



Datum	14-02-2025
Document	Privacy SWV PO 3105
Onderwerp	Jaarverslag 2024 Informatie- beveiliging en Privacy
Team/project	Directie van SWV PO 3105
Opgesteld door	Mihelina Delarosette (FG)

Inhoudsopgave

1. INLEIDING.....	2
2. METHODIEK.....	2
3. JAAROVERZICHT 2024	3
3.1 Activiteiten en contactmomenten in 2024.....	3
3.2 Kindkans, advies en risico's.....	4
4. RESULTATEN TOETSINGSKADER.....	4
5. CONCLUSIE EN AANBEVELINGEN.....	6
6. AANBEVELINGEN EN VERBETERACTIES 2025.....	6
BIJLAGE:.....	7
BIJLAGE 1: TOELICHTING PER STATEMENT.	7
BIJLAGE 2: RESULTATEN 2023	10

1. INLEIDING

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht en organisaties die persoonsgegevens verwerken zijn verplicht om aan de AVG te voldoen. Door de AVG en technische ontwikkelingen wordt het veld rondom privacy, verwerking van persoonsgegevens en informatiebeveiliging voor organisaties steeds complexer. Dit vereist voortdurend aandacht en monitoring. De functionaris gegevensbescherming (FG) houdt toezicht en adviseert gevraagd en ongevraagd over de naleving van wet- en regelgeving met betrekking tot de privacy van leerlingen, ouders, klanten, medewerkers en partners.

Op basis van dit jaarverslag informeert de FG directie van de SWV PO 3105 over de status van de implementatie en werking van de beheersmaatregelen op het gebied van privacy en informatiebeveiliging. Daarnaast wordt ingegaan op de uitdagingen die in het afgelopen jaar zijn tegengekomen en de verbeteringen die zijn doorgevoerd om toekomstige risico's te minimaliseren.

Het doel van organisatie is om een transparante en verantwoorde benadering van gegevensbescherming te handhaven, waarbij voortdurend wordt aangepast aan de veranderende wet- en regelgeving en technologische ontwikkelingen. De inzet blijft gericht op het waarborgen van de privacy en veiligheid van de gegevens die aan de organisatie zijn toevertrouwd.

2. METHODIEK

De status van de maatregelen wordt beoordeeld op basis van een door de directie goedgekeurd toetsingskader. Dit toetsingskader, bestaande uit 22 privacy statements, evalueert de naleving van de AVG en identificeert aandachtspunten. Details van deze statements zijn te vinden in bijlage 1. Conform Artikel 32 AVG nemen de verwerkingsverantwoordelijke en verwerker passende organisatorische en technische maatregelen om de verwerking te beveiligen. Hierdoor hebben een aantal statements raakvlakken met maatregelen in het kader van de informatiebeveiliging. De resultaten vormen de input voor dit jaarverslag.

Elk statement wordt getoetst op opzet, bestaan en werking, wat aantoont dat de organisatie haar beleid naleeft. De opzet verwijst naar beleid en procedures, bestaan naar de implementatie hiervan, en werking naar de naleving gedurende een jaar. De status van elke verklaring wordt met een score van 0 tot 3 aangeduid en toegelicht in tabel 1.

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.

Tabel1: toelichting score toetsingskader

Input voor de beoordeling zijn verstrekte informatie door betrokkene medewerker bij de SWV PO en beschikbare documenten en bewijsstukken in Teams omgeving.

SWV PO 3105 kan op basis van de score en status gericht keuzes maken voor de verdere naleving en borging van de AVG.

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

Tabel 2: Volwassenheidsniveau

3. JAAROVERZICHT 2024

3.1 Activiteiten en contactmomenten in 2024

Dit hoofdstuk beschrijft de activiteiten van de FG in 2024.

In januari 2024 hebben SWV PO 3105 en SWV PO 3106 Kindkans in gebruik genomen. Na deze constatering heeft de FG een formeel negatief advies uitgebracht aan de directie. Er is opnieuw geadviseerd om een gegevens-effect beoordeling (DPIA) uit te laten voeren voordat de applicatie in gebruik wordt genomen.

Daarnaast is in januari ook geadviseerd over het sluiten van de overeenkomst met de nieuwe ICT-leverancier.

In Q1 is verder ook het toetsingskader voor 2023 ingevuld en is het FG-jaarverslag 2023 opgeleverd.

Q2 stond in het teken van DPIA Kindkans. De FG heeft DPIA beoordeeld, aanvullende vragen gesteld en uiteindelijk in juni een advies uitgebracht. Het positief advies was uitgebracht met voorwaarde dat de leverancier aan de gestelde eisen gaat voldoen. Zie 3.2.

In 2024 hebben twee formele privacy overleggen met directie en FG plaatsgevonden. Door het jaar heeft FG voortdurend contact gehad met de directie over de stand van zaken met betrekking tot DPIA Kindkans en overige privacy gerelateerde vraagstukken.

De FG heeft geadviseerd over het bewustwordingsplan, inzetten en gebruik van de AI, actualiseren van het register van verwerkingen en zorgen voor de bewustwording bij de gebruikers van Kindkans door een privacy pop-up te maken en toestemmingsverklaring aan te passen.

In september is een mogelijke datalek gemeld op de website van de SWV PO. Na het uitvoeren van het aanvullend onderzoek is geconstateerd dat er geen persoonsgegevens zijn gelekt. Naar aanleiding van de melding heeft een opschoning plaatsgevonden op de website. Er is in 2024 één datalek incident gemeld en geregistreerd. Deze is als niet meldplichtig bij de Autoriteit Persoonsgegevens aangemerkt.

3.2 Kindkans, advies en risico's

In 2024 is veel aandacht besteed aan de applicatie Kindkans van de leverancier Gouwe Academie B.V.. De applicatie ondersteunt het bieden van passend onderwijs in samenwerkingsverbanden en onderwijsinstellingen. Binnen Kindkans worden persoonsgegevens verwerkt van leerlingen in het kader van passend onderwijs. Deze applicatie hebben SWV PO 3105 en SWV PO 3106 in januari 2024 ondanks ontbrekende maatregelen en negatief FG-advies (26-01-2024) in gebruik genomen. In samenwerking met de SWV PO 3104 is in het voorjaar alsnog een geveenseffect beoordeling (DPIA) uitgevoerd terwijl de applicatie al in gebruik was. Tijdens deze DPIA zijn risico's geconstateerd. Een hoog geclassificeerde risico is geen versleutelde opslag van gegevens in ruste. Om deze risico te mitigeren, heeft de FG in zijn advies op 21-06-2024 een eis gesteld dat dit door de leverancier uiterlijk aan het eind van het jaar 2024 opgelost moet zijn.

Vanuit de FG's Het Privacy Huys zijn over deze problematiek alarmbrieven naar het Kennisnet en de Autoriteit persoonsgegevens verstuurd.

Helaas is deze eis door de leverancier in de afgesproken termijn niet nagekomen, waardoor het risico op onveilige gegevensopslag blijft bestaan. Dit leidt tot een verhoogde kans op datalekken en mogelijke schendingen van de privacywetgeving. Het is essentieel dat er spoedig maatregelen worden genomen om dit risico te elimineren en de gegevensopslag te beveiligen volgens de gestelde eisen en normen. De directie SWV PO 3105 en SWV PO 3106 blijft in gesprek met de leverancier en volgens zijn plan zouden in Q1 2025 de maatregelen worden gerealiseerd. Indien de leverancier niet met een oplossing komt is de FG in 2025 genoodzaakt om het positief advies in te trekken.

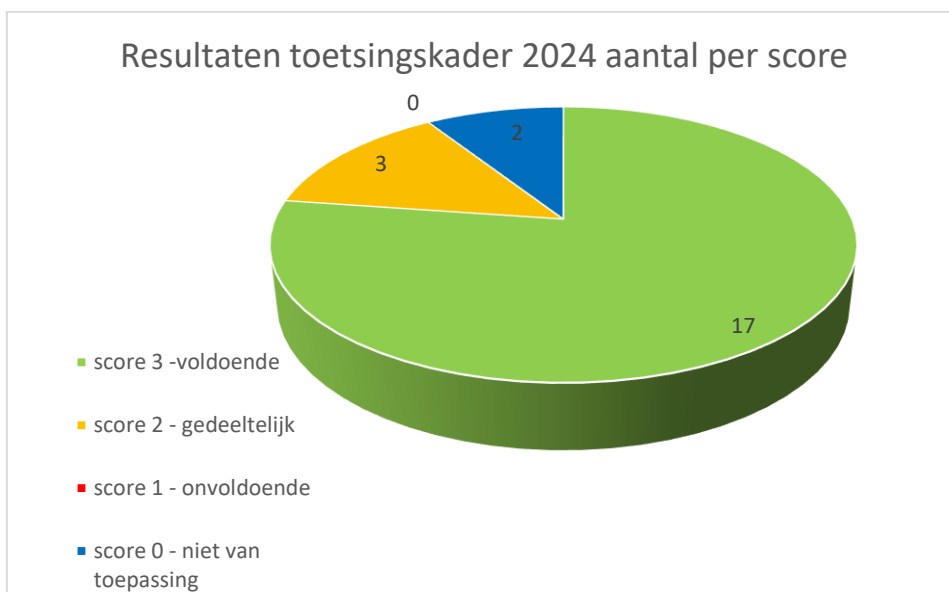
4. RESULTATEN TOETSINGSKADER

Alle borgingsacties uit het jaarplan (JAN) 2024 zijn uitgevoerd. DPIA Kindkans is afgerond. Twee van de drie aanbevelingen uit het advies van de FG zijn doorgevoerd. Het register van verwerkingen is geactualiseerd en data is geclassificeerd. Er is een overzicht van de geautoriseerde personen gegeneerd en beoordeeld. Er is bij de teamoverleggen structureel aandacht besteed aan de privacy en informatiebeveiliging.

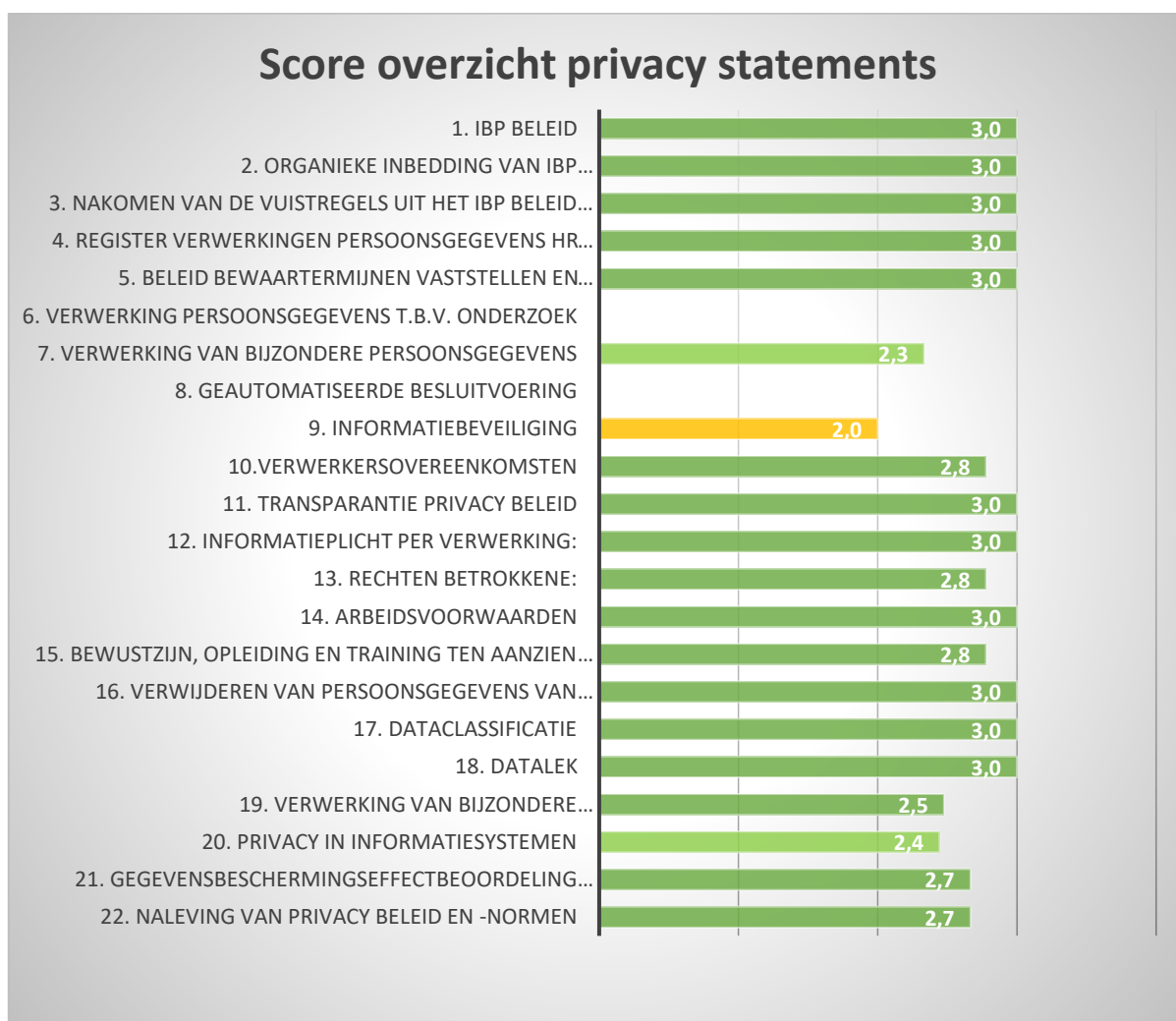
Aandachtspunt in het verslag van 2023 was het vastleggen van processen en handelingen. Dit is gedeeltelijk opgepakt. Door de kleine omvang van de organisatie en tijdsgebrek blijkt dit lastig te realiseren. De score in het toetsingskader zijn vergelijkbaar met 2023. Dit bewijst stabiele borging van de gegevensbescherming bij de SWV PO 3105.

In de onderstaande grafiek is te zien hoeveel statements in 2024 volledig voldoen (score 3) en waar nog verbetering mogelijk is (score 2). De statements met betrekking tot de verwerking van persoonsgegevens voor onderzoek en geautomatiseerde besluitvorming zijn niet van toepassing en hebben een score van 0.

De doelstelling blijft om de naleving en werking verder te optimaliseren, zodat gedeeltelijk aantoonbare statements (totaal 3) volledig aantoonbaar worden. Statements met een score van 2 moeten naar 3 worden gebracht en op dit niveau blijven. Daarnaast is het belangrijk dat statements met de huidige score van 3 deze score behouden. In 2025 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 2024 SWV PO 3105



Grafiek 2: Score overzicht per statement 2024 SWV PO 3105

5. CONCLUSIE EN AANBEVELINGEN

Alle borgingsacties uit het jaarplan 2024 zijn uitgevoerd. De scores in het toetsingskader zijn op enkele statements verbeterd of stabiel gebleven ten opzichte van 2023. Dit wijst op een goede gegevensbescherming. De continuïteit van borging blijft essentieel, met extra aandacht voor naleving van maatregelen en vastlegging van processen.

Het advies is om deze beheersmaatregelen te baseren op het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs gepubliceerd op Kennisnet. Het vastleggen maakt AVG-compliance aantoonbaar en borgt continuïteit. De kennis in de organisatie gaat niet verloren bij het vertrek of functiewijziging van een medewerker. Daarnaast is het van belang om in 2025 het risico dat door gebruik van Kindkans bestaat te elimineren.

Het nieuwe Informatiebeveiligingskader van Kennisnet zal in 2025 worden toegepast voor betere verantwoording. Dit kader kan de basis vormen bij de beoordeling en actualisatie van de privacy en informatiebeveiligingsbeleidskaders. De aandachtspunten bij de actualisatie zijn het nieuwe informatiebeleidskader, bewustwordingsplan, verwerking van bijzondere persoonsgegevens, uitwerking van de rechten van betrokkenen en toestemmingsverklaring.

6. AANBEVELINGEN EN VERBETERACTIES 2025

Op basis van de resultaten, doelstellingen en conclusie zijn de volgende verbeteracties voorgesteld voor 2025.

- Blijft in gesprek met de leverancier en zorg voor de versleutelde opslag in Kindkans.
- Actualiseer Privacy en informatiebeveiligingsbeleid.
- Maak een bewustwordingsjaarplan.
- Maak een plan voor de implementatie van het Normenkader Informatiebeveiliging en privacy.

BIJLAGE:

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	IBP beleid: <ul style="list-style-type: none">a. Formuleren IBP beleid (zie ook statements 6,7 en 8)b. Toetsingskader IBP benoemen in IBP beleidc. Goedkeuren IBP beleid door bestuurd. Communicatie IBP beleid naar medewerkers.
2	Organieke inbedding van IBP verantwoordelijkheden: <ul style="list-style-type: none">a. Het bestuur legt de verdeling van de IBP taken en verantwoordelijkheden vastb. Het bestuur bekrachtigt deze met de nodige middelen en rapportage
3	Nakomen van de vuistregels uit het IBP beleid in het uitvoeringsdomein: Gedragsregels IBP in kaart brengen, vereenvoudigen en goedkeuren.
4	Register verwerkingen persoonsgegevens HR en onderwijs <ul style="list-style-type: none">a. Inventariseren bestaande verwerkingen van persoonsgegevens (categorie personeel)b. Inventariseren bestaande verwerkingen van persoonsgegevens (categorie leerlingen)c. Proceseigenaren en manager IBP melden nieuwe of aangepaste verwerkingen van persoonsgegevens bij de FG/POd. De FG/PO houdt een register bij conform art. 30 AVG.
5	Beleid bewaartermijnen vaststellen en uitvoeren <ul style="list-style-type: none">a. Per verwerking bewaartermijnen vastleggen (fysiek en digitaal).b. Check of bewaartermijnen juist worden toegepast. Eventueel documenten opschoonen
6	Verwerking persoonsgegevens t.b.v. onderzoek Toevoegen aan IBP beleid, vastleggen dat proceseigenaar hierop toeziet.
7	Verwerking van bijzondere persoonsgegevens Toevoegen aan IBP beleid, vastleggen dat proceseigenaar hierop toeziet. Naleving via statements 9 en 19
8	Geautomatiseerde besluitvoering Toevoegen aan IBP beleid, vastleggen dat proceseigenaar hierop toeziet.
9	Informatiebeveiliging <ul style="list-style-type: none">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.

Een aantal statements zou aan niveau 3 of 4 moeten voldoen om privacy risico's te mitigeren.

- 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 2023

Score overzicht privacy statements

