[logo organisatie]

[naam organisatie]

**PROJECTPLAN**   
**voor Conformiteit met de Europese   
Algemene Verordening voor Gegevensbescherming**

|  |  |
| --- | --- |
| Code: |  |
| Versie: |  |
| Datum versie: |  |
| Gemaakt door: |  |
| Goedgekeurd door: |  |
| Classificatie: |  |

**Versieblad**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Versie** | **Gemaakt door** | **Omschrijving van de wijziging** |
| dd.mm.jjjj | 0.1 | EUGDPRAcademy | Concept basisdocument |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhoudsopgave**

[1. Doel, Toepassingsgebied en Gebruikers 3](#_Toc512499029)

[2. Gerefereerde Documenten 3](#_Toc512499030)

[3. EU AVG Implementatieproject 3](#_Toc512499031)

[3.1. Projectdoelstelling 3](#_Toc512499032)

[3.2. Projectresultaten 3](#_Toc512499033)

[3.3. Deadlines 5](#_Toc512499034)

[3.4. Projectorganisatie 5](#_Toc512499035)

[3.4.1. Projectsponsor 5](#_Toc512499036)

[3.4.2. Projectmanager 6](#_Toc512499037)

[3.4.3. Projectteam 6](#_Toc512499038)

[3.5. Voornaamste projectrisico’s 6](#_Toc512499039)

[3.6. Tools voor Projectimplementatie, Rapportage 6](#_Toc512499040)

[4. Registratiebeheer op basis van dit document 7](#_Toc512499041)

[5. Geldigheid en documentbeheer 7](#_Toc512499042)

# Doel, Toepassingsgebied en Gebruikers

Het doel van het Projectplan is om heldere doelstellingen te definiëren bij het implementatieproject van de Europese Algemene Verordening Gegevensbescherming (EU AVG), de te schrijven documenten, deadlines enrollen en verantwoordelijkheden in het project.

Het Projectplan van toepassing op alle activiteiten welke worden uitgevoerd in het EU AVG implementatieproject.

Gebruikers van dit document zijn leden van het [hoogste management] en leden van het projectteam.

# Gerefereerde Documenten

* EU AVG 2016/679 (Verordening (EU) 2016/679 van het Europese Parlement en van de Raad van 27 april 2016 over de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EC)
* [relevante nationale wet- of regelgeving voor AVG- implementatie]
* [andere lokale wetten en regelgeving]

# EU AVG Implementatieproject

## Projectdoelstelling

De projectdoelstelling is om het EU AVG Managementsysteem te implementeren welke uiterlijk per [datum] in overeenstemming is met de Algemene Verordening Gegevensbescherming (EU AVG 2016/679) van het Europese Parlement en van de Raad.

## Projectresultaten

Teneinde de meest efficiënte projectplanning te waarborgen, dient de organisatie de AVG Vragenlijst Beoordeling Niveau Voorbereiding te gebruiken om te bepalen op welke gebieden van de AVG compliance het meeste werk moet worden verricht.

Gedurende het EU AVG implementatieproject, zullen de volgende documenten (enkele van welke bijlagen bevatten die hier niet uitdrukkelijk zijn vermeld) worden opgesteld:

* **Beleid voor Bescherming Persoonsgegevens** – een beleid bedoeld om algemene gegevensbeveiligingsgrondbeginselen te vestigen, als ook de toewijding van de organisatie aan deze grondbeginselen aan te tonen;
* **Beleid voor Bescherming Persoonsgegevens werknemer –** eenbeleid om de voorwaarden uiteen te zetten onder welke de organisatie de persoonsgegevens van haar werknemers verwerkt;
* **Geheimhoudingsverklaring –** een verklaring om de voorwaarden uiteen te zetten onder welke de organisatie de persoonsgegevens van haar klanten/websitebezoekers verwerkt;
* **Register van Geheimhoudingsverklaringen** – een document waarin de gepubliceerde verklaringen dienen te worden vermeld;
* **Beleid voor Gegevenswissing –** een beleid om een periode uiteen te zetten waarin persoonsgegevens mogen worden bewaard door de organisatie;
* **Functieomschrijving Functionaris voor Gegevensbescherming –** een document dat de verantwoordelijkheden van een functionaris voor gegevensbescherming beschrijft;
* **Richtlijnen voor Gegevensinventarisatie en het In Kaart Brengen van Verwerkingsactiviteiten –** een document welke uitlegt hoe alle gegevensverwerkingsactiviteiten te vermelden;
* **Register van Verwerkingsactiviteiten –** een document bedoeld om te worden gebruikt door de organisatie om compliance aan te tonen aan de vereisten van art. 30 van de EU AVG;
* **Formulier Toestemming Betrokkene -**  een document gebruikt door de organisatie om toestemming te verkrijgen van de betrokkenen voor een specifiek doel;
* **Formulier Intrekking Toestemming Betrokkene -** een document gebruikt door de betrokkenen om hun toestemming in te trekken;
* **Formulier Ouderlijke Toestemming -** een document gebruikt door de organisatie om toestemming te verkrijgen van de ouder/voogd/vertegenwoordiger van een minderjarige om persoonsgegevens voor een specifiek doel te verwerken;
* **Formulier Intrekking Ouderlijke Toestemming** - een document gebruikt door de ouder/voogd/vertegenwoordiger van een minderjarige om de toestemming voor het verwerken van persoonsgegevens voor een specifiek doel in te trekken;
* **Procedure Verzoek Toegang Betrokkene –** een document om het proces uiteen te zetten waarin de organisatie antwoord op het verzoek van de betrokkene;
* **Methodologie voor Gegevensbeschermingseffectbeoordeling (DPIA)** – een document dat beschrijft hoe de noodzaak en de verhouding van een bepaalde procesactiviteit te beoordelen en de maatregelen te leveren om het potentiële risico ten aanzien van de rechten en vrijheden van de betrokkenen te mitigeren;
* **DPIA Register –** een document gebruikt door de organisatie om het DPIA-proces te documenteren. Het omvat de Drempelvragenlijst en de DPIA-vragenlijst;
* **Procedure voor Grensoverschrijdende Verwerking van Persoonsgegevens –** een document voor het vaststellen van voorwaarden onder welke grensoverschrijdende gegevensverwerking kan worden uitgevoerd;
* **Standaard Contractuele Clausules –** modelclausules uitgegeven door de EU Commissie om toereikende waarborgen te leveren ten aanzien van de bescherming van de privacy en fundamentele rechten en vrijheden van natuurlijke personen en betreffende de uitoefening van de corresponderende rechten.
* **Vragenlijst Verwerker AVG –** een vragenlijst bedoeld om de compliance van de leverancier aan de EU AVG te beoordelen;
* **Overeenkomst Gegevensverwerking Leverancier –** een contractueel document bedoeld om de beperkingen en voorwaarden vast te stellen onder welke een leverancier (verwerker) persoonsgegevens kan verwerken ten behoeve van de organisatie (verwerkingsverantwoordelijke);
* **IT-beveiligingsbeleid** – beschrijft de basis beveiligingsregels voor alle werknemers;
* **Toegangscontrolebeleid** – definieert hoe het management de toegangsrechten aan specifieke gebruikers en informatiesystemen goedkeurt;
* **Beveiligingsprocedures voor de IT-afdeling** – omschrijft de beveiligingsregels die b worden gebruikt voor de IT infrastructuur;
* **Beleid voor Bring Your Own Device (BYOD)** – beschrijft de regels voor het gebruik van mobiele en andere niet bedrijfsapparaten voor zakelijke doeleinden;
* **Beleid voor Draagbare Apparaten en Telewerken** – beschrijft de beveiligingsregels voor het gebruiken van laptops, mobiele telefoons en andere apparaten buiten de organisatie terrein;
* **Clear Desk en Clear Screen Beleid** – definieert hoe informatie te beschermen dat zich bevindt op de werkplek en op beeldschermen;
* **Beleid Informatieclassificatie** – definieert hoe gegevens vertrouwelijk te classificeren conform het beschermingsniveau;
* **Beleid voor Anonimisatie en Pseudonimisatie** – definieert hoe deze technieken te gebruiken teneinde de verwerking van persoonsgegevens te beschermen;
* **Beleid voor Gebruik Encryptie** – definieert hoe cryptografische maatregelen en sleutels te gebruiken om de vertrouwelijkheid en integriteit van de gegevens te beschermen;
* **Bedrijfscontinuïteitsplan** – definieert hoe de infrastructuur en gegevens moeten worden hersteld na een incident;
* **Procedure Interne Audit** – definieert hoe de organisatorische en technische waarborgen in een organisatie te testen, te beoordelen en te evalueren;
* **Bijlage** **– ISO 27001 Checklist Interne Audit** levert een reeks van vragen gebaseerd op 114 beheersmaatregelen die zijn opgesomd in de ISO 27001 Bijlage A;
* **Procedure Reactie en Notificatie Inbreuk Persoonsgegevens –** een procedure die de verplichtingen van de organisatie vaststelt in geval van een inbreuk op persoonsgegevens;
* **Register Inbreuk Persoonsgegevens –** InternBedrijfsregister van inbreuken op persoonsgegevens;
* **Formulier Notificatie Inbreuk Persoonsgegevens naar Toezichthoudende Instantie** – het document om te worden gebruikt in geval van een inbreuk op gegevens
* **Formulier Notificatie Inbreuk Persoonsgegevens naar Betrokkenen** – het document om te worden gebruikt in geval van een inbreuk op gegevens

## Deadlines

Deadlines voor acceptatie van individuele documenten in de loop van de EU GDPR implementatie zijn als volgt:

|  |  |
| --- | --- |
| ***Document*** | ***Deadlines voor acceptatie document*** |
| \* |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Eindpresentatie van projectresultaten wordt gepland voor [datum].

## Projectorganisatie

### Projectsponsor

Elk project heeft een toegewezen "sponsor" die niet actief deelneemt in het project. De projectsponsor moet regelmatig geïnformeerd worden door de projectmanager over de projectstatus en interveniëren als het project stokt.

[Naam, functie] is de aangestelde projectsponsor.

### Projectmanager

De rol van de projectmanager is om de noodzakelijke middelen voor de projectimplementatie zeker te stellen, het project te coördineren, de sponsor te informeren over de voortgang en om het administratieve werk, verbonden aan het project, te verzorgen. De bevoegdheid van de projectmanager dient van dien aard te zijn dat een ononderbroken projectimplementatie binnen de gestelde deadlines verzekerd wordt.

[Naam, functie] is de aangestelde projectmanager.

### Projectteam

De rol van het projectteam is om bij verscheidene aspecten van de projectimplementatie ondersteuning te bieden , om taken zoals gespecificeerd uit te voeren in het project en om te beslissen over verschillende issues die een multidisciplinaire benadering vereisen. Het projectteam ontmoet elkaar elke keer voordat een definitieve versie van een document van hoofdstuk 2 van dit Projectplan is afgerond en in alle andere gevallen wanneer de projectmanager dit nodig acht.

*Tabel van deelnemers aan het project*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Naam* | *Organisatieonderdeel* | *Functie* | *Telefoon* | *E-mail* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Voornaamste projectrisico’s

De voornaamste risico’s in de implementatie zijn als volgt:

1. Verlenging van deadlines
2. Uitvoeren van activiteiten die onnodige kosten opleveren en tijd verspillen
3. Tekort of gebrek aan bekwame werknemers (bijv. een FG)

Maatregelen die de bovengenoemde risico’s mitigeren zijn als volgt:

* De projectmanager verzekert dat alle activiteiten in het project binnen de gedefinieerde deadlines worden uitgevoerd en vraagt om tijdige interventie door de projectsponsor
* Inhuren van een consultant om te waarborgen dat tijd en middelen niet worden uitgegeven aan activiteiten die niet belangrijk zijn voor het project en dat individuele activiteiten niet de verkeerde richting opgaan
* Het in de arm nemen van een gegevensbeschermingsexpert om de meest geschikte activiteiten voor te stellen

## Tools voor Projectimplementatie, Rapportage

Een gezamenlijke map inclusief alle tijdens het project geproduceerde documenten zal worden aangemaakt op het lokale netwerk. Alle leden van het projectteam zullen toegang hebben tot deze documenten. Alleen de projectmanager [en leden van het projectteam] worden geautoriseerd om wijzigingen te doen en bestanden te verwijderen.

De projectmanager zal op maandelijkse basis een projectimplementatierapport opstellen en het doorsturen naar de projectsponsor.

# Registratiebeheer op basis van dit document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Naam registratie | Locatie opslag | Persoon verantwoordelijk voor de opslag | Beheer voor beschermingsregistratie | Bewaartermijn |
| Project- implementatie rapport (in elektronische vorm) | Gedeelde map voor project-gerelateerde activiteiten | Projectmanager | Alleen de project- manager is bevoegd om de gegevens te bewerken | Het rapport is bewaard voor een periode van 3 jaar |

# Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

Eigenaar van dit document is [functie].

[functie]

[naam]

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

[handtekening]