den Projektstatus unterrichtet werden und greift ein, falls das Projekt unterbrochen wird.

[Name, Stellenbezeichnung] wurde zum Projekt-Sponsor ernannt.

### Projektmanager

Die Rolle des Projektmanagers umfasst folgende Aufgaben: Sicherstellung der für die Projekt-Umsetzung notwendigen Ressourcen, Koordination des Projekts, Information des Projekt-Sponsors über den Projektfortschritt, Durchführung von administrativen Aufgaben im Zusammenhang mit dem Projekt. Die Befugnisse des Projektmanagers sollten diesen in die Lage versetzen, die Projekt-Umsetzung ohne Unterbrechungen innerhalb der gesetzten Fristen sicherzustellen.

[Name, Stellenbezeichnung] wurde zum Projektmanager ernannt.

### Projektteam

Die Rolle des Projektteams umfasst folgende Aufgaben: Unterstützung bei verschiedensten Aspekten der Projekt-Umsetzung, Durchführung der im Projekt spezifizierten Aufgaben, sowie Entscheidungen zu verschiedenen Aspekten welche einen fachübergreifenden Ansatz erfordern. Das Projektteam kommt immer zusammen bevor die endgültige Version eines Dokumentes aus Abschnitt 2 dieses Projektplans erstellt wird. Außerdem in allen anderen Fällen für die es der Projektmanager als notwendig erachtet.

*Verzeichnis der Projekt-Teilnehmer*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Name* | *Organisationseinheit* | *Stellenbezeichnung* | *Telefon* | *E-Mail* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Hauptrisiken im Projekt

Folgendes sind die Hauptrisiken bei der Umsetzung des Projekts:

1. Überschreitung der Fristen in der Risikoeinschätzungs-Phase
2. Überschreitung der Fristen bei der Ausarbeitung der Pläne für Geschäftskontinuität
3. Durchführung von Aktivitäten, die unnötige Kosten und Zeitaufwände nach sich ziehen
4. Auswahl zu vieler und/oder zu kostspieliger Maßnahmen

Folgendes sind die Maßnahmen zur Reduzierung der oben genannten Risiken:

* Vom Projektmanager wird überwacht, dass alle Projekt-Aktivitäten zu den festgesetzten Fristen umgesetzt werden und er fordert vom Projekt-Sponsor zeitnah dessen Eingreifen an
* Es wird ein Berater engagiert um sicherzustellen, dass Zeiten und Ressourcen nicht auf für das Projekt unwichtige Aktivitäten verwendet werden und dass einzelne Aktivitäten nicht in die falsche Richtung gehen
* Es wird ein Berater engagiert der die effektivsten Maßnahmen empfehlen soll

## Werkzeuge für Projekt-Umsetzung, Berichtswesen

Auf dem lokalen Netzwerk wird ein gemeinsamer Ordner eingerichtet, der alle Dokumente enthält, die während des Projektes erstellt werden. Alle Mitglieder des Projektteams bekommen Zugang zu diesen Dokumenten. Nur der Projektmanager [und Mitglieder des Projektteams] werden die Berechtigungen dafür erhalten, Änderungen durchzuführen oder Dateien zu löschen.

Der Projektmanager wird einen monatlichen Projektumsetzungsbericht erstellen und ihn an den Projekt-Sponsor weiterleiten.

# Verwaltung von Aufzeichnungen zu diesem Dokument

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name der Aufzeichnung | Aufbewahrungs-Ort | Verantwortlicher für Aufbewahrung | Maßnahme zum Schutz der Aufzeichnung | Aufbewahrungs-Dauer |
| Projektumsetzungs-Bericht (in elektronischer Form) | Gemeinsamer Ordner für Projekt-bezogene Aktivitäten | Projektmanager | Nur der Projektmanager hat die Berechtigung, Daten zu bearbeiten | Der Bericht wird für die Dauer von 3 Jahren aufbewahrt |

# Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

Der Inhaber des Dokumentes ist [Stellenbezeichnung].

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

* Ob alle am Projekt beteiligten Mitarbeiter ihre Aktivitäten nach den Vorgaben dieses Dokumentes durchführen
* Ob alle Projekt-Fristen eingehalten werden

[Stellenbezeichnung]

[Name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Unterschrift]