Privacycheck [vul in verwerking]

Onderwerp :

Betrokken :

Referenties : verwerking [vul in verwerkingsnummer (register)]
ticket [Vul in ticketnummerl]

Datum :

Samensteller :
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Stap 1 – Inventarisatie

*Gebruik eventueel de* [*AVG-canvas als praatplaat*](https://pec.surf.nl/asset/avg-canvas-voor-medewerkers/)*.*

|  |  |
| --- | --- |
| **Informatievraag** | **Antwoord** |
| Wat is de behoefte/doel? |  |
| Beschrijving wat is nodig voor dit doel? Processen/activiteiten |  |
| Welke gegevens zijn nodig? | [ ]  Categorie 1 – Publiek/openbaar[ ]  Categorie 2 – Intern[ ]  Categorie 3 – Vertrouwelijk[ ]  Categorie 4 – Strikt vertrouwelijk (geheim/bijzondere pg) |
| Over wie en om hoeveel personen gaat het? |  |
| Manier van verzamelen | Ongestructureerd, SaaS, webform, etc. licht toe:[ ]  ook smartphone-app? |
| Wie gaan de gegevens gebruiken |  |
| Wie is betrokken bij opslaan/verzamelen (plus de juridische verhouding)? |  |
| Bewaartermijn |  |
| Gaat het om een verwerking waar een verwijderverzoek moet worden gefaciliteerd? |  |
| Is het een pilot?  | [ ]  nee [ ]  ja 🡪 vermeld: eind-/evaluatiedatum: |
| Gaat het om schaduw-IT | [ ]  nee [ ]  ja 🡪 beschrijf de regels voor toegestaan gebruik: |
| Van belang voor OR of SR? | [ ]  nee [ ]  ja 🡪 OR of SR: |

Voorwaarden gebruik persoonsgegevens

|  |  |  |
| --- | --- | --- |
| **nr.** | **voorwaarde** | **toelichting** |
| 1 | Rechtmatige verwerkingsgrondslag - is de beoogde verwerking rechtmatig/legitiem volgens de AVG?  | Grondslag: [ ]  Proportionaliteit/doeltreffendheid\*[ ]  Subsidiariteit\* |
| 2 | Doelbinding – de gegevens worden alleen voor het verzameldoel gebruikt |   |
| 3 | Dataminimalisatie – er worden niet meer gegevens verzameld dan nodig voor het doel en als ze niet meer nodig zijn, worden ze verwijderd |   |
| 4 | Transparantie – de betrokkene kan nagaan waarvoor de gegevens worden gebruikt en wordt geïnformeerd over zijn rechten |   |
| 5 | Data-integriteit – de gegevens zijn juist en correct |   |
| 6 | Gegevensbescherming  | Zie stap 2 - privacycheck |

\* Zie bijlage, toelichting rechtmatigheid

Risicoklasse

Voor de deze verwerking is [een of geen] BIV-codering uitgevoerd. Er is [een of geen] DPIA vereist/er wordt volstaan met dit document als verantwoording van de verwerking.

Dataflow/gegevensset

[plak een tekening met dataflow]

*Bij smartphone-app: wat voor permissies en waarvoor en blijft de toegang in een eigen bubbel op de smartphone? Gebruik eventueel* [*Exodus Privacy*](https://reports.exodus-privacy.eu.org/en/)*.*

Stap 2 – Gegevensbescherming

Zijn de gegevens zijn op een adequate manier beschermd (technische en organisatorische maatregelen)? Controleer de applicatie en techniek via in de acht stappen van het Framework Privacy by Design.

Bevindingen

|  |  |  |
| --- | --- | --- |
| **Onderdeel PbD** | **Beschermd?** | **Toelichting** |
| Anonimiseren | Ja/nee/n.v.t. |   |
| Dataminimalisatie | Ja/nee/n.v.t. |   |
| Pseudonimiseren | Ja/nee/n.v.t. |   |
| Toegangsmanagement | Ja/nee/n.v.t. |   |
| Rechten gefaciliteerd | Ja/nee/n.v.t. |   |
| Veilige verwerking | Ja/nee/n.v.t. |   |
| Bewaren/vernietigen | Ja/nee/n.v.t. |  |
| Testen en beheren | Ja/nee/n.v.t. |   |

# Stap 3 – Maatregelen voor compliance

Verplichte beheersmaatregelen

Bijvoorbeeld: training, doelen bijstellen, opslaglocatie aanpassen, betrokkenen informeren, MFA, SSO, etc.

[plak eventueel de maatregelen die naar voren komen uit de AVG-impactvragen]

Concrete acties voor verdere verbetering (AVG)

[concretiseer en neem mee Privacy by Default]

# Stap 4 – Administratie op orde

[ ]  Controle op afsluiten VO/GUO/SCC/BCR/DTIA

[ ]  Verwerkingsregister bijwerken

[ ]  AVG-check afronden, beheer belegd

[ ]  Terugkoppeling aan aanvrager

[ ]  Opnemen in PDCA

# Toelichting rechtmatigheid (noodzakelijkheidstoets)

Proportionaliteit en doeltreffendheid

Bij verwerking op basis van een van de noodzakelijkheidsgrondslagen (dat zijn alle grondslagen behalve de grondslag 'toestemming'), geldt dat deze ook de noodzakelijkheidstoets moeten doorstaan. Daarvoor kijk je naar de proportionaliteit en doeltreffendheid:

[ ]  Behaal je met de verwerking van gegevens het gestelde doel of is dat niet zeker? Licht kort toe:

[ ]  Staat het legitieme doel in verhouding tot het feit dat hiervoor persoonsgegevens moeten worden verwerkt? Licht kort toe:

Subsidiariteit

[ ]  Is dit de beste manier om het te bereiken: kan het doel niet op een andere, minder ingrijpende wijze worden bereikt? Licht kort toe: