Brabantse Wal

Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Informatiebeveiligings- en privacy beleid (IPB)

Samenwerkingsverband Brabantse Wal VO

Vastgesteld door Samenwerkingsverband Brabantse Wal VO

Versie	Datum	Naam	Functie
1.0	9 juli 2020	T..J. van Rijzewijk	Directeur-bestuurder
1.0		E. van den Bosch	Voorzitter Ondersteuningsplanraad

T.J. van Rijzewijk

E. van den Bosch

Brabantse Wal

Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Brabantse Wal
Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Het belang van informatiebeveiliging en privacy

Het onderwijs - zo ook het samenwerkingsverband - is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. 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. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Toelichting informatiebeveiliging en privacy

Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid 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 persoonlijke- en financiële schades en imagoverlies.

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.

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 Samenwerkingsverband Brabantse Wal VO te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

Doel en reikwijdte

Doel

IBP-beleid heeft de volgende doelen:

- Het waarborgen van de continuïteit van de werkzaamheden/taken binnen het (i.c. passend) onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Samenwerkingsverband Brabantse Wal VO persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- 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 waarbij er een juiste balans moet 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 Samenwerkingsverband Brabantse Wal VO voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen Samenwerkingsverband Brabantse Wal VO geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle apparaten van waar geautoriseerde toegang tot het netwerk verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Samenwerkingsverband Brabantse Wal VO, waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Samenwerkingsverband Brabantse Wal VO persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Samenwerkingsverband Brabantse Wal VO. Hieronder valt tevens de gecontroleerde informatie, die door het samenwerkingsverband zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop het samenwerkingsverband kan worden aangesproken (b.v. uitspraken van medewerkers in discussies, op (persoonlijke pagina's van) websites en of social media).

- Het IBP-beleid geldt voor de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Samenwerkingsverband Brabantse Wal VO 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 Samenwerkingsverband Brabantse Wal VO raakvlakken met o.a.:
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers en vertrouwensfuncties.
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen.

Beleid – Hoe doen we dat?

Samenwerkingsverband Brabantse Wal VO hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van Samenwerkingsverband Brabantse Wal VO neemt 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. In termen van de wet is het bestuur de 'verwerkingsverantwoordelijke'.

2. Samenwerkingsverband Brabantse Wal VO voldoet aan alle relevante wet- en regelgeving.

3. Bij Samenwerkingsverband Brabantse Wal VO is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Samenwerkingsverband Brabantse Wal VO 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 te allen tijde hun toestemming herzien.

4. Samenwerkingsverband Brabantse Wal VO zal alle betrokkenen helder en actief informeren over de verwerkingen van 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 (bezwaar tegen –verdere- verwerking van persoonsgegevens), dataportabiliteit en profilering.

5. Samenwerkingsverband Brabantse Wal VO legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Samenwerkingsverband Brabantse Wal VO voldoet hiermee aan de documentatieplicht.

6. Binnen Samenwerkingsverband Brabantse Wal VO is het veilig en betrouwbaar omgaan met 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. Samenwerkingsverband Brabantse Wal VO 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. Samenwerkingsverband Brabantse Wal VO 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. Samenwerkingsverband Brabantse Wal VO sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van het samenwerkingsverband, persoonsgegevens verwerken. Als voorbeeld kan genoemd worden het digitale administratiesysteem voor de verwerking van aanvragen van een toelaatbaarheidsverklaring. Dit geldt ook voor andere organisaties/systemen indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. Samenwerkingsverband Brabantse Wal VO 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. Samenwerkingsverband Brabantse Wal VO heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Samenwerkingsverband Brabantse Wal VO een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Samenwerkingsverband Brabantse Wal VO kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Samenwerkingsverband Brabantse Wal VO 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 Samenwerkingsverband Brabantse Wal VO aanvullende afspraken vast over de technische maatregelen.

14. Samenwerkingsverband Brabantse Wal VO zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en (indien nodig) melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

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.

Relevante wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- Burgerlijk wetboek (met name artikel 1:377c, recht op informatie niet met gezag belaste ouder).

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.

Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking van persoonsgegevens (art. 5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens, te weten:

1. **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.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

3. **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 (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: Samenwerkingsverband Brabantse Wal VO 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. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister. Het IBP-beleid van Samenweringsverband Brabantse Wal VO is in 2020 volop in ontwikkeling en zal steeds verder vormgegeven worden, onder meer door documenten en/in de bijlage te updaten zodra mogelijk/nodig.

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. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van Samenwerkingsverband Brabantse Wal VO, met het bestuur als eindverantwoordelijke, en de Functionaris voor Gegevensbescherming.

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. 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 de betrouwbaarheidsaspecten die van belang zijn.
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. Vanaf de start van nieuwe (ict-)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

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 datalekken. 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 incidentenregister.

Alle (beveiligings-)incidenten moeten gemeld worden via privacy@swvbrabantsewal.nl én telefonisch, dan wel schriftelijk. Wanneer de beleidsmedewerker(s) kwaliteitszorg of de directeur-bestuurder van het samenwerkingsverband voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze de Functionaris voor Gegevensbescherming een verzoek om de verzamelde informatie te bekijken. De Functionaris voor Gegevensbescherming beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door 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 Samenwerkingsverband Brabantse Wal VO 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 hierin actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

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 alle medewerkers hun verantwoordelijkheid nemen en elkaar aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij onder andere de aanstelling, tijdens functioneringsgesprekken, met een gedragscode en met periodieke bewustwordingscampagnes.
Voor toezicht op de naleving van de AVG vervult Samenwerkingsverband Brabantse Wal VO samen met de Functionaris voor Gegevensbescherming een belangrijke rol. De Functionaris voor Gegevensbescherming wordt aangesteld door Samenwerkingsverband Brabantse Wal VO, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De Functionaris voor Gegevensbescherming werkt via een door Samenwerkingsverband Brabantse Wal VO vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan het Samenwerkingsverband Brabantse Wal VO de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

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

Organisatie - Wie doet wat?

Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij het Samenwerkingsverband Brabantse Wal VO.

<u>Directeur-bestuurder</u>
Eindverantwoordelijk voor AVG-beleid, invulling, toezicht en naleving en stelt processen, richtlijnen en procedures IBP vast waaronder:

- Protocol beveiligingsincidenten en datalekken
- Incidentafhandeling (registreren en evalueren)
- Verwerkersovereenkomsten
- Informatie documentatie richting leerlingen, ouders / verzorgers
- Security awareness activiteiten
- Gedragscode ICT en internetgebruik
- Dataregister
- Privacyreglement.

<u>Functionaris voor Gegevensbescherming</u>

- Toezicht houden op bestaande en nieuwe (DPIA) verwerkingen van persoonsgegevens
- Controleren van het verwerkings- en incidentenregister en logbestanden
- Toezicht houden op naleving privacywetgeving
- Geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen, vaak op basis van actuele ontwikkelingen
- Jaarlijks afstemming met de beleidsmedewerker kwaliteitszorg / directeur-bestuurder en het opstellen van een verslag van werkzaamheden
- Analyse uitvoeren en risicoanalyse maken op afwijkingen. Vervolgens adviseren over te nemen maatregelen
- Classificeren gegevens en informatiesystemen waarop dit beleid van toepassing is
- Rapporteren naar directeur-bestuurder, bij incidenten en structureel periodiek
- Eerste aanspreekpunt, begeleiding en afhandeling bij datalek
- Overleg met (contactpersoon van) de Autoriteit Persoonsgegevens na overleg met de verwerkingsverantwoordelijke
- Het (laten) afhandelen van klachten inzake privacy.

Beleidsmedewerker(s) Kwaliteitszorg samenwerkingsverband met ondersteuning door secretariaat

- Voorbereiden en uitvoeren IBP-beleid
- Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers
- Incidentafhandeling (registreren en evalueren)
- Periodiek 'informatiebeveiliging' onder de aandacht te brengen in werkoverleggen, beoordelingen etc.
- Opstellen protocol beveiligingsincidenten en datalekken
- Voorbereiden en zorgdragen voor ondertekening verwerkersovereenkomsten door directeur-bestuurder
- Opstellen gedragscode ICT en internetgebruik
- Opstellen dataregisters en jaarlijks herbeoordelen
- Eerste contactpersoon voor de Functionaris voor Gegevensbescherming
- Rapporteren over voortgang doelstellingen IBP-beleid aan directeur-bestuurder / bestuur.

Medewerkers

- Houden zich aan de onderdelen zoals beschreven in de gedragscode
- Spreken elkaar aan op onvolkomenheden.

Bijlage: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal is vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten[1]:
Gedragscode d.d. *
Privacyreglement d.d. *
Privacy statement personeel en sollicitanten d.d. *
Privacy statement leerlingen en ouders d.d. *
Protocol datalekken d.d. *
Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming d.d.*
Register beveiligingsincidenten (jaarlijks door FG)

[1] Deze lijst zal aangevuld worden naarmate het IBP-beleid van Samenwerkingsverband Brabantse Wal VO verder vormgegeven wordt.