WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

Bestuurlijke rapportage Informatiebeveiliging en Privacy Werkzaak Rivierenland

Nulmeting 2023

Jos Baan (FG) en Robin Heffelaar (CISO), mei 2023

Inhoudsopgave

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

1. Inleiding

Het voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en de diverse normen is een uitdaging. Een belangrijk deel van de maatregelen dient nog geborgd te worden in de organisatie. Dat betekent in dit geval het toewijzen van taken, verantwoordelijkheden, bevoegdheden, bewustzijn creëren en dit vervolgens te kunnen aantonen.

De AVG en de BIO leggen de verantwoordelijkheid bij Werkzaak Rivierenland om aantoonbaar te maken dat wij voldoen aan de gestelde eisen. Op het gebied van gegevensbescherming zijn we aan het groeien. Er is al veel bereikt, maar er is ook nog veel winst te behalen. Met name het risico gebaseerd werken, werken vanuit de PDCA-methodiek, inzicht in huidige invulling van de AVG en BIO en bewustwording in alle lagen van de organisatie verdienen extra aandacht. Dit is onder andere vastgelegd in de “Strategie uitvoering gegevensbescherming: privacy & informatiebeveiliging 2022-2024”.

Om inzicht te krijgen in hoeverre Werkzaak voldoet aan de gestelde eisen is voorliggende nulmeting uitgevoerd met behulp van het vorig jaar aangeschafte en geïmplementeerde Information Security Management System (ISMS) Recourse. De meting is uitgevoerd door de medewerkers die op dit moment het meeste van de inhoud weten. In de toekomst wordt de eindverantwoordelijkheid van de normen overgedragen aan de proceseigenaren (teammanagers) waarbij de inhoudsdeskundigen rapporteren.

2. Samenvatting

BIO:

Op het gebied van informatiebeveiliging in het algemeen zijn we als Werkzaak op de belangrijkste onderdelen in control. Wij kunnen nog verbeteren op het gebied van borging en kwaliteit. Dit is terug te zien in de verbetermaatregelen die wij de komende jaren gaan aanpakken. De uitkomsten uit de nulmeting worden gebruikt om de basis te leggen voor de doorontwikkeling en verdere implementatie (PDCA) van informatiebeveiliging binnen Werkzaak. De focus ligt daarbij op het minimaliseren van de beveiligingsrisico's en niet op een 100% score.

AVG:

Op het gebied van privacy en gegevensbescherming kunnen en moeten wij nog slagen maken. De uitkomsten uit de nulmeting worden gebruikt om de basis te leggen voor de doorontwikkeling en verdere implementatie (PDCA) van privacy binnen Werkzaak. Ook hier moet de focus niet liggen op een 100% score maar op het minimaliseren van de privacyrisico's en het beschermen van de persoonlijke levenssfeer van onze cliënten en medewerkers.

3. Status informatiebeveiliging (BIO)

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

3a. Toelichting bouwstenen BIO

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van Werkzaak Rivierenland:

- Volgt het beleid van de informatiebeveiligingsdienst gemeenten (IBD)
- Zorgt ervoor dat de juiste activiteiten ten aanzien van informatiebeveiliging door de organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

1. BELEID EN ORGANISATIE
H5 / H6 / H18

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- De informatiebeveiligingsorganisatie is geregeld
- Waar, wanneer houden we ons aan onze afspraken en leven we de wet- en regelgeving na

Het bestuur en medewerkers zijn actief betrokken bij informatiebeveiliging. Er is een organisatiebreed beleid dat richting en sturing geeft. De organisatie is effectief ingericht, waarbij rollen, taken en bevoegdheden zijn ondergebracht. Verantwoording is structureel ingericht, zodat naleving is geborgd.

2. PERSONEEL EN TOEGANG
H7 / H9 / H11

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

Alleen de juiste personen hebben toegang tot de gebouwen, systemen en gegevens van Werkzaak. Er zijn passende organisatorische en technische maatregelen getroffen. Dit gaat om waarborgen rondom in- en externe medewerkers, toegang tot gebouwen en omgeving en toegang tot de (digitale) informatievoorziening.

3a. Toelichting bouwstenen BIO

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

3. CONTINUÏTEIT EN INCIDENTEN
H16 / H17

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten
- Wij komen onze afspraken met de burger en bedrijven na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

De diensten van Werkzaak Rivierenland worden geleverd volgens de afspraken die de organisatie daarover maakt met de burger en bedrijven. Ook bij incidenten worden de diensten geleverd volgens deze afspraken.

4. INFORMATIESYSTEMEN
H12 / H14 / H15

Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers
- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

Informatiesystemen zijn een keten van mensen, processen en middelen. Hierin zijn procedures en maatregelen beschikbaar ter bescherming van de omgeving. Het gaat hierbij om zowel de interne als de externe informatiesystemen (uitbesteding, leveranciers en Cloud-toepassingen).

5. DATABESCHERMING
H8 / H10 / H13

Veilige omgang met data in onze software
- Data wordt op de juiste manier beschermd
- De gegevens van de burgers en bedrijven worden veilig opgeslagen en gecommuniceerd. Binnen en buiten de organisatie.

3b. Status BIO bij Werkzaak Rivierenland

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

BESTUURLIJKE UITGANGSPUNTEN

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van Werkzaak Rivierenland:

- Volgt het beleid van de IBD
- Zorgt ervoor dat de juiste informatiebeveiliging door de organisatie wordt uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

Op het gebied van informatiebeveiliging in het algemeen is Werkzaak op de belangrijkste onderdelen in control. Er is echter nog veel winst te behalen op het gebied van borging en kwaliteit. Dit is terug te zien in de verbeteracties die de komende jaren moeten worden uitgevoerd. De uitkomsten uit de nulmeting worden gebruikt om de basis te leggen voor de doorontwikkeling en verdere implementatie (PDCA) van informatiebeveiliging binnen Werkzaak. De focus ligt daarbij op het minimaliseren van de beveiligingsrisico's en niet op een 100% score.

1. BELEID EN ORGANISATIE Actueel beleid en organisatie van informatiebeveiliging en controle op naleving	De verschillende beveiligingsrollen zijn vastgelegd en toegewezen. Er is vastgesteld welke wet- en regelgeving van toepassing is. Er is een systeem ingericht t.b.v. een PDCA-cyclus en het borgen van kwaliteit. Een overzicht wie, wanneer en in welke gevallen met (overheids)instanties contact heeft inclusief procedures ontbreekt nog. Hiernaast is er geen vastgesteld bedrijfscontinuïteitbeleid ingericht en is het huidige beleid (2020) niet up-to-date.
2. PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	Door gebruik te maken van de KPN-werkplek omgeving i.c.m. 2 factor authenticatie hebben we een zeer veilige basis. Veel eisen en normen worden (onbewust) deels toegepast en vastgelegd. Er zijn periodieke bewustwordingstrainingen, maar deze moeten nog verder geprofessionaliseerd worden. Wat ontbreekt en essentieel is voor de toegangsbeveiliging van Werkzaak is een functieautorisatiematrix.
3. CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten	V.w.b. het beheer van beveiligingsincidenten zijn diverse procedures (informeel) ingericht en verlopen op dit moment goed. De procedures zijn niet vastgelegd en het borgen en evalueren dient ook vastgelegd en ingericht te worden. Er is nog geen vastgesteld bedrijfscontinuïteitsbeleid, maar wel zijn er enkele informele afspraken m.b.t. bedrijfscontinuïteit.
4. INFORMATIESYSTEMEN Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers	De inrichting en beveiliging van het netwerk voldoet aan de gestelde eisen. De beheerprocedures zijn nog niet allemaal beschreven en vastgelegd. Tevens vindt er niet altijd een expliciete risicoafweging plaats v.w.b. het beheer. Met de meeste leveranciers zijn er service-overleggen waar de KPI's en SLA's besproken worden. Er is nog geen vastgestelde procedure aanwezig die gevolgd wordt bij de inkoop van software.
5. DATABESCHERMING Veilige omgang met data in onze software	De inrichting van het elektronisch berichtenverkeer voldoet aan de eisen zoals gesteld in de normenkaders. Het beheer van onze bedrijfsmiddelen is deels op orde. Procedures en een actuele registratie van bedrijfsmiddelen en processen met eigenaren en beheerders ontbreekt. Werkzaak Rivierenland beschikt nog niet over een cryptografiebeleid dat is afgestemd met de organisaties waarmee digitale communicatie plaatsvindt.

4. Status privacy (AVG)

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

4a. Bouwstenen AVG

Bestuurlijke principes en beleid, organisatie van privacy en naleving

Het bestuur van Werkzaak:

- Volgt het beleid van de Vereniging Nederlandse Gemeenten (VNG) en de informatiebeveiligingsdienst gemeenten (IBD)

- Zorgt ervoor dat de juiste activiteiten ten aanzien van privacy door de organisatie worden uitgevoerd

- Controleert de juiste werking van de privacy in de organisatie

1. BELEID

Actueel beleid en organisatie van privacy en controle op naleving

- Bestuur, directie en management laten zien dat privacy belangrijk is
- De informatiebeveiliging en privacy organisatie is geregeld
- Waar, wanneer houden we ons aan onze afspraken en leven we de wet- en regelgeving na

Het bestuur en medewerkers zijn actief betrokken bij privacy. Er is een organisatiebreed beleid dat richting en sturing geeft. De organisatie is effectief ingericht, waarbij rollen, taken en bevoegdheden zijn ondergebracht. Verantwoording is structureel ingericht, zodat naleving is geborgd.

2. PROCESSEN

Verwerkingen van persoonsgegevens dienen te voldoen aan de AVG

- Toetsing en inrichting van de werkprocessen conform privacy basisbeginselen:
    - Behoorlijkheid;
    - Transparantie;
    - Doelbinding;
    - Dataminimalisatie;
    - Opslagbeperking;
    - Juistheid;
    - Integriteit;
    - Vertrouwelijkheid.

4a. Bouwstenen AVG

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

3. ORGANISATORISCHE INBEDDING

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy en informatiebeveiliging.

Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden, bevoegdheden en het creëren van bewustzijn.

4. RECHTEN VAN BETROKKENEN

Werkzaak dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen.

Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

5. SAMENWERKEN

Werkzaak Rivierenland werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties.

In veelvoorkomende gevallen zal er **sprake** zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. Werkzaak Rivierenland dient dan ook afspraken te maken met deze andere partijen.

4a. Bouwstenen AVG

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

6. BEVEILIGING

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat Werkzaak Rivierenland passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens.

Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

7. NALEVING

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels.

Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat het bestuur aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

4b. Status AVG

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland

BESTUURLIJKE UITGANGSPUNTEN

Bestuurlijke principes en beleid, organisatie van privacy en naleving

Het bestuur van Werkzaak:

- Volgt het beleid van de VNG/IBD
- Zorgt ervoor dat privacy op de juiste manier door de organisatie wordt toegepast en uitgevoerd
- Controleert de juiste werking van privacy in de organisatie

Op het gebied van privacy en gegevensbescherming is in het algemeen nog veel winst te behalen. De uitkomsten uit de nulmeting worden gebruikt om de basis te leggen voor de doorontwikkeling en verdere implementatie (PDCA) van privacy binnen Werkzaak. De focus moet daarbij niet liggen op een 100% score maar op het minimaliseren van de privacyrisico's en het beschermen van de persoonlijke levenssfeer van onze cliënten en medewerkers.

1. BELEID Actueel beleid en organisatie van privacy	Het beleid is opgesteld en vastgesteld door directie en bestuur. De verantwoordelijkheden en taken zijn op hoofdlijnen beschreven en vastgelegd. Het afgelopen jaar is een ISMS systeem ingericht t.b.v. een PDCA-cyclus en het borgen van de privacy (beheers)maatregelen in de organisatie. Het beleid en de organisatie van privacy zijn echter nog niet voldoende geborgd in de organisatie.
2. PROCESSEN Verwerkingen van persoonsgegevens dienen te voldoen aan de AVG	De hoog risicoverwerkingen zijn op dit moment niet inzichtelijk en privacy/risicogebaseerd werken is niet geborgd in de organisatie. De focus zal daarbij liggen op het integraal uitvoeren van privacy bij procesoptimalisaties, procesbeschrijvingen en het combineren van het processenoverzicht met een verwerkingsregister. Op basis van inzicht in hoog risicoverwerkingen zullen er jaarlijks DPIA's uitgevoerd moeten worden op deze processen.
3. ORGANISATORISCHE INBEDDING Het toewijzen van taken, verantwoordelijkheden, bevoegdheden en het creëren van bewustzijn.	In de praktijk voert de aangestelde FG gezien de volwassenheid van de organisatie vooral operationele taken in plaats van toezichthoudende en adviestaken uit. Er waren vorig jaar geen privacy officer(s) en/of ambassadeurs actief, hierdoor is juridische kennis en ervaring onvoldoende geborgd. Er loopt een bewustwordingscampagne maar deze moet verder worden geprofessionaliseerd.
4. RECHTEN VAN BETROKKENEN Transparantieverplichting richting betrokkenen	De procedure Rechten van betrokkenen is beschreven deze is echter onvoldoende geborgd in de organisatie. Sinds 2022 is het wel mogelijk om via DigiD digitaal een verzoek in te dienen. Er vindt binnen Werkzaak geen geautomatiseerde besluitvorming plaats. Niet op alle vlakken wordt er transparant en helder over privacygerelateerde onderwerpen gecommuniceerd.

4b. Status AVG

BESTUURLIJKE UITGANGSPUNTEN

Bestuurlijke principes en beleid, organisatie van privacy en naleving

Het bestuur van Werkzaak:

- Volgt het beleid van de VNG/IBD
- Zorgt ervoor dat privacy op de juiste manier door de organisatie wordt toegepast en uitgevoerd
- Controleert de juiste werking van privacy in de organisatie

Op het gebied van privacy en gegevensbescherming is in het algemeen nog veel winst te behalen. De uitkomsten uit de nulmeting worden gebruikt om de basis te leggen voor de doorontwikkeling en verdere implementatie (PDCA) van privacy binnen Werkzaak. De focus moet daarbij niet liggen op een 100% score maar op het minimaliseren van de privacyrisico's en het beschermen van de persoonlijke levenssfeer van onze cliënten en medewerkers.

5. SAMENWERKING Verantwoorde verwerking persoonsgegevens door derden	Er is beperkt overzicht in de externe partijen en samenwerkingspartners waarmee Werkzaak samenwerkt en verantwoordelijk voor is. De daarbij behorende (verwerkers)overeenkomsten worden niet structureel afgesloten. Intern kunnen eenmalige gegevensverstrekkingen via een formulier worden aangevraagd en getoetst aan de privacybeginselen.
6. BEVEILIGING Passende technische en organisatorische maatregelen	Er wordt geen eenduidig privacy by design en default beleid/procedure gehanteerd. Daardoor worden privacy eisen niet structureel meegenomen in de aanbesteding/aanpassing van systemen/software. Er is een vastgestelde procedure en meldformulier voor het melden van datalekken. In het geval van grote incidenten/datalekken is er geen crisisplan. Intern ontbreekt er een vastgesteld loggingsbeleid.
7. NALEVING Verantwoordingsplicht AVG	Er worden geen periodieke evaluaties en/of DPIA's uitgevoerd. Op ad hoc basis vinden er wel evaluaties en risico analyses plaats. Jaarlijks wordt er vanuit privacy gerapporteerd over de stand van zaken en in 2022 is er voor de eerste keer een nulmeting uitgevoerd.

Alleen samen houden we Werkzaak veilig!

WERKZAAK RIVIERENLAND
Talent werkt voor Rivierenland