Informatiebeveiligings- en privacy beleid

Samenwerkingsverband Zuidoost-Friesland VO

Versie	Status	Datum	Auteur	Omschrijving
1.0	vastgesteld	19/06/2023	MdV	Vastgesteld na bespreking MrP
0.1	Concept	09/03/2021	MdV	- Check versie juni 2020 na overname werkzaamheden - Aanpassingen obv template kennisnet - Vervolgens ter vaststelling incl. MRp. Nb. Versiebeheer is sindsdien opgestart.

Vastgesteld door

Versie	Datum	Naam	Functie
1.0	19/06/2023	Jan Boven	Directeur

Bron: Kennisnet
Bewerkt door: Samenwerkingsverband Zuidoost Friesland

Inhoudsopgave

1. Het belang van informatiebeveiliging en privacy in het samenwerkingsverband 3
2. Toelichting informatiebeveiliging en privacy 3

a. Toelichting informatiebeveiliging 3
b. Toelichting privacy 3
c. Vervlechting informatiebeveiliging en privacy 3

3. Doel en reikwijdte 4

a. Het doel 4
b. Het samenwerkingsverband en de persoonsgegevens 4
c. Reikwijdte 5

4. Beleid – Hoe doen we dat? 5
5. Uitwerking van het beleid – Wat doen we? 6

a. Relevante wet- en regelgeving 6
b. Basisregels bij het omgaan met persoonsgegevens 7
c. Ondersteunende richtlijnen en procedures 7
d. Voorlichting en bewustzijn 7
e. Classificatie en risicoanalyse 7
f. Incidenten en datalekken 8
g. Planning en controle 8
h. Naleving en sancties 8
i. Logging en monitoring 8

6. Organisatie: rollen en verantwoordelijkheden 9
Bijlagen 10

1. Het belang van informatiebeveiliging en privacy in het samenwerkingsverband

Het samenwerkingsverband Zuidoost Friesland VO (het samenwerkingsverband) is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe. Het samenwerkingsverband wil op een goede en zorgvuldige manier omgaan met persoonsgegevens van ouders, leerlingen en personeel. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Daarom is het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid noodzakelijk. Zo kunnen we de gevolgen van deze risico's tot een aanvaardbaar niveau reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal waarborgen.

Dit doet het samenwerkingsverband binnen de kaders van de wet- en regelgeving van de Algemene verordening gegevensbescherming (AVG), per 25 mei 2018. Het gaat wettelijk om drie taken in dit verband:

- Het toelaatbaar verklaren van leerlingen tot (voortgezet) speciaal onderwijs, het praktijkonderwijs, het geven aan aanwijzingen voor Leerwegondersteunend onderwijs (LWOO) en het afgeven van beschikkingen voor het OPDC;
- Het geven van adviezen aan de aangesloten scholen over de ondersteuningsbehoeften van leerlingen;
- Het toekennen van middelen voor extra ondersteuning en -voorzieningen aan scholen, ten behoeve van de ondersteuning van leerlingen.

2. Toelichting informatiebeveiliging en privacy

a. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een aantal samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

b. Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

c. Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP.

Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen het samenwerkingsverband te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

a. Het doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs, de dienstverlening en de bedrijfsvoering
- Het garanderen van de privacy van alle betrokkenen waarvan het samenwerkingsverband persoonsgegevens verwerkt van leerlingen, hun ouders/verzorgers en de medewerkers van het samenwerkingsverband
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het IBP-beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren. Daarbij moet er een juiste balans zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en het samenwerkingsverband voldoet aan relevante wet- en regelgeving.

b. Het samenwerkingsverband en de persoonsgegevens

Het samenwerkingsverband wordt voor het ICT-beheer ondersteund door een ICT-bedrijf. Met dit bedrijf is een verwerkersovereenkomst afgesloten.
Het samenwerkingsverband heeft vanuit haar taken te maken met de volgende persoonlijke informatie:

Aanvragen van scholen en toekenningen door het samenwerkingsverband i.v.m. toelaatbaarheidsverklaringen voor praktijkonderwijs en vso, aanwijzingen voor lwoo en beschikkingen voor het OPDC;

- Het gaat hier om aangeleverde dossiers
- Via Indigo worden deze gegevens beveiligd aangeleverd en verwerkt. Indigo voldoet aan alle veiligheidseisen voor de AVG. Met Indigo is een verwerkingsovereenkomst afgesloten.

Informatie over leerlingen van de diverse scholen die op het OPDC onderwijs krijgen en begeleid worden:

- Het gaat hier om de leerlingdossiers van het OPDC
- Voor zover dit het OPP van de leerlingen betreft, geldt per leerling het IBP-beleid van de school waar de leerling staat ingeschreven. Er is geen verwerkers overeenkomst tussen samenwerkingsverband en scholen nodig.
- Voor zover het gaat om eigen leerlinggegevens van het OPDC geldt dat deze zijn opgenomen in een beveiligde Office365-omgeving met beperkte autorisatie van alleen de betrokkenen rondom de leerling. Dit valt onder de eigen verantwoordelijkheid van het samenwerkingsverband. Wie geautoriseerd zijn, staat in de autorisatiematrix

Informatie van het consultatieteam en het thuiszittersteam over leerlingen die ondersteund worden door medewerkers van het samenwerkingsverband:

- Hiervoor geldt per leerling het IBP-beleid van de school waar de leerling staat ingeschreven.
- Voor zover het gaat om eigen leerlinggegevens van het samenwerkingsverband geldt dat deze zijn opgenomen in een beveiligde Office365-omgeving met beperkte autorisatie van alleen de betrokkenen rondom de leerling. Dit valt onder de eigen verantwoordelijkheid van het samenwerkingsverband. Wie waarvoor geautoriseerd zijn, staat in autorisatiematrix.

Informatie over de medewerkers van het samenwerkingsverband en van sollicitanten bij vacatures:

- Voor persoonsgegevens van de medewerkers geldt dat deze zijn opgenomen in een beveiligde Office

365-omgeving met beperkte autorisatie. Wie geautoriseerd zijn, staat in de autorisatiematrix. Met het administratiekantoor dat het programma AFAS gebruikt, is een verwerkersovereenkomst afgesloten.
- Voor het omgaan met gegevens van sollicitanten geldt de sollicitatiecode en de hierin opgenomen regeling rondom vertrouwelijkheid. Deze valt binnen de werkomgeving van Office365.

c. Reikwijdte

Medewerkers en bestuur van het samenwerkingsverband hanteren het volgende:

- Het IBP-beleid binnen het samenwerkingsverband geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het samenwerkingsverband waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het samenwerkingsverband persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het samenwerkingsverband. Hieronder valt ook de gecontroleerde informatie, die door het samenwerkingsverband zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop het samenwerkingsverband kan worden aangesproken. (Bijv. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of sociale media.)
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van het samenwerkingsverband evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen het samenwerkingsverband raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - *Medezeggenschap* van medewerkers

4. Beleid – Hoe doen we dat?

Het samenwerkingsverband hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van het samenwerkingsverband heeft de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. De verwerkingsverantwoordelijkheid is op grond van het bestuursmandaat opgedragen aan de directeur van het samenwerkingsverband.
2. Het bestuur van het samenwerkingsverband voldoet aan alle relevante wet- en regelgeving.
3. Bij het samenwerkingsverband is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één of meer van de wettelijke grondslagen. Een goede balans tussen het belang van het samenwerkingsverband om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. Het samenwerkingsverband zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Het samenwerkingsverband legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het samenwerkingsverband voldoet hiermee aan de documentatieplicht.
6. Binnen het samenwerkingsverband is het veilig en betrouwbaar omgaan met digitale en papieren informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. Het samenwerkingsverband is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert het samenwerkingsverband informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Het samenwerkingsverband classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. Het samenwerkingsverband sluit met alle leveranciers van digitale middelen verwerkersovereenkomsten af als zij, in opdracht van het samenwerkingsverband, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Het samenwerkingsverband verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het samenwerkingsverband heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij het samenwerkingsverband een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Het samenwerkingsverband kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy.
13. Het samenwerkingsverband neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt het samenwerkingsverband aanvullende afspraken vast over de technische maatregelen.
14. Het samenwerkingsverband zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5. Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

a. Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

b. Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen over verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de vijf vuistregels:

- *Doelbepaling en doelbinding:* persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
- *Grondslag:* verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen, te weten toestemming, een vitaal belang, en wettelijke verplichting, een overeenkomst, het algemeen belang en een gerechtvaardigd belang.
- *Dataminimalisatie:* bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
- *Transparantie:* de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
- *Data-integriteit:* er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

c. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Op de laatste pagina van dit IBP-beleidsplan staan alle bijlagen. Zij omvatten de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

d. Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Het bewustzijn van de individuele medewerkers wordt voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

e. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie van informatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van belang.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden.

f. Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregi
Alle (beveiligings)incidenten kunnen worden gemeld bij de P.O. en/of de F.G.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

g. Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door de directeur namens het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent het samenwerkingsverband een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

h. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bijvoorbeeld bij de aanstelling, tijdens functioneringsgesprekken, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG is aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan het bestuur van het samenwerkingsverband de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

i. Logging en monitoring

Logging en monitoring door IT-beheer zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6. Organisatie: rollen en verantwoordelijkheden

Binnen het samenwerkingsverband Zuidoost Friesland is in het kader van de verdeling van de taken en de rollen de hieronder beschreven rol en verantwoordelijkheidsverdeling van toepassing

Eindverantwoordelijk en vaststellen beleid	
Verwerkingsverantwoordelijke: Directeur op grond van de mandaatregeling met het bestuur.	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en communiceren ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Organisatie IBP inrichten; toewijzen van de taken en rollen en autorisaties • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Voorbeeldfunctie naar alle medewerkers
Voorbereiding en uitwerken beleid	
Privacy Officer	• (Laten) voorbereiden IBP-beleid, classificatie/risicoanalyse/autorisatie • Inhoudelijk verantwoordelijk voor uitwerking van IBP-beleid • Adviseert verwerkingsverantwoordelijke over IBP-beleidsaanpassingen • Uitwerken (nieuw) algemeen IBP-beleid naar uniform specifiek beleid • Beheren van processen, richtlijnen en procedures • Incident afhandeling: registreren en evalueren • Organiseren van de implementatie van nieuwe richtlijnen • Planmatige bewustwording (PDCA) van alle betrokken medewerkers • Toezien op de uitvoering door de medewerkers volgens PDCA-cyclus • Evalueren van het IBP-beleid en de maatregelen volgens PDCA-cyclus • Risicoanalyse in PDCA-cyclus (laten) uitvoeren • Voorbeeldfunctie naar alle medewerkers
ICT-beheerder	• Technisch aanspreekpunt voor IBP-incidenten. • Technisch advies en uitvoering inrichten ICT-structuur en beveiliging
Alle medewerkers	• Werken conform de vastgestelde richtlijnen, afspraken en procedures • Signaalfunctie en melden potentiële incidenten • Deelnemen aan scholing en bewustwording
Toezicht naleving en communicatie	
Functionaris voor gegevensbescherming	• Toezicht houden op naleving privacywetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Vraagbaak voor alle privacy-aandachtspunten

	• Voorlichting privacy geven en stimuleren van bewustwording • Afwikkeling IBP-klachten en incidenten (Autoriteit Persoonsgegevens)

Bijlagen

Het Privacyreglement is de basis voor het formele beleid en kent daarnaast de volgende werkprocessen en uitvoeringsregelingen:

1. Privacyreglement
2. Privacyverklaring
3. Rechten betrokkenen en procedure afhandeling verzoeken
4. Autorisatiematrix
5. Protocol beveiligingsincidenten en datalekken
6. Incident- en datalekregister
7. Verwerkersovereenkomsten
8. Risicoanalyse werkprocessen
9. Overeenkomst Functionaris voor Gegevensbescherming
10. Protocol sociale media
11. Bewustwording medewerkers
12. PDCA cyclus
13. Verwerkersregister
14. Protocol bewaartermijnen en vernietiging
15. Privacybeleid werknemers