[Logo der Organisation]

[Name der Organisation]

**PROJEKTPLAN**  
**für die Einhaltung der europäischen Datenschutz-Grundverordnung**

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

**Änderungsprotokoll**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Erstellt von** | **Beschreibung der Änderung** |
| TT.MM.JJJJ | 0.1 | EUGDPRAcademy | Gliederung des Grunddokumentes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Nutzer 3](#_Toc500419972)

[2. Referenzdokumente 3](#_Toc500419973)

[3. EU DSGVO Umsetzungsprojekt 3](#_Toc500419974)

[3.1. Projektziel 3](#_Toc500419975)

[3.2. Projektergebnisse 3](#_Toc500419976)

[3.3. Fristen 5](#_Toc500419977)

[3.4. Projektorganisation 5](#_Toc500419978)

[3.4.1. Projektsponsor 5](#_Toc500419979)

[3.4.2. Projektmanager 6](#_Toc500419980)

[3.4.3. Projektteam 6](#_Toc500419981)

[3.5. Wesentliche Projektrisiken 6](#_Toc500419982)

[3.6. Tools für die Projektumsetzung, Berichterstattung 6](#_Toc500419983)

[4. Aufzeichnungen, die gemäß diesem Dokument aufzubewahren sind, managen 7](#_Toc500419984)

[5. Gültigkeit und Dokumentenmanagement 7](#_Toc500419985)

# Zweck, Anwendungsbereich und Nutzer

Der Zweck des Projektplans ist es, das Ziel des Umsetzungsprojektes der Europäischen Datenschutz- Grundverordnung (EU DSGVO) klar zu definieren, festzulegen, welche Dokumente geschrieben werden müssen und Fristen, Rollen und Verantwortlichkeiten im Projekt zu definieren.

Der Projektplan bezieht sich auf alle Tätigkeiten, die im EU DSGVO Umsetzungsprojekt durchgeführt werden.

Nutzer dieses Dokumentes sind Mitglieder des [Top-Managements] und Mitglieder des Projektteams.

# Referenzdokumente

* 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/EG)
* [relevantes nationales Gesetz oder Verordnung bezüglich der DSGVO Umsetzung]
* [andere örtlichen Gesetze und Vorschriften]

# EU DSGVO Umsetzungsprojekt

## Projektziel

Das Projektziel ist die Umsetzung des EU DSGVO Managementsystems im Einklang mit der Datenschutz-Grundverordnung (EU DSGVO 2016/679) des Europäischen Parlaments und des Rates spätestens bis zum [Datum].

## Projektergebnisse

Um die wirksamste Projektplanung sicherzustellen, sollte das Unternehmen den DSGVO Bereitschaftsfragebogen nutzen, um festzustellen, welche Bereiche der DSGVO Übereinstimmung am meisten bearbeitet werden müssen.

Während des EU DSGVO Umsetzungsprojektes werden folgende Dokumente (von denen einige Anhänge beinhalten, die hier nicht ausdrücklich erwähnt werden) geschrieben:

* **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 personenbezogener Daten von Arbeitnehmern –** 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 ist;
* **Richtlinien für das Datenverzeichnis und 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;
* **Verfahren des Zugangsersuchens betroffener Personen –** ein Dokument, das einen Prozess erstellt anhand dem das Unternehmen auf Ersuchen betroffener Personen antwortet;
* **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;
* **Verfahren der grenzüberschreitenden personenbezogenen 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;
* **DSGVO Einhaltungsfragebogen für den Auftragsverarbeiter –** ein Fragebogen zur Bewertung der Übereinstimmung des Zulieferers mit EU DSGVO;
* **Vereinbarung über die Datenverarbeitung mit Lieferanten** **–** ein Vertragsdokument, das die Grenzen und Bedingungen festlegt, unter denen der Zulieferer (Auftragsverarbeiter) personenbezogene Daten für das Unternehmen (Verantwortliche) verarbeiten darf;
* **IT Sicherheitspolitik** – beschreibt die Grundsicherheitsvorschriften für alle Arbeitnehmer;
* **Zugangssteuerungsrichtlinie** – definiert auf welche Weise das Management Zugangsrechte bestimmten Nutzern des Informationssystems genehmigt;
* **Sicherheitsverfahren für die IT-Abteilung** – beschreibt Sicherheitsregeln, die in der IT-Infrastruktur befolgt werden müssen;
* **Bring Your Own Device (BYOD) Richtlinie** – beschreibt die Regeln für Nutzung von Handys und anderer firmenfremder Geräte zu Geschäftszwecken;
* **Richtlinie zu Mobilgeräten und Telearbeit** – beschreibt die Sicherheitsregeln für den Gebrauch von Laptops, Handys und anderer Geräte außerhalb des Firmengeländes;
* **Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm** – definiert wie Informationen am Arbeitsplatz und auf Computerbildschirmen geschützt werden;
* **Richtlinie zur Klassifizierung von Informationen** – definiert, wie Daten in Bezug zu Vertraulichkeit zu klassifizieren sind und wie Daten entsprechend geschützt werden;
* **Richtlinie der Anonymisierung und Pseudonymisierung** – definiert wie diese Techniken angewendet werden, um die personenbezogene Datenverarbeitung zu schützen;
* **Richtlinie des Einsatzes von Verschlüsselung** – definiert, wie kryptografische Kontrollen und Schlüssel zu benutzen sind, um die Vertraulichkeit und Integrität der Daten zu schützen;
* **Notfallwiederherstellungsplan** – definiert, wie die Infrastruktur und Daten nach einem Störfall wiederherzustellen sind;
* **Verfahren für interne Audits** – definiert, wie die organisatorischen und technischen Sicherungsvorkehrungen in einem Unternehmen zu testen, zu beurteilen und zu evaluieren sind;
* **Anhang** **– ISO 27001 Interne Audit Checkliste** bietet eine Serie von Fragen, denen 114 Kontrollen, die in ISO 27001 Anhang A aufgeführt sind, zugrunde liegen;
* **Reaktion auf eine Datenschutzverletzung und Meldeverfahren –** ein Verfahren, das, im Falle einer Datenschutzverletzung, die Verpflichtungen des Unternehmens festlegt;
* **Verzeichnis der Datenschutzverletzung** – internes Register der Datenschutzverletzungen des Unternehmens;
* **Meldungsformular der Datenschutzverletzung an die Aufsichtsbehörde** – Dokument, das im Falle einer Datenschutzverletzung genutzt wird;
* **Meldungsformular der Datenschutzverletzung an betroffene Personen –** Dokument, das im Falle einer Datenschutzverletzung genutzt wird.

## Fristen

Fristen für die Annahme von Einzeldokumenten im Rahmen der EU DSGVO Umsetzung sind folgende:

|  |  |
| --- | --- |
| ***Dokument*** | ***Fristen für die Dokumentenannahme*** |
| \* |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Die abschließende Präsentation der Projektergebnisse ist für den [Datum] geplant.

## Projektorganisation

### Projektsponsor

Jedes Projekt hat einen ihm zugeordneten "Sponsor", der nicht aktiv am Projekt teilnimmt. Der Projektsponsor muss regelmäßig vom Projektmanager über den Projektstatus unterrichtet werden. Er greift ein, wenn das Projekt zum Halten kommt.

[Name, Arbeitsbezeichnung] wurde zum Projektsponsor ernannt.

### Projektmanager

Die Rolle des Projektmanagers ist es, die notwendigen Ressourcen für die Umsetzung des Projektes sicherzustellen, das Projekt zu koordinieren, den Sponsor über den Fortschritt zu informieren und die Verwaltungsarbeiten bezüglich des Projektes zu bewältigen. Die Autorität des Projektmanagers sollte die kontinuierliche Projektumsetzung innerhalb der gesetzten Fristen sicherstellen.

[Name, Arbeitsbezeichnung] wurde zum Projektmanager ernannt.

### Projektteam

Die Rolle des Projektteams ist es die verschiedenen Aspekte der Projektumsetzung zu unterstützen, die im Projekt festgelegten Aufgaben durchzuführen und unterschiedliche Entscheidungen zu treffen, die einen multidisziplinaren Ansatz verlangen. Das Projektteam trifft sich jedes Mal, bevor die Endversion eines Dokumentes aus dem Abschnitt 2 dieses Projektplans abgeschlossen ist und in anderen Fällen, wenn der Projektmanager dies für nötig hält.

*Tabelle aller Mitwirkender im Projekt*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Name* | *Organisatorische Abteilung* | *Arbeitsbezeichnung* | *Telefonnummer* | *E-Mail* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Wesentliche Projektrisiken

Wesentliche Risiken bei der Projektumsetzung sind die folgenden:

1. Fristenverlängerungen
2. Durchführung von Tätigkeiten, die unnötige Kosten und Zeitverschwendung nach sich ziehen
3. Mangel oder Fehlen von fachkundigen Mitarbeitern (z.B. DSB)

Maßnahmen zur Minderung oben angeführter Risiken:

* Der Projektmanager stellt sicher, dass alle Tätigkeiten innerhalb der festgesetzten Fristen durchgeführt werden und sorgt für ein rechtzeitiges Eingreifen des Projektsponsors.
* Einstellung eines Beraters, der sicherstellt, dass Zeit oder Ressourcen nicht an Tätigkeiten verschwendet werden, die für das Projekt nicht wichtig sind und dass Einzelaktivitäten nicht in die falsche Richtung gehen.
* Vertrag mit einem Datenschutzexperten abschließen, der die angemessensten Tätigkeiten vorschlägt.

## Tools für die Projektumsetzung, Berichterstattung

Ein Netzwerkordner, der alle während des Projektes erzeugten Dokumente umfasst, wird auf dem lokalen Netzwerk kreiert. Alle Mitglieder des Projektteams haben Zugriff auf diese Dokumente. Nur der Projektmanager [und Mitglieder des Projektteams]sind autorisiert, die Dateien zu verändern oder zu löschen.

Der Projektmanager bereitet einmal im Monat einen Bericht über die Projektumsetzung vor und sendet ihn dem Projektsponsor.

# Aufzeichnungen, die gemäß diesem Dokument aufzubewahren sind, managen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bezeichnung der Aufzeichnung | Speicherort | Für die Speicherung verantwortliche Person | Aufzeichnungsschutzkontrolle | Dauer der Speicherung |
| Projektumsetzungsbericht (in elektronischer Form) | Gemeinsamer Ordner für projektbezogene Tätigkeiten | Projektmanager | Nur der Projektmanager ist ermächtigt, die Daten zu bearbeiten. | Der Bericht wird für die Dauer von 3 Jahren gespeichert. |

# Gültigkeit und Dokumentenmanagement

Dieses Dokument ist gültig ab dem [Datum].

Der Eigentümer dieses Dokumentes ist [Stellenbezeichnung].

[Arbeitsbezeichnung]

[Name]

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

[Unterschrift]