



Bijlage SAP
Antwoord template
Security-, Archiving-, Privacy by Design
Uitnodiging tot Inschrijving
E-Publicatie

© UWV Uitvoeringsinstituut werknemersverzekeringen.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden vervaelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enig andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Inhoudsopgave

0	INVULINSTRUCTIE ANTWOORDTEMPLATE	3
0.1	INLEIDING.....	3
0.2	INVULINSTRUCTIE.....	3
1	LEESWIJZER	4
1.1	INSTRUCTIE.....	4
1.2	BEOORDELINGSASPECTEN	4
2	MANAGEMENTSAMENVATTING.....	5
2.1	INSTRUCTIE.....	5
2.2	BEOORDELING.....	5
3	SECURITY-, ARCHIVING-, PRIVACY BY DESIGN	6
3.1	INSTRUCTIE.....	6
3.2	TENMINSTE TE ADRESSEREN ONDERWERPEN.....	6
3.3	BEOORDELINGSASPECTEN SECURITY-, ARCHIVING-, PRIVACY BY DESIGN.....	6

0 Invulinstructie antwoordtemplate

Inschrijver dient alle instructies uit dit template te verwijderen en niet terug te laten komen in de uitgewerkte versie van uw beschrijving van de oplossing.

0.1 Inleiding

Voorliggend antwoordtemplate dient als format te worden gebruikt voor de uitwerking van het Gunningscriterium **Security-, Archiving-, Privacy by design** dat de Inschrijver in het kader van de Europese aanbesteding E-Publicatie van UWV dient in te dienen. UWV heeft gepoogd om duidelijk te beschrijven wat er in dit kader van Inschrijver verwacht wordt en wat Inschrijver op dat onderdeel in het antwoord template dient op te nemen. Het is aan Inschrijver om bij onduidelijkheden hier vragen over te stellen en vervolgens de minimaal te adresseren onderwerpen in het antwoordtemplate te beschrijven.

U dient de structuur c.q. hoofdstukindeling van het format te volgen. Daarbinnen heeft Inschrijver de vrijheid de aan te bieden oplossing voor dit Gunningscriterium naar eigen inzicht uit te werken. Aan Inschrijver wordt zo de ruimte geboden de eigenheid van zijn oplossing en de best practices een plek te geven.

In totaal kan **maximaal 210 punten** op het Gunningscriterium Security-, Archiving-, Privacy by design worden gescoord. De beoordeling vindt plaats op basis van de in deze template genoemde beoordelingsaspecten.

0.2 Invulinstructie

In deze antwoordtemplate beschrijft UWV wat hij uitgewerkt wil zien in dit antwoordtemplate en welke aspecten voor UWV relevant zijn bij de beoordeling van het Gunningscriterium Security-, Archiving-, Privacy by design.

Inschrijver dient met de uitwerking van zijn oplossing te voorzien in de gestelde eisen en, indien van toepassing, op welke wijze de wensen van UWV gerealiseerd worden.

De volgende uitgangspunten zijn van belang:

1. Uw beschrijving dient uit te gaan van de door UWV gestelde kaders in de aanbestedingsdocumenten en mag daarmee dus ook niet conflicteren.
2. Inschrijver dient de structuur van de hoofdstukken strikt te hanteren. Inschrijver is daarbij vrij om per hoofdstuk de paragraafindeling zelf te bepalen;
3. Inschrijver heeft de mogelijkheid om meer aspecten inzichtelijk te maken dan de aspecten die expliciet vermeld worden in dit antwoordtemplate, teneinde op die manier duidelijk te maken op welke wijze aan het Gunningscriterium invulling wordt gegeven;
4. Uw beschrijving van de oplossing inzake Security-, Archiving-, Privacy by design dient als een samenhangend, volledig en leesbaar geheel te zijn uitgewerkt, zodat UWV een goed beeld verkrijgt van uw oplossing.
5. De antwoord template dient als losse Bijlage bij de Inschrijving te worden opgenomen;
6. Uw beschrijving heeft exclusief hoofdstuk één (1) - leeswijzer en hoofdstuk twee (2) - management samenvatting, een omvang van maximaal **10 pagina's A4 (inclusief bijlagen)**. Inschrijver gebruikt voor de beantwoording een **minimale lettergrootte van 9pt Arial**.
7. Inschrijver dient alle instructies uit dit template te verwijderen en niet terug te laten komen in de uitgewerkte versie van uw beschrijving van de oplossing.

1 Leeswijzer

1.1 Instructie

Dit hoofdstuk bevat een leeswijzer waaruit de opzet en de structuur van de door u beschreven oplossing voor de E-Publicatie inzake Security-, Archiving-, Privacy by design duidelijk wordt. Voorts verzoekt UWV in de leeswijzer een tabel met verwijzingen op te nemen waaruit blijkt in welke paragraaf de borging van de relevante eisen en wensen uitgewerkt is.

1.2 Beoordelingsaspecten

De gevraagde leeswijzer wordt niet betrokken in de beoordeling van dit sub-Gunningscriterium en telt ook niet mee bij toepassing van de norm betreffende de maximale omvang van de beschrijving van uw oplossing voor dit Gunningscriterium.

2 Managementsamenvatting

2.1 Instructie

Dit hoofdstuk beschrijft in maximaal **één (1) A4 minimale lettergrootte van 9pt Arial** de essentie van uw oplossing inzake e-publicatie op directie- en managementniveau. De samenvatting geeft inzicht in de oplossing die door Inschrijver wordt voorgesteld. De Managementsamenvatting is hoofdstuk twee (2) van uw beschrijving.

2.2 Beoordeling

De gevraagde managementsamenvatting wordt niet betrokken in de beoordeling de aangeboden oplossing en telt ook niet mee bij toepassing van de norm betreffende de maximale omvang van de beschrijving van uw oplossing voor dit Gunningscriterium.

3 Security-, archiving-, Privacy by design

3.1 Instructie

In het hoofdstuk drie (3) geeft u een beschrijving van de door u voorgestelde oplossing voor **Security-, Archiving-, Privacy by design** en deze bestaat uit maximaal **10 pagina's A4** (inclusief bijlagen). Bij overschrijding van het maximaal aantal pagina's worden de meerdere pagina's niet beoordeeld. Inschrijver gebruikt voor de beantwoording een **minimale lettergrootte van 9pt Arial**.

3.2 Tenminste te adresseren onderwerpen

Bij de uitwerking van het Gunningscriterium **Security-, Archiving-, Privacy by design** dient Inschrijver tenminste de onderstaande onderwerpen te beschrijven. Het risico van slordigheden, onjuistheden en onvolledigheden in de beschrijving van de oplossing ligt volledig bij de Inschrijver. Indien één of meerdere van deze onderwerpen ontbreken in de beantwoording van Inschrijver, dan kan de beantwoording worden beoordeeld als onvoldoende en kan Inschrijver uitgesloten worden van verdere deelname aan de aanbesteding en kan hij niet meer in aanmerking komen voor gunning van de opdracht.

De tenminste in de beschrijving van uw oplossing te adresseren onderwerpen zijn: beveiliging, archivering en privacy, duurzame opslag en metadatering. Deze worden getoetst op de tabel onder paragraaf 3.3 opgenomen beoordelingsaspecten.

3.3 Beoordelingsaspecten Security-, Archiving-, Privacy by design

In Programma van Eisen heeft u aangegeven **dat** u zult voldoen aan de gestelde eisen. Om de verschillende aangeboden oplossingen te kunnen beoordelen willen wij echter ook een goed beeld krijgen **hoe** u daar op het onderdeel **Security-, Archiving-, Privacy by design** van de aangeboden applicatie invulling aan geeft. Toon dit tevens aan door middel van het bijsluiten van bewijsstukken als bijlage (dit is vormvrij maar kan bijvoorbeeld omvatten: certificaten, portfolioprojecten bij opdrachtgevers bij voorkeur vergelijkbaar met UWV, diploma's van de beoogde medewerkers en/of opleidingsprogramma's).

De mate waarin de door Inschrijver beschreven oplossing beter/vollediger invulling geeft aan onderstaande aspecten bepaald de hoogte van de score.

	Omschrijving	Maximaal te behalen punten per oordeel
SAP 1	U beschrijft hoe uw applicatie invulling geeft aan duurzame toegankelijkheid en beschrijft een duidelijke visie op duurzame toegankelijkheid bij de doorontwikkeling van de applicatie.	44
SAP 2	U beschrijft hoe uw applicatie standaard ondersteuning biedt aan het borgen van de security en privacy en u beschrijft een duidelijke visie op deze 2 aspecten bij de doorontwikkeling van de applicatie.	44

SAP 3	Alle toegangen tot de applicatie (registraties en raadplegingen) moeten op zodanig worden gelogd dat audit trails kunnen worden gegenereerd waarmee inzichtelijk wordt wie wanneer toegang heeft gehad tot welke gegevens. Dit zowel vanuit de casus gezien (welke medewerkers hebben wanneer een bepaalde object ingezien/bewerkt) als vanuit de medewerkers (welke object heeft een medewerker in een op te geven periode ingezien/bewerkt). Er vindt monitoring plaats op de logging en er is een incident response management proces ingericht.	33
SAP 4	U heeft maatregelen genomen met betrekking tot de preventie en opsporing van Beveiligingsincidenten. Het gebruik van de systemen en de toegang daartoe wordt vastgelegd op een manier die in overeenstemming is met het risico en zodanig dat oorzaak, veroorzaker en gevolg aantoonbaar zijn. De vastlegging is zodanig voorzien van maatregelen dat de vastlegging blijft bestaan en niet gewijzigd kan worden. De vastlegging dient bewaart te worden voor een termijn die in overeenstemming is met wettelijke eisen.	22
SAP 5	Ten behoeve van testen, opleiden en systeemmonitoring mogen alleen geanonimiseerde dan wel gepseudonimiseerde gegevens gebruikt worden.	22
SAP 6	U beschikt over een reguliere informatiebeveiligingsorganisatie waarin naast duidelijke participatie van het hoogste management, een beveiligingsfunctionaris is benoemd die verantwoordelijk is voor het opstellen, de implementatie, het onderhoud en de naleving van het beleid betreffende Informatiebeveiliging. Daar waar Opdrachtnemer geen reguliere beveiligingsfunctionaris heeft, vervult een daartoe aangewezen lid van de directie van Opdrachtnemer die functie.	11
SAP 7	Gegevens moeten op basis van vooraf gedefinieerde bewaartermijnen definitief kunnen worden verwijderd door een geautoriseerd persoon.	11
SAP 8	U beschikt over een actief beleid op het gebied van wijzigingen, patches etc. aan software en hardware en bent in staat hierover te allen tijde aan UWV te rapporteren. Hieronder valt ten minste het informeren over nieuwe marktontwikkelingen, het informeren over patches en bedreigingen en het informeren over de compatibiliteit en het uit support raken van de hardware en/of software stack voor zover door Opdrachtgever gebruikt.	11
SAP 9	U heeft actief beleid voor het screenen van personeel en onderaannemers om misbruik van informatie te voorkomen.	11
	Maximaal op dit subcriterium Security-, archiving-, privacy by Design te behalen	210