BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 951

29 september 2023

Officiële uitgave van de gemeenschappelijke regeling WVS-groep

Privacy beleid

Binnen WVS wordt veel gewerkt met persoonsgegevens van medewerkers. Persoonsgegevens worden verzameld bij de medewerkers voor het uitvoeren van onderdelen van de Wet sociale werkvoorziening, de Participatiewet en voor de wettelijke taken als werkgever.

De medewerkers en overige betrokkenen moeten er op kunnen vertrouwen dat WVS zorgvuldig en veilig met de persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen in toenemende mate eisen aan de bescherming van gegevens en privacy.
WVS, bestuur en management, is zich bewust van de verantwoordelijkheid op het gebied van het borgen van privacy en informatiebeveiliging.

Dit beleid biedt een kader om (toekomstige) maatregelen voor de verwerking en bescherming van persoonsgegevens te toetsen aan wetgeving en/of vastgestelde 'best practices' (of norm) en om de taken, verantwoordelijkheden en bevoegdheden van WVS te beleggen.

Doel en reikwijdte

Het privacy beleid heeft als doel het waarborgen van de rechten en vrijheden van alle betrokkenen op het gebied van verwerking van persoonsgegevens door WVS. Het beschrijft de organisatie, inrichting en de borging van de verwerking en bescherming van persoons-gegevens. Het is gericht op de kwaliteit, beschikbaarheid en beveiliging van informatie, waaronder persoonsgegevens, waarbij er een juiste balans gezocht wordt tussen privacy, functionaliteit en veiligheid. De reikwijdte van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van WVS en externe partijen en het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Voor wie is dit beleid

Het privacy beleid is van toepassing op de gehele organisatie d.w.z. bestuur, management en medewerkers.

Gebruikte afkortingen

AVG: Algemene Verordening Gegevensbescherming
UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming
BIO: Baseline Informatiebeveiliging Overheid, van toepassing voor Gemeenten
ISO 27001&2: Standaard voor Informatiebeveiliging
IT: Informatie Technologie
FG: Functionaris Gegevensbescherming
CISO: Chief Information Security Officer/ informatiebeveiliger

Uitgangspunten

WVS houdt zich aan de volgende uitgangspunten:

- De basis voor het privacy beleid is voldoen aan de Algemene Verordening Gegevensbescherming (hierna AVG), het Uitvoeringsbesluit AVG (hierna UAVG) en de fair information principes (OECD 1980).
- De basis voor het beschermen van persoonsgegevens en de inrichting van het WVS informatiebeveiligingsmanagement is ISO 27001. Formele certificering conform ISO 27001 wordt voor WVS niet als noodzakelijk gezien. Wel stelt WVS vanuit de regierol BIO minimale eisen aan certificeringen voor hosting partijen, Saas en Vendoren. Tevens is WVS aangesloten bij de Informatie Beveiligings Dienst (IBD) Gemeenten.
- Waar het gaat om de verwerking en beveiliging van medische gegevens wordt er gewerkt met partijen / applicaties die voldoen aan NEN 7510.
- Maatregelen worden genomen op basis van 'best practices' waarbij het op ISO 27002 gebaseerde Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt wordt genomen.
- Informatiebeveiliging gaat over alle IT- en informatiemiddelen en -processen, waarbij vooral 3 aspecten van belang zijn, nl. beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

- Een risicoanalyse vormt de basis voor passende maatregelen. Ten behoeve van deze risicoanalyse worden gegevens en systemen geclassificeerd volgens de BIV methodiek.
- Privacy en informatiebeveiliging is ieders verantwoordelijkheid.
- De verantwoordelijkheid voor privacy en informatiebeveiliging wordt in de lijn en binnen het bedrijfsproces belegd en kan afdeling overschrijdend zijn.
- Aandacht voor de wijze waarop persoonsgegevens beveiligd zijn is een continu proces. Ontwikkelingen binnen en buiten de organisatie maken het noodzakelijk om periodiek beleid en maatregelen te auditeren en te evalueren.
- Privacy en informatiebeveiligingsmanagement worden als proces ingericht.
- Beleid, procedures en werkwijzen worden opgenomen in de periodieke evaluatiecyclus volgens de “Plan, Do, Check, Act” methodiek.
- Aandacht voor informatiebeveiliging en privacy is onderdeel
  - van elke aanpassing van de IT infrastructuur
  - en ontwerp van nieuwe bedrijfsprocessen en aanpassing van bestaande processen.
- Privacy management en informatiebeveiliging hebben elk afzonderlijk aandacht binnen de jaarplannen van WVS.

Evaluatie en borging
Dit beleid wordt opgesteld voor een periode van drie jaar. Het beleid wordt tenminste iedere 3 jaar geëvalueerd en aan de hand van de review wordt bepaald of het beleid aangepast moet worden. De bevindingen van de interne en externe controles evenals mogelijke externe eisen t.a.v. beveiliging en verwerking zijn input voor de nieuwe jaarplannen van WVS. Deze kunnen ook tot wijziging van dit beleid leiden. De naleving bestaat uit concreet toezicht op de dagelijkse praktijk van het verwerken van persoonsgegevens. Van belang hierbij is dat leidinggevenden de medewerkers aanspreken in geval van tekortkomingen. Voor de toetsing op de naleving van de AVG is de Functionaris Gegevensbescherming (FG) verantwoordelijk.

Rollen taken en verantwoordelijkheden
In het privacy beleid van WVS worden de volgende rollen onderscheiden:

Bestuur
Eindverantwoordelijk voor het privacy en informatiebeveiligingsbeleid. Het bestuur stelt het beleid vast. Het bestuur verleent vervolgens mandaat aan de directie van WVS.

Directie
De directie is verantwoordelijk voor de informatiebeveiliging en de verwerking van persoonsgegevens binnen WVS en stelt de basismaatregelen vast.

Portefeuillehouder en privacy
Privacy valt onder de verantwoordelijkheid van de portefeuillehouder privacy. Dit is de algemeen directeur van WVS.

Functionaris Gegevensbescherming (FG)
De FG houdt toezicht op de toepassing en naleving van de AVG en toets dit periodiek. Hij geeft gevraagd en ongevraagd advies aan het hoogste managementniveau en werkt zonder instructie. Hij is intermediair tussen de organisatie en de Autoriteit Persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie.

Privacy Officer
De privacy officer geeft het privacy beleid operationeel uitvoering en is tevens de coördinator van het privacy team. Hij adviseert proceseigenaren over een privacy bestendige uitvoering van gegevensverwerkingen. Verder is hij verantwoordelijk voor het actueel houden van het register van verwerkingen.

Chief Information Security Officer (CISO)
De CISO is een rol op strategisch en tactisch niveau. Hij adviseert de directie. De CISO geeft advies over het informatiebeveiligingsbeleid en helpt bij een juiste vertaling daarvan naar de bedrijfsonderdelen,

ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden.

Proceseigenaar
Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, al dan niet gebruikmakend van meerdere systemen.

Privacy Team
Privacy teamleden zijn medewerkers die de organisatie ondersteunen bij operationele privacy & informatiebeveiligingsactiviteiten en zijn aanspreekpunt voor collega's op dit gebied.

Bewustwording en opleiding
De zwakste schakel bij privacy en security is "de mens". Medewerkers dienen zich bewust te zijn van de risico's, valkuilen en impact van cybercrime en het bewust beveiligen van de (persoons)gegevens-informatie waarmee ze werken. Vanaf april 2023 organiseert WVS voor alle medewerkers met een zakelijk emailadres security awareness trainingen in de vorm van (maandelijkse) e-learning modules. Deelname hieraan is niet vrijblijvend. Indien nodig organiseert WVS voor specifieke groepen medewerkers bedrijfs brede bewustwordingssessies die in brede zin aandacht geven aan het omgaan en beveiligen van bedrijfs-, en persoonsgegevens.

Informatiebeveiliging
Er zal een Informatiebeveiligingsplan worden opgesteld waarbij de Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt wordt genomen.

Wet en regelgeving
Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringsbesluit AVG (UAVG)
WVS heeft de wettelijke vereisten met betrekking tot het verwerken van persoonsgegevens ingebed in dit beleid. Handelen conform dit beleid leidt in beginsel tot voldoen aan de beveiligingsvereisten uit de wet.
Archiefwet (bewaartermijnen)
WVS houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die zijn vastgelegd in de Archiefwet. Dit betreft alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e-mail enzovoorts.
Auteurswet en portretrecht
WVS respecteert auteursrechten en portretrecht en handelt daarnaar. Er worden heldere afspraken gemaakt met medewerkers en overige betrokkenen.
Telecommunicatiewet
De Telecommunicatiewet is o.a. van toepassing daar waar cookies worden gebruikt op eigen websites, bij gebruik van nieuwsbrieven en de diverse vormen van online marketing.

Normering en standaarden
- ISO 27001 & 2,
- Privacy principles (Fair information principles / OECD 1980), ISO 29100,
- NEN 7510.

Vaststelling en wijziging
Dit privacy beleid treedt in werking op de dag na vaststelling door het dagelijks bestuur van WVS. Op de datum van in werking treding komt het privacy beleid zoals vastgesteld op 25 mei 2020 te vervallen. Vaststelling en aanpassingen van dit beleid worden aangekondigd via de website en / of OneTeam. De meest actuele versie van het beleid is te vinden op Zenya.

Aldus vastgesteld door het dagelijks bestuur op 25 september 2023.
De secretaris, De voorzitter,
P.F.J.M. Havermans T.C. Melisse.