



|                |   |
|----------------|---|
| Datum          | 30-01-2026  |
| Document       | Privacy<br>SWV PO 3106                                    |
| Onderwerp      | Jaarverslag 2025<br>Informatie- beveiliging en<br>Privacy |
| Team/project   | Directie van SWV PO 3106                                  |
| Opgesteld door | Mihelina Delarosette (FG)                                 |

## Inhoudsopgave

|   |    |
|---|----|
| 1. INLEIDING .....                                | 2  |
| 2. METHODIEK .....                                | 2  |
| 3. JAAROVERZICHT 2025 .....                       | 3  |
| 3.1 Activiteiten en contactmomenten in 2025 ..... | 3  |
| 3.2 Status Kindkans .....                         | 4  |
| 4. RESULTATEN TOETSINGSKADER .....                | 4  |
| 5. CONCLUSIE EN AANBEVELINGEN .....               | 6  |
| 6. AANBEVELINGEN EN VERBETERACTIES 2026 .....     | 7  |
| BIJLAGE 1: TOELICHTING PER STATEMENT .....        | 8  |
| BIJLAGE 2: RESULTATEN 2024 .....                  | 11 |

## 1. INLEIDING

De Samenwerkingsverband Passend Onderwijs Westelijke Mijnstreek (SWV PO 3104), Samenwerkingsverband Passend Onderwijs Maastricht Heuvelland (SWV PO 3105) en Samenwerkingsverband Passend Onderwijs Parkstad (SWV PO 3106) verwerken in het kader van hun taken persoonsgegevens van kwetsbare jongeren. Het gaat hierbij vaak om gevoelige en soms bijzondere persoonsgegevens, die direct raken aan de persoonlijke levenssfeer en veiligheid van deze jongeren. Juist vanwege hun kwetsbare positie is zorgvuldige omgang met deze gegevens van groot belang en brengt verantwoordelijkheden met zich mee op het gebied van privacy en gegevensbescherming. De Algemene Verordening Gegevensbescherming (AVG) stelt duidelijke eisen aan het verwerken, beveiligen en verantwoorden van persoonsgegevens, ongeacht de omvang van de organisatie.

Dit jaarverslag heeft als doel inzicht te geven in de wijze waarop SWV PO in het afgelopen jaar invulling heeft gegeven aan deze verantwoordelijkheden. Het biedt transparantie over de verwerkingen van persoonsgegevens, de genomen maatregelen ter bescherming daarvan en de aandachtspunten en ontwikkelingen op het gebied van privacy en gegevensbescherming. Daarmee draagt dit verslag bij aan bewustwording binnen de organisatie en aan het vertrouwen van jongeren, ouders/verzorgers, bestuur, medewerkers en samenwerkingspartners.

Dit verslagjaar is het laatste jaar waarin de beoordeling plaatsvindt conform dit privacy gerichte toetsingskader met de 22 statements. De focus ligt in dit verslag nog primair op privacy en AVG-naleving. Vanaf verslagjaar 2026 zal de verantwoording plaatsvinden op basis van het nieuwe geïntegreerde kader voor privacy en informatiebeveiliging van Kennisnet, waarin gegevensbescherming een integraal onderdeel vormt van het bredere informatiebeveiligingsbeleid. Het jaarverslag 2026 zal conform dit nieuwe kader worden opgesteld.

## 2. METHODIEK

De status van de privacymaatregelen is beoordeeld aan de hand van een door de directie vastgesteld toetsingskader. Dit toetsingskader bestaat uit 22 privacy statements die inzicht geven in de mate waarin de organisatie voldoet aan de eisen van de Algemene Verordening Gegevensbescherming (AVG). De uitwerking van deze statements is opgenomen in bijlage 1. Bij de beoordeling is aansluiting gezocht bij artikel 32 AVG, waarin is bepaald dat verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen. Hierdoor hebben meerdere privacy statements raakvlakken met maatregelen op het gebied van informatiebeveiliging. De resultaten van deze toetsing vormen de basis voor dit jaarverslag.

Elk statement is getoetst op opzet, bestaan en werking. Opzet ziet op vastgesteld beleid en procedures, bestaan op de implementatie daarvan en werking op de naleving in de praktijk gedurende het verslagjaar. Per statement is een score toegekend van 0 tot en met 3, zoals toegelicht in tabel 1. De beoordeling is gebaseerd op aangeleverde informatie door betrokken medewerkers en beschikbare documentatie en bewijsstukken.

| Score | Omschrijving   |
|-------|--|
| 0     | Niet van toepassing  |
| 1     | Er is geen bewijsmateriaal waarmee opzet/bestaan of werking aangetoond kan worden. (ad hoc)  |
| 2     | Opzet, bestaan en werking zijn per onderdeel gedeeltelijk aantoonbaar. Bijvoorbeeld: er is een beleidsdocument dat niet is vastgesteld, er is beperkt bewijsmateriaal beschikbaar om volledig te kunnen toetsen. |
| 3     | Er is een beleidsstuk of een procedure met bewijsstukken die implementatie en werking aantonen.  |

Tabel 1: toelichting score toetsingskader

Op basis van de behaalde scores en de vastgestelde status kan de organisatie gerichte keuzes maken voor verdere verbetering en borging van privacy en informatiebeveiliging.

De gemiddelde score van de resultaten zijn te vertalen naar het volwassenheidsniveau van de organisatie volgens de onderstaande tabel. Om volwassenheidsniveau 3 te kunnen bereiken zullen in het toetsingskader genoemde maatregelen bij alle statements in opzet, bestaan en werking aangetoond moeten zijn.

| Niveau | Omschrijving   |
|--------|--|
| 1      | Processen zijn ad hoc georganiseerd en erg afhankelijk van bepaalde personen.<br><b>Ad hoc.</b>  |
| 2      | Herhaalbaar maar intuïtief. Er wordt op een vaste manier gewerkt.<br><b>Beleid is gemaakt en goedgekeurd en bij een kleine groep bekend (opzet en bestaan).</b>          |
| 3      | Gedefinieerd proces. De processen zijn gedocumenteerd en bekend bij betrokkenen. <b>Beleid is bij alle betrokken medewerkers, relaties en externen bekend (werking).</b> |
| 4      | Beheerd en meetbaar. De processen worden beheerd, zitten in een verbetercyclus en zijn meetbaar (PDCA).<br><b>IBP is onderdeel geworden van de PDCA cyclus.</b>          |
| 5      | Geoptimaliseerd. Er wordt als vanzelfsprekend verbeterd en volgens best practice gewerkt.<br><b>IBP is toekomstbestendig, effectief en efficiënt.</b>                    |

Tabel 2: Volwassenheidsniveau

### 3. JAAROVERZICHT 2025

#### 3.1 Activiteiten en contactmomenten in 2025

In 2025 heeft de FG structureel invulling gegeven aan zijn toezichthoudende en adviserende rol. In dit jaar hebben drie privacy-overleggen plaatsgevonden en was er daarnaast regelmatig contact per e-mail. Tijdens deze momenten zijn verschillende onderwerpen besproken, waaronder Kindkans, het jaarplan en toetsingskader, de evaluatie van het beleidskader en aanbevelingen voor de actualisatie een analyse van de status binnen de SWV PO in het kader van het Privacy en informatiebeveiligingsnormenkader van Kennisnet.

Door de FG zijn in 2025 diverse adviezen uitgebracht, onder meer over de inzet van AI, de gebruikersovereenkomst voor apparatuur en gedragsafspraken. Daarnaast is op verzoek ook geadviseerd over het Model Privacy convenant samenwerking Onderwijs gemeenten en jeugdhulp. Naast het advies om lead te nemen en ervoor zorgen om die te ondertekenen is als vervolgstap ook een DPIA geadviseerd.

Voor de beoordeling van de privacyrisico's met betrekking tot Kindkans is in 2025 een externe adviseur ingeschakeld. Deze heeft eind 2025 een rapport uitgebracht.

In 2025 zijn totaal vijf incidenten geregistreerd, voor SWV PO 3105 drie en SWV PO 3106 twee. De oorzaken van deze incidenten lagen bij een foutieve koppeling van documenten en/of onjuiste autorisaties binnen de Kindkans. Alle incidenten deden zich voor binnen de bestaande gebruikersgroep van Kindkans die de constatering ook zelf hebben gemeld. Er was geen sprake van externe toegang of datalekken buiten de organisatie.

Op basis van de uitgevoerde risico-inschatting is vastgesteld dat het privacyrisico voor betrokkenen beperkt was. De incidenten zijn intern opgepakt en waar nodig zijn corrigerende maatregelen genomen. Gelet op de aard en impact van de incidenten is geconcludeerd dat melding bij de Autoriteit Persoonsgegevens (AP) niet noodzakelijk was.

### 3.2 Status Kindkans

Door aanhoudende vragen over de versleuteling van data in rust besloot het bestuur op 23 juni 2025 een onafhankelijke externe deskundige in te schakelen. Op basis van diens rapport en eindconclusie is door de FG in januari 2026 parallel met het opstellen van dit jaarverslag een eindadvies opgesteld. Aangezien in het jaar 2025 veel aandacht is besteed aan vervolg van Kindkans is door de FG besloten om een samenvatting van het advies op te nemen in dit jaarverslag.

De externe deskundige concludeert dat de toepassing van "99,9% encryptie van data in rust" binnen Kindkans geen materieel risico vormt. Het niet-versleutelbare deel is technisch zeer beperkt en uitsluitend theoretisch uitleesbaar bij fysieke toegang tot het datacentrum. Aangezien meerdere beveiligingslagen al vóór dit punt ingrijpen en alle betrokken partijen werken binnen professionele en gecertificeerde beveiligingskaders, wordt Kindkans in het rapport als veilig beoordeeld.

De FG heeft naar aanleiding van dit auditrapport aanvullende vragen gesteld over onder meer de positionering van betrokken partijen, certificeringen, auditverklaringen en de aantoonbaarheid van versleuteling. De nadere toelichting van de auditor heeft bijgedragen aan een beter begrip van de gehanteerde afwegingen. Tegelijkertijd constateert de FG dat er op enkele punten verschil blijft bestaan in perspectief, met name waar het gaat om de expliciete aantoonbaarheid van de technische implementatie van versleuteling in rust.

De FG concludeert dat absolute zekerheid over volledige versleuteling van data in rust niet kan worden gegeven. Hoewel het uitgevoerde onderzoek het restrisico verder heeft gemitigeerd, blijft een beperkt restrisico aanwezig. Gezien de aard en omvang van dit restrisico adviseert de FG om dit bestuurlijk te accepteren en tegelijkertijd de afspraken met de leverancier formeel vast te leggen. Dit omvat onder meer duidelijke afspraken over versleuteling, sleutelbeheer, rapportage, monitoring en periodieke verificatie, zodat sprake is van transparant en verantwoord risicobeheer. Dit advies geldt zowel voor de SWV PO 3104 alsook voor SWV PO 3105 en SWV PO 3106, die Kindkans reeds in gebruik hebben.

## 4. RESULTATEN TOETSINGSKADER

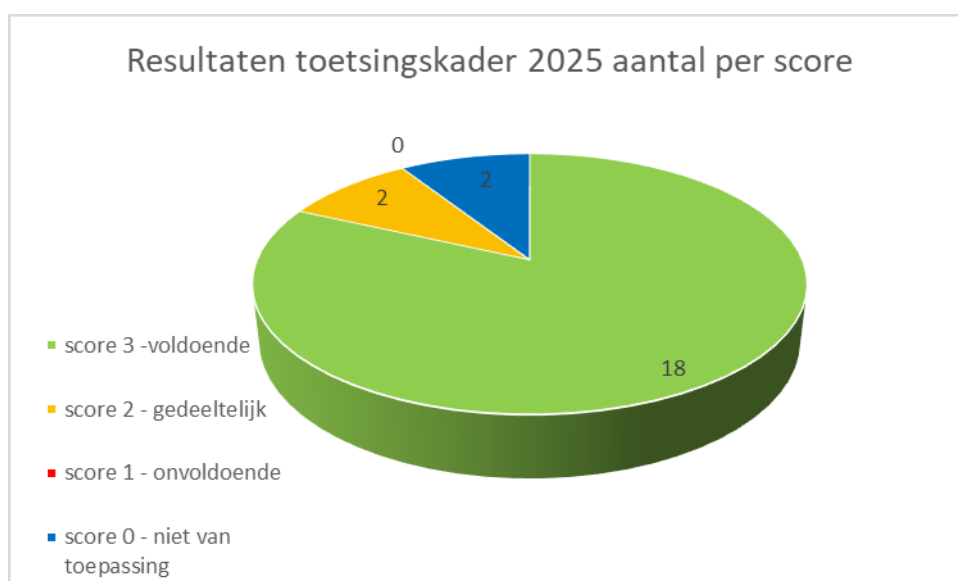
Binnen het borgingskader kan worden vastgesteld dat de resultaten in 2025 stabiel zijn gebleven. Op het gebied van informatiebeveiliging (IB) is zelfs een groei geconstateerd. Deze positieve ontwikkeling is te verklaren aan de aantoonbare werking van meerdere maatregelen, denk aan het vastgelegen en controleren van de autorisaties, inrichten van 2FA en consequent opschonen van de apparatuur en hanteren van bewaartermijnen.

De borging van privacy en informatiebeveiliging is mede mogelijk gemaakt door de inzet van de medewerker die, naast de eigen vakinhoudelijke rol, verantwoordelijk is voor het beheer van privacy binnen de organisatie. De combinatie van inhoudelijke kennis en praktische uitvoering draagt aantoonbaar bij aan de groei en kwaliteit van de naleving.

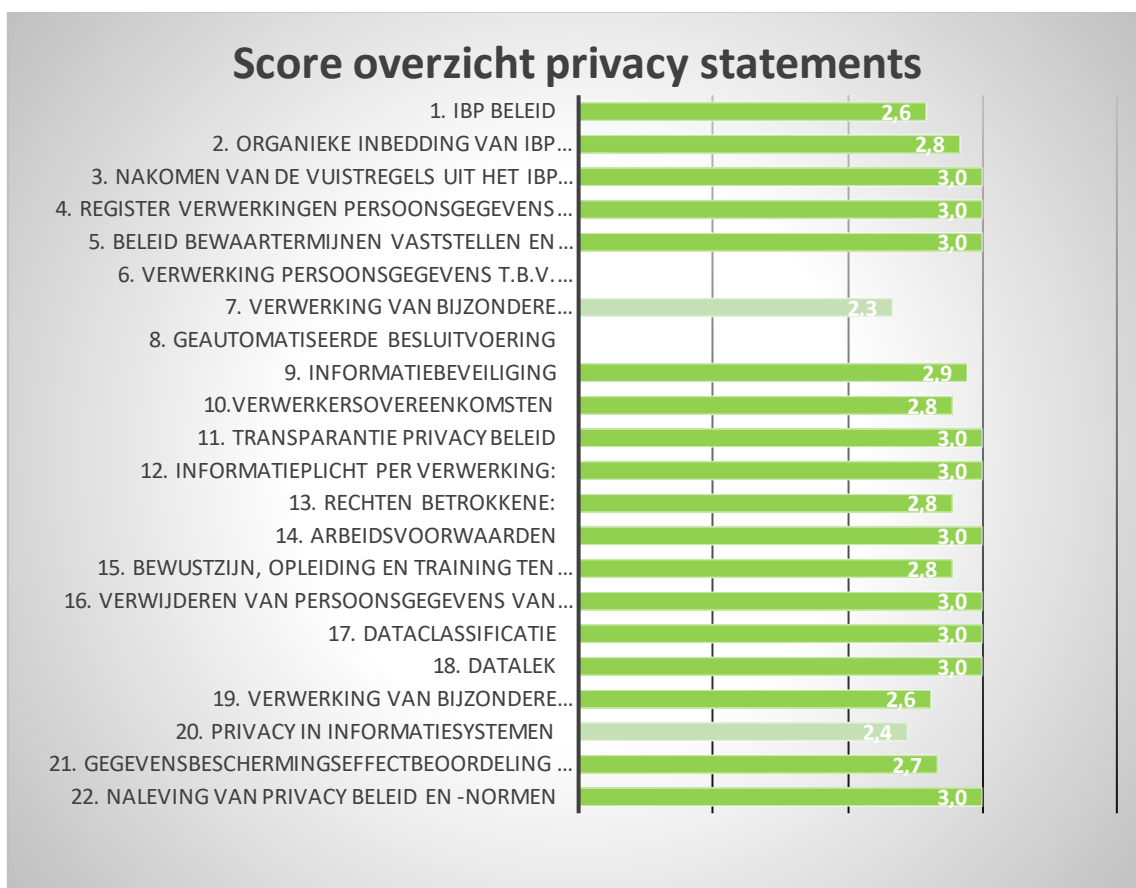
Met uitzondering van de geplande actualisatie van het beleid zijn alle in het jaarplan opgenomen acties afgerond. De aanbeveling met betrekking tot het vervolg van Kindkans is opgevolgd. Het bestaande privacy en informatiebeveiligingsbeleid blijft ongewijzigd nog van kracht. Daarbij blijft structurele aandacht bestaan voor bewustwording binnen de organisatie. In 2025 is er een AI training gevolgd door de medewerkers en zijn privacyonderwerpen besproken tijdens de werkoverleggen.

Vooruitkijkend is reeds voorzichtig nagedacht over de aanpak van de implementatie van het (vervolg) normenkader van Kennisnet in het nieuwe jaar. In 2026 zal het Privacy en Informatiebeveiliging beleid gezamenlijk met alle drie SWV PO worden geactualiseerd tot een integraal beleid. Waar bij de drie organisaties afwijkingen zijn, worden deze in een apart document verder uitgewerkt.

In 2026 zal bij de toetsing van de informatiebeveiliging het nieuwe Informatiebeveiligingskader van Kennisnet worden toegepast, wat de verantwoording van de score nog inzichtelijker maakt.



Grafiek 1: Resultaten toetsingskader 2025 SWV PO 3105 en SWV PO 3106



Grafiek 2: Score overzicht per statement 2025 SWV PO 3105 en SWV PO 3106

## 5. CONCLUSIE EN AANBEVELINGEN

Op basis van de uitgevoerde borgingsactiviteiten in 2025 kan worden geconcludeerd dat de organisatie privacy en informatiebeveiliging op een stabiel niveau heeft geborgd. Alle borgingsacties uit het jaarplan 2025 zijn uitgevoerd. De scores binnen het toetsingskader zijn stabiel gebleven ten opzichte van 2024, wat wijst op een consistente en adequate borging van gegevensbescherming.

Deze stabiliteit laat zien dat de ingezette maatregelen effect hebben. Tegelijkertijd blijft de continuïteit van borging essentieel. Dit vraagt blijvende aandacht voor de naleving van vastgestelde maatregelen en voor een zorgvuldige vastlegging van processen, zodat de organisatie aantoonbaar in control blijft en minder afhankelijk wordt van individuele inzet.

Het advies is om de ingezette koers voort te zetten en de beheersmaatregelen, gebaseerd op het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (Kennisset), verder te implementeren. Daarbij ligt een duidelijke afweging voor om hiervoor een ondersteunende tool in te zetten. De huidige capaciteit binnen de organisatie is beperkt in verhouding tot de hoeveelheid werkzaamheden en de vereiste mate van borging. Automatisering kan bijdragen aan overzicht, consistentie, monitoring en aantoonbaarheid, en daarmee de kwaliteit en duurzaamheid van de borging versterken.

Naast technische en organisatorische maatregelen blijft bewustwording een belangrijk aandachtspunt. Gerichte trainingen, afgestemd op rollen en verantwoordelijkheden, zijn noodzakelijk om kennis actueel te houden en correct handelen te bevorderen.

Bij de geplande actualisatie van het beleid in het komende jaar verdienen met name de volgende onderwerpen aandacht: het nieuwe informatiebeleidskader, een samenhangend bewustwordingsplan, de verwerking van bijzondere persoonsgegevens, de verdere uitwerking van de rechten van betrokkenen en de actualisatie van de toestemmingsverklaring.

## 6. AANBEVELINGEN EN VERBETERACTIES 2026

Op basis van de resultaten, doelstellingen en conclusie zijn de volgende verbeteracties voorgesteld voor 2026:

- Voortzetten van de implementatie van de beheersmaatregelen uit het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (Kennisset).
- Actualisatie Privacy en informatiebeveiligingsbeleid.
- Overweeg inzet van een ondersteunende tool voor privacy- en IB-borging, om vastlegging, monitoring en aantoonbaarheid te verbeteren en de beperkte capaciteit te ontlasten.
- Investeer structureel in gerichte trainingen en bewustwording, afgestemd op rollen en verantwoordelijkheden, om naleving en correct handelen te borgen. Maak een bewustwordingsjaarplan.

## BIJLAGE 1: TOELICHTING PER STATEMENT.

Om volwassenheidsniveau 3 op alle statements te kunnen aantonen zullen de hieronder genoemde maatregelen in werking moeten zijn. Deze toelichting beschrijft in detail de activiteiten en maatregelen die ingepland moeten worden om dit niveau te bereiken.

In 2022 kan de IBP-evaluatie worden ingepland.

| P | Omschrijving  |
|---|---|
| 1 | <b>IBP beleid:</b> <ul style="list-style-type: none"><li>a. Formuleren IBP beleid (zie ook statements 6,7 en 8)</li><li>b. Toetsingskader IBP benoemen in IBP beleid</li><li>c. Goedkeuren IBP beleid door bestuur</li><li>d. Communicatie IBP beleid naar medewerkers.</li></ul>   |
| 2 | <b>Organieke inbedding van IBP verantwoordelijkheden:</b> <ul style="list-style-type: none"><li>a. Het bestuur legt de verdeling van de IBP taken en verantwoordelijkheden vast</li><li>b. Het bestuur bekrachtigt deze met de nodige middelen en rapportage</li></ul>  |
| 3 | <b>Nakomen van de vuistregels uit het IBP beleid in het uitvoeringsdomein:</b><br>Gedragsregels IBP in kaart brengen, vereenvoudigen en goedkeuren.   |
| 4 | <b>Register verwerkingen persoonsgegevens HR en onderwijs</b> <ul style="list-style-type: none"><li>a. Inventariseren bestaande verwerkingen van persoonsgegevens (categorie personeel)</li><li>b. Inventariseren bestaande verwerkingen van persoonsgegevens (categorie leerlingen)</li><li>c. Proceseigenaren en manager IBP melden nieuwe of aangepaste verwerkingen van persoonsgegevens bij de FG/PO</li><li>d. De FG/PO houdt een register bij conform art. 30 AVG.</li></ul> |
| 5 | <b>Beleid bewaartermijnen vaststellen en uitvoeren</b> <ul style="list-style-type: none"><li>a. Per verwerking bewaartermijnen vastleggen (fysiek en digitaal).</li><li>b. Check of bewaartermijnen juist worden toegepast. Eventueel documenten opschonen</li></ul>  |
| 6 | <b>Verwerking persoonsgegevens t.b.v. onderzoek</b><br>Toevoegen aan IBP beleid, vastleggen dat proceseigenaar hierop toeziet.  |
| 7 | <b>Verwerking van bijzondere persoonsgegevens</b><br>Toevoegen aan IBP beleid, vastleggen dat proceseigenaar hierop toeziet.<br>Naleving via statements 9 en 19   |
| 8 | <b>Geautomatiseerde besluitvoering</b><br>Toevoegen aan IBP beleid, vastleggen dat proceseigenaar hierop toeziet.   |
| 9 | <b>Informatiebeveiliging</b> <ul style="list-style-type: none"><li>a. Om aan niveau 3 te voldoen moet de organisatie minimaal niveau 2 aantonen op 84 items uit het toetsingskader IB, d.w.z. opzet en bestaan en gedeeltelijke werking.<br/>Een aantal statements zou aan niveau 3 of 4 moeten voldoen om privacy risico's te mitigeren.</li></ul>   |

- b. Nadruk ligt op passende beveiliging bijzondere persoonsgegevens (zie ook st. 19)

10

- a. Model verwerkersovereenkomst vaststellen.
- b. Vanuit het register worden alle verwerkers en overeenkomsten benoemd.
- c. Per verwerker en per verwerking worden verwerkersovereenkomsten ondertekend.
- d. Periodieke controle en rapportage van nakoming afspraken uit overeenkomsten.

11

#### Transparantie privacy beleid

- a. De organisatie informeert ouders, bezoekers en leveranciers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en begrijpelijk in duidelijke en eenvoudige taal over het privacybeleid en de rechten en verplichtingen van betrokkenen.
- b. De organisatie informeert de medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en begrijpelijk in duidelijke en eenvoudige taal over het privacybeleid en de rechten en verplichtingen van betrokkenen.

12

#### Informatieplicht per verwerking:

- a. Ouders en bezoekers worden vooraf geïnformeerd over de verwerkingen waar hun persoonsgegevens bij betrokken zijn.
- b. Medewerkers worden vooraf geïnformeerd over de verwerkingen waar hun persoonsgegevens bij betrokken zijn.

13

#### Rechten betrokkene:

- a. Bezoekers en medewerkers van klanten worden actief geïnformeerd over hun privacy rechten.
- b. Medewerkers worden actief geïnformeerd over hun rechten.
- c. Workflow en werkwijze vastleggen en testen.
- d. Overzicht rechten betrokkenen opstellen.

14

#### Arbeidsvoorwaarden

- a. Medewerkers worden via arbeidsvoorwaarden gebonden aan de gedragscodes met betrekking tot privacy, security en acceptabel internet.
- b. Contractanten zijn via de leveringsvoorwaarden gebonden aan de gedragscodes met betrekking tot privacy, security en acceptabel internetgebruik.

15

#### Bewustzijn, opleiding en training ten aanzien van privacy

- a. Opleidingsplan met activiteiten voor het lopende jaar
- b. Overzicht met cursussen bijscholingen
- c. Documentatie m.b.t. de aanmelding en aanwezigheid van de cursisten
- d. Opleidingsmaterialen vastleggen

16

#### Verwijderen van persoonsgegevens van apparatuur

- a. Procedure voor het vernietigen van apparatuur, waarbij de vernietiging altijd gedocumenteerd wordt
- b. Checklijst voor verwijderen apparatuur conform procedure
- c. Registerlijst met alle verwijderde apparatuur met verwijzing naar het gebruik van persoonsgegevens

17

#### Dataclassificatie

- a. Overleg bewijs waaruit het beleid en de criteria rondom dataclassificatie blijken;
- b. Overleg de actuele BIV classificatie, dit kan zijn opgenomen in de dataregisters.

## 18 Datalek

- a. De meldplicht datalekken wordt genoemd in het beleid IBP
- b. De medewerkers zijn geïnformeerd over het beleid meldplicht datalekken (flyers en presentaties), kunnen datalekken herkennen en weten waar ze deze moeten melden.
- c. Privacy- en informatiebeveiligingsincidenten behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd aan de FG en de verantwoordelijke
- d. Er wordt een incidentenregister bijgehouden

## 19 Verwerking van bijzondere persoonsgegevens vraagt om extra maatregelen: (zie ook 7)

- a. Expliciet motiveren waarom deze noodzakelijk zijn.
- b. Gebruik blijft beperkt tot gevallen die strikt noodzakelijk en evenredig zijn.
- c. Speciale toegangsrechten worden beperkt en beheerst.
- d. Toewijzen van geheime authenticatie-informatie gaat volgens een formeel beheersproces.
- e. Gebruikers houden zich aan de gebruiksvoorschriften met betrekking tot geheime authenticatie-informatie
- f. Toegang tot systeemfuncties van toepassingen wordt beperkt volgens het beleid van toegangsbeperkingen en gelogd.
- g. Encryptie tijdens transport en in opslag.

## 20 Privacy in informatiesystemen

- a. Masterclass Privacy by Design voor leden Privacy Team incl. documentatie.
- b. Aandacht voor privacy is geborgd in de projectmethodiek en zichtbaar in de projectverslagen
- c. De FG heeft een voorafgaande adviesfunctie bij nieuwe verwerkingen

## 21 Gegevensbeschermingseffectbeoordeling (GBEB, voorheen PIA):

- a. Projectmethodiek beschrijft vereiste aandacht voor privacy en risico analyse. Dit komt aan de orde in de Masterclass Privacy by Design
- b. Aantoonbare periodieke evaluaties van de bestaande gegevensverwerkingen (hierin volgen we de aanpak en planning van de PO-raad).

## 22 Naleving van privacy beleid en -normen

Tenminste alle managers van de systemen en de belangrijkste processen stellen periodiek vast dat alle procedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van privacy beleid en -normen.

Kopie van 2 meest recente rapportages waaruit blijkt dat managers naleving vaststellen.

Voorbeelden:

- Naleving AVG op websites en social media aantonen.
- AVG Instructies secretariaat
- AVG Instructies OT
- Proces mdw in dienst/uit dienst/mutatie

## BIJLAGE 2: RESULTATEN 2024

### Score overzicht privacy statements

