Projecttitel

Versie 0.1 – jan 2021

|  |  |  |
| --- | --- | --- |
| Projectnaam Projectplan | | Datum opgesteld: |
| Naam opdrachtgever | x | Voor akkoord:  Datum: |
| Naam projectmanager | xxx | |

Inhoudsopgave

[Inleiding 3](#_Toc96075690)

[Vraagstelling en achtergrond 3](#_Toc96075691)

[Op te leveren resultaat/resultaten 3](#_Toc96075692)

[Afbakening 3](#_Toc96075693)

[Randvoorwaarden 3](#_Toc96075694)

[Risicoanalyse 4](#_Toc96075695)

[Fasering en planning van tussenresultaten 4](#_Toc96075696)

[Kwaliteit 4](#_Toc96075697)

[Organisatie 4](#_Toc96075698)

[Privacy 5](#_Toc96075699)

[Security 5](#_Toc96075700)

[Appendix 1: tenderprocedure 6](#_Toc96075701)

## Inleiding

Dit projectplan is opgesteld voor …

Aanleiding project: Hoe is men bij het idee gekomen?

## Vraagstelling en achtergrond

Doelstellingen

Welke systemen worden aangepast of gerealiseerd?

Betrokken afdelingen

Betrokken leveranciers

## Op te leveren resultaat/resultaten

Software

Websites

Fysieke producten

Nieuwe diensten

Besparingen

## Afbakening

Wat is er wel in scope van het project?

Wat is er expliciet niet in scope van het project?

## Randvoorwaarden

Afhankelijkheden andere projecten

Benodigde middelen

Benodigde capaciteit van organisatie

Eventuele externe afhankelijkheden

## Risicoanalyse

Wat zijn de grootste risico’s van het project, inclusief kant en impact? Denk hierbij aan datalekken, integriteit gegevens,

Welke mitigerende maatregelen worden er genomen?

## Fasering en planning van tussenresultaten

[planning invoegen of verwijzing naar planning]

Is er een maandelijks of wekelijks projectoverleg?

Wordt er gewerkt in sprints?

## Kwaliteit

Kwaliteitsbewaking binnen het project:

Is er een demo na elke sprint?

Is er een definition of done?

Acceptatieproces: Wanneer wordt getest? Door wie?

## Organisatie

|  |  |  |  |
| --- | --- | --- | --- |
| Wie | Functie | Verantwoordelijkheid | Bevoegdheid |
| A | Opdrachtgever | Communicatie met projectmanager, akkoord op resultaten | Afkeuren van resultaten, wijzigen van plannen |
| B | Projectmanager (en teamlid) | Fasen managen en planning bijsturen | Capaciteit verschuiven |
| C | Product Owner (en teamlid) | Inhoudelijke beslissingen en kwaliteit producten |  |
| . | Teamlid |  |  |
| . | Teamlid |  |  |
| . | Teamlid |  |  |
| . | Gebruiker 1(teamleider) |  |  |
| . | Gebruiker 2 |  |  |
| . | Gebruiker 3 |  |  |
| . | Stakeholder |  |  |
| . | Stakeholder |  |  |
| . | Security officer |  |  |
|  | Data protection officer |  |  |

## Privacy

Heeft dit project een impact op privacy, bijvoorbeeld doordat er nieuwe persoonsgegevens worden verzameld of bestaande persoonsgegevens anders worden gebruikt?

Welke maatregelen worden er gedaan om privacy te waarborgen? Denk aan:

* Minimaal data verzamelen
* Transparantie
* Niet langer opslaan dan nodig is
* Aggregatie van data in rapportages
* Gebruikers zelf controle geven over hun data

Is er een inschatting gedaan door de Data Protection Officer or er een Data Protection Impact Assessment moet worden gedaan? Zie <https://softwarezaken.nl/2018/03/avg-template-voor-dpia/> voor template DPIA.

Zo ja: Is deze afgerond? Wat is de uitkomst?

Hoe wordt er in de acceptatie aandacht besteed aan privacy?

Zijn er externe leveranciers betrokken bij dit project? Krijgen zij toegang tot persoonsgegevens? Zo ja: wordt er een nieuwe verwerkersovereenkomst gesloten?

## Security

Wat is het ontwerp van de applicatie?

Is er een gedetailleerd ontwerp dat de servers, communicatielijnen en eventuele poorten en protocollen weergeeft?

Is dit ontwerp gereviewt en goedgekeurd door stakeholders, bijvoorbeeld de Data Protection Officer?

Hoe zijn authenticatie en authorisatie geregeld?

Beschikt de applicatie over logging? Welke events worden er gelogd? Hoe zijn de logs raadpleegbaar?

Wordt er binnen test- en acceptatie getest op security?

Wordt er ook getest op specifieke security-eisen voor grote klanten zoals RvR en politie? Bij deze klanten mogen contactpersonen elkaar gegevens niet zien.

Zijn securityrisico’s in kaart gebracht en ingeschat?

Welke extra security-maatregelen worden er genomen?

## Appendix 1: tenderprocedure

Bij veel projecten zal het voorkomen dat er externe leveranciers worden ingeschakeld, zoals leveranciers van software. Hier zijn best practices voor die door de projectleider moeten worden toegepast:

1. Het opstellen van een een request for proposal (RfP) met hierin opgenomen eisen die gesteld zijn aan leverancier en oplossing.
2. Validatie van eisen met stakeholders
3. Het vragen van voorstellen aan leveranciers en vergelijken van de ingezonden voorstellen op basis van eisen en wensen. Hierbij worden kwaliteit en prijs meegenomen.
4. Het uitnodigen van minimaal de twee best scorende leveranciers om het voorstel toe te lichten en hun ook hun aanpak te laten uitleggen. Mogelijk verzoek om aanpassing voorstel op basis van inzichten uit discussie.
5. Definitieve keuze en contractering

In de eisen kan worden meegenomen:

* Eis aan minimale omvang van leverancier in het kader van business continuiteit en verandercapaciteit
* Het hebben van een ISO27001 of vergelijkbaar certificaat (als eis of wens afhankelijk van project)
* Software-systemen moeten voldoen aan OWASP-top 10
* Leverancier moet NDA en verwerkersovereenkomst willen tekenen
* Eis om persoonlijke data binnen EU te verwerken of passende waarborgen te bieden. Bij verwerking persoonsgegevens moet de leverancier kunnen voldoen aan AVG
* Afhankelijk van project: vragen om referentieklanten en voorbeeldprojecten

Bij leveranciers van standaardsoftware die geen RfP’s beantwoorden (denk aan Microsoft of andere pure software-leveranciers) worden er eisen/criteria opgesteld en meerdere alternatieven vergeleken en gescoord. De interview-stap is dan niet van toepassing, partijen worden op basis van beschikbaar gemaakte informatie beoordeeld.