

Memo AB

Aan: AB Werkzaak Rivierenland

Van: Jos Baan (FG), Marlieke Meersschaert (Privacy Officer), Robin Heffelaar (Ciso)

Datum: 15 mei 2025

Onderwerp: Bestuursrapportage Informatiebeveiliging en Privacy 2024

Doel memo: het AB informeren

De Functionaris gegevensbescherming (FG) en Chief Information Security Officer (CISO) brengen periodiek verslag uit van de uitgevoerde werkzaamheden, de bevindingen en geven aanbevelingen aan het dagelijks bestuur in haar rol als eindverantwoordelijk orgaan voor de verwerkingen van persoonsgegevens en op het gebied van informatiebeveiliging. Het dagelijks bestuur wordt geïnformeerd vanuit de wettelijke taak van de FG en CISO om toe te zien op de naleving van de privacywetgeving, informatiebeveiligingsmaatregelen en het interne beleid. Dit is vastgelegd in de BIO2 onder 5.02.02: *“Er is een CISO aangesteld die bevoegd is om onafhankelijk en zelfstandig te adviseren en te rapporteren aan het bestuur en of het controlerend orgaan over informatiebeveiliging.”*, en in de AVG onder artikel 38 lid 3: *“...De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.”* Dit jaarverslag is bedoeld voor het dagelijks bestuur enerzijds als controlerend orgaan, anderzijds als zelfstandig orgaan voor de verwerkingen van persoonsgegevens.

Werkzaak heeft de afgelopen jaren veel gedaan op het gebied van informatiebeveiliging en privacy. Om in kaart te brengen in hoeverre Werkzaak invulling geeft aan de gestelde normen voortkomend uit de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG) is er een meting uitgevoerd. De meting is uitgevoerd met behulp van het Information Security Management System (ISMS).

Werkzaak wil op ieder moment een actueel en accuraat overzicht hebben van alle aandachtspunten die betrekking hebben op de implementatie (uitvoering en borging) van de BIO en AVG. Alleen op basis van duidelijke, beschreven en geborgde processen kan er PDCA-gericht worden gewerkt en kunnen risico's worden herkend en gemitigeerd. De focus ligt hierbij op het minimaliseren van de risico's en het beschermen van de persoonlijke levenssfeer van onze cliënten en medewerkers en niet op een 100% score van de normen.

Het beoogde effect van deze rapportage voor Werkzaak is:

- Minimaliseren van de risico's en het beschermen van de persoonlijke levenssfeer van de cliënten en medewerkers van Werkzaak (in control komen)
- PDCA-gericht werken d.m.v. periodieke cyclus BIO en AVG

- Werkzaak is bewust bekwaam op het gebied van informatiebeveiliging en privacy
- Kunnen anticiperen op de wettelijke verplichtingen uit de nieuwe wet- en regelgeving zoals de NIS2

Op het gebied van informatiebeveiliging en privacy in het algemeen is Werkzaak op de belangrijkste onderdelen in control. Er is een flinke verbetering te zien ten opzichte van de eerste meting uit 2022. De resultaten uit de eerste meting hebben geleid tot verbeterpunten en maatregelen die in 2023 en 2024 zijn ingevoerd en waarvan sommige maatregelen nu nog lopen. Vooral in het kader van bewustzijn zijn er flinke stappen gemaakt de afgelopen jaren. De uitkomsten uit de meting worden gebruikt om de basis te leggen voor de doorontwikkeling en verdere implementatie (PDCA) van informatiebeveiliging en privacy binnen Werkzaak.