



**PRIVATY**

SECURITY EN BESCHERMING  
VAN PRIVACYGEGEVENS

# *Digitale veiligheid in een digitale samenleving*

## *Jaarverslag Informatiebeveiliging en Privacy*

SWV Passend Primair Onderwijs regio Leiden periode 2024





**PRIVATY**  
SECURITY EN BESCHERMING  
VAN PRIVACYGEGEVENS

# Voorwoord

Conform artikel 39 van de algemene verordening gegevensbescherming (AVG) informeren wij hierbij het bestuur, Raad van Toezicht en management over de ontwikkeling bij PPO met betrekking tot informatiebeveiliging en privacy (IBP).

Het doel van dit jaarverslag is het bestuur, RvT en management te informeren over uitgevoerde activiteiten, risico's en de status van compliance IBP. Hieruit voortgekomen aanbevelingen zijn ook beschreven. Hiermee wordt duidelijk welke prioriteiten er zijn welke door het bestuur en management meegenomen dienen te worden in het IBP activiteitenplan voor 2025.

Informatie is verzameld uit het Governance-Risk-Compliance (GRC) –systeem, overlegsituaties, correspondentie en overige gerealiseerde IBP maatregelen.

PowerPoint is gebruikt voor de presentatie vanwege de compacte en overzichtelijke weergave. Hierdoor komen kernpunten en aandachtgebieden beter tot zijn recht.

Na de Inhoudsopgave, volgt de Managementsamenvatting. Daarna wordt in de Inleiding beschreven hoe de verdere structuur van dit rapport is opgebouwd.



# Inhoudsopgave

1. Voorwoord
2. Inhoudsopgave
3. Managementsamenvatting
4. Inleiding
5. Maatschappelijke context
6. Ontwikkeling en status Volwassenheidsniveau IBP
7. Ontwikkeling en status van de Registers
8. Ontwikkeling en status Audits, DPIA & Bewustwording
9. Ontwikkeling Actiepunten
10. Conclusies
11. Aanbevelingen

## Bijlagen

1. Privacy en het verschil met Informatiebeveiliging
2. Volwassenheidsniveaus – Capability Maturity Model
3. Kaderbegrippen Informatiebeveiliging
4. Kaderbegrippen Privacy



# Managementsamenvatting

De introductie van het normenkader IBP FO heeft geleid tot meer druk en focus op het implementatietraject IBP. Het nieuwe normenkader eist soms nieuw beleid en aanscherping van bestaand beleid. Het aanwezige beleid welke 3 tot 6 jaar oud is zal merendeels toe zijn aan een review en een update naar de gewenste situatie.

Het IBP volwassenheidsniveau is door het nieuwe normenkader lager dan voorheen en staat nu op een 2.0. Een benchmark met het funderend onderwijs laat zien dat het volwassenheidsniveau bij PPO rond het gemiddelde niveau ligt.

Om door te groeien naar een volwassenheidsniveau 3 verdienen met name organisatorische maatregelen aandacht. Het formeel beleggen van proceseigenaarschap is niet alleen een voorwaarde voor een implementatietraject maar is ook noodzakelijk geworden vanuit de norm.

Eigenaarschap beleggen is essentieel, zodat bij het nemen van de verantwoordelijkheden ook taken kunnen worden uitgevoerd. Daardoor ontstaat overzicht en wordt coördinatie van het IBP beleid mogelijk. Door deze ontwikkelcyclus op te starten en te waarborgen kan het volwassenheidsniveau 3 worden behaald.

## Top 2 uitgevoerde actiepunten

- 1) Start VOG Kinderopvang voor alle medewerkers
- 2) Verdere invoering van MFA

## Top 3 risico's

- 1) Niet uitvoeren van DPIA's of interne audits blokkeren het verbeterproces en is er onvoldoende IBP waarborging welke leidt tot verhoogde kans op hacken en lekken.
- 2) Zonder een samenwerkingsovereenkomst met partijen lopen meerdere partijen het volle risico en de maximale aansprakelijkheid. Bedrijfscontinuïteit is dan niet gewaarborgd.
- 3) Eigenaarschap, taken en rollen t.a.v. IBP zijn nog onvoldoende aangebracht waardoor de realisatie van het volwassenheidsniveau 3 IBP FO per 2027 lastig wordt.



**PRIVATY**  
SECURITY EN BESCHERMING  
VAN PRIVACYGEGEVENS

# Inleiding

Waarom de digitale weerbaarheid aandacht behoeft wordt in het kort vermeld in de maatschappelijke context. Informatiebeveiliging is het fundament voor het beveiligen van uw bedrijfsinformatie en persoonsgegevens. Zo is de combinatie van informatiebeveiliging en privacy (IBP) onlosmakelijk aan elkaar verbonden.

Na de maatschappelijke context volgt een weergave over het volwassenheidsniveau van de organisatie, getoetst aan het normenkader IBP FO. We richten ons met name op de normen benoemd in Fase 1 van het groeipad. In 2027 moet het volledige normenkader IBP zijn geïmplementeerd met een volwassenheidsniveau 3.

In hst 7, 8 en 9 worden de ontwikkelingen en realisaties bij de organisatie van het afgelopen jaar getoond. Vanuit de huidige situatie worden conclusies en aanbevelingen beschreven in respectievelijk hst. 10 en 11.

In de bijlage worden IBP begrippen en definities uitgelegd en toegelicht.



# Maatschappelijke context 1/2

## *Digitale veiligheid in een digitale samenleving*

Overheid, lokale overheden, stichtingen, verenigingen, kortom alle organisaties lopen helaas nog achter op de 'gewenste digitale weerbaarheid'. Deze achterstand is zo opgelopen en *nijpend* geworden dat de centrale overheid, waaronder het Ministerie van OCW, maatregelen heeft genomen waaraan alle partijen zich dienen te houden. Deze maatregelen zijn ook door internationale- en Europese verordeningen ontstaan.

Privacy en gegevensbescherming zijn in een data en digitaal gedreven samenleving geen bijzaak meer, maar een essentieel onderdeel van het fundament van elke organisatie. Waarom? Omdat persoonsgegevens de ruggengraat vormen van veel bedrijfsprocessen. Ze zijn onmisbaar voor het behalen van organisatiedoelen, maar tegelijkertijd ook een grote verantwoordelijkheid. Het raakt direct de beleidsdoelen en het vertrouwen van alle stakeholders.

IBP volwassenheid ontstaat niet door enkel protocollen op te stellen of technische oplossingen te implementeren. Het vraagt om een sterke cultuur, duidelijk eigenaarschap, bewustwording en doelgericht leiderschap.



## Maatschappelijke context 2/2

Gegevensbescherming zou hoog op de agenda moeten staan, zowel door de maatschappelijke ontwikkelingen als door de gestelde eisen bij het ministerie van OCW. Toch wordt informatiebeveiliging en privacy in veel organisaties nog vaak gezien als een juridische verplichting of een technische uitdaging. Juist daar ligt een cruciale kans én verantwoordelijkheid voor het management.

**Incidenten zijn onvermijdelijk**, maar hoe een organisatie hierop reageert bepaalt of het een bedreiging blijft of een kans wordt. Het management speelt hierin een sleutelrol door eigenaarschap te tonen, bewustzijn te creëren en te sturen op concrete verbeteringen. Een up-to-date verwerkingsregister, een doordacht incidentmanagement en betrokken leiderschap vormen samen de fundering voor IBP volwassenheid.

**Informatiebeveiliging en Privacy is geen bijzaak**; het is een strategisch voordeel dat vertrouwen versterkt, processen verbetert en risico's beperkt. Dit vraagt om leiders / professionals die IBP niet alleen naleven, maar ook uitdragen als een kernwaarde binnen de organisatie.

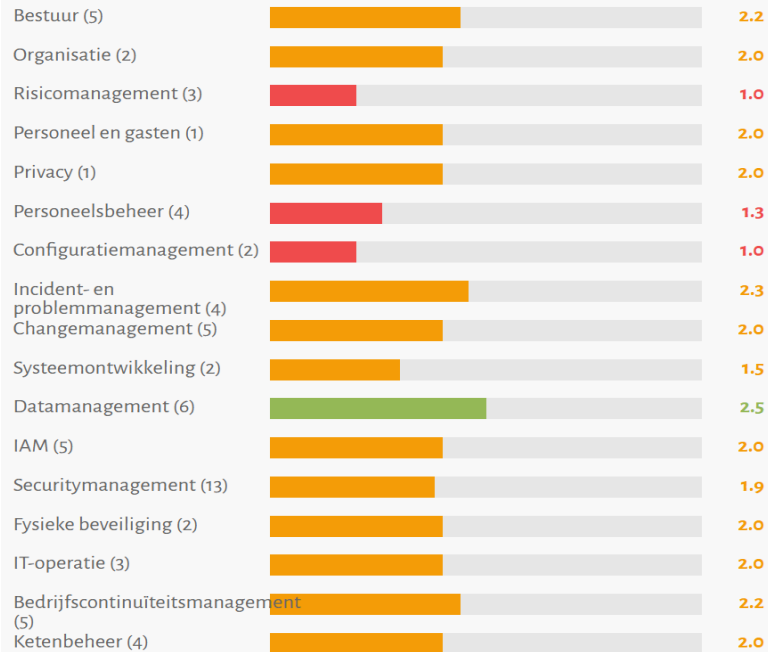


# Status volwassenheidsniveau IBP

## Normenkader Informatiebeveili...



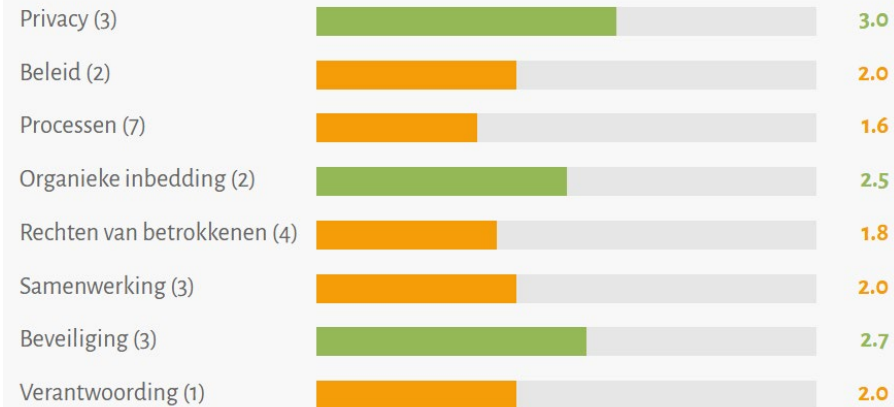
67 beheersmaatregelen binnen scope  
2 beheersmaatregelen buiten scope



## Normenkader Privacy



25 beheersmaatregelen binnen scope  
geen beheersmaatregelen buiten scope



Begin 2024 is de start geweest van het nieuwe normenkader IBP FO, geïnitieerd door Ministerie van OCW samen met PO-Raad en VO-raad.

Het doel voor de sector Funderend Onderwijs is dat iedere norm van toepassing uit het normenkader IBP FO op een volwassenheidsniveau 3 dient te staan in 2027. Om hier planmatig naar toe te werken is er door Kennisnet een Groeipad met 5 Fases opgesteld. PPO is in 2024 gestart met Fase 1.

Eind 2024 laat PPO een gemiddelde volwassenheidsniveau zien van 2.0 over het gehele normenkader IBP. Het merendeel van de normen hebben de status 2. Enkele normen staan nog in de statblokken met een 1 en een enkele norm staan op een 3.

Het normenkader, DPIA's, Risico's, Registers en taken worden geadmistreerd in PCC - Governance, Risk, Compliance (GRC)-applicatie. Toelichting op het volwassenheidsmodel en de niveaus, zie bijlage.



# Ontwikkeling en status van de Registers

## ❖ Register van verwerkingen

Meest belangrijke leveranciers en applicaties zijn opgenomen in het register. Er zijn leveranciers opgenomen in het register waarvan nog geen verwerkersovereenkomst is geregistreerd in het register.

Inzichtelijk bij alle bedrijfsmiddelen is dat de BIV-classificatie is aangegeven. De praktijk laat zien dat alle applicaties de hoogste classificatie hebben. Met andere woorden deze verwerkingen hebben een hoge mate van beveiliging nodig voor het waarborgen van de vertrouwelijkheid, waaronder een geactiveerde 2FA.

Het onderhouden en beheren van het register is essentieel om risico's inzichtelijk te maken om vervolgens mitigerende maatregelen te nemen, waar dit mogelijk is.

## ❖ Register van beveiligingsincidenten en datalekken

In 2024 zijn er geen beveiligingsincident geregistreerd.

## ❖ Register van verzoeken

Er zijn geen verzoeken of klachten ingediend in 2024.



# Ontwikkeling en status van Audits, DPIA's, Bewustwording

## ❖ Audit

Audits resulteren in het identificeren van bedreigingen op bepaalde processen en daarmee de bedrijfscontinuïteit. De organisatie dient eerst focus te hebben op het implementeren van het normenkader IBP FO. Wanneer het beleid is gecommuniceerd en taken worden uitgevoerd heeft een audit toegevoegde waarde. Er is geen audit uitgevoerd.

## ❖ DPIA's

Intern zijn er geen risicoanalyses, met betrekking tot informatiebeveiliging en privacy ofwel DPIA's, uitgevoerd. Privacy by design, het op voorhand nemen van noodzakelijke passende maatregelen om beveiliging en bescherming van Informatie en Persoonsgegevens naar huidige maatstaven te waarborgen, is een wettelijke plicht. DPIA's zijn hier onderdeel van. Denk hierbij aan processen die de organisatie wil wijzigen of wil voorzien van een nieuwe applicatie. Dit wordt in het normenkader Changemanagement en Risicomanagement genoemd. DPIA-plichtige verwerkingen zijn opgenomen in PCC. Het gebruik van AI is nog niet geïnventariseerd. Voor het gebruik van AI is een protocol noodzakelijk, met vermelding van doeleinde, wat de risico's zijn van AI en hoe daarmee om te gaan.

## ❖ Bewustwording

Meer dan 80% van hacken en lekken wordt veroorzaakt door menselijk handelen. Daardoor is het een verplichting om een voortdurend bewustwordingsprogramma voor alle medewerkers aan te bieden, inclusief IBP training bij onboarding. Er is nu onvoldoende sprake van aantoonbare voorziening van bewustwordingsactiviteiten.



# Ontwikkeling Actiepunten

## Gerealiseerde actiepunten

- ❖ Start aanvraag VOG Kinderopvang (doorlopende screening) voor medewerkers
- ❖ Controle op toegang op de juiste gebruikers voor de juiste applicaties

## Niet gerealiseerde actiepunten of zijn onderhanden

- ❖ Structureel en aantoonbare bewustwordingsactiviteiten voor alle medewerkers.
- ❖ IBP verantwoordelijkheden toewijzen aan proceseigenaren en het toewijzen aan uitvoerders.
- ❖ Waar nodig 2FA verder afdwingen voor applicaties waarbij de BIV classificatie HOOG is. HOOG impliceert dat op deze verwerkingen bedrijfskritische, gevoelige en bijzondere persoonsgegevens verwerkt worden.
- ❖ Hoofdstuk of paragraaf over IBP opnemen in het Schoolplan of Strategisch plan. Het betreft visie en strategie over IBP vertalen in het meerjarenplan van de organisatie. IBP is een onherroepelijk onderdeel geworden van de bedrijfsvoering, zoals personeelszaken, financiën, IT en maatschappelijke relevante ontwikkelingen dat ook zijn.
- ❖ Aantoonbare uitvoering van opschoning data en dataminimalisatie.



# Conclusies

- ❖ Goede ontwikkeling is de continue screening van een VOG.
- ❖ Het benoemen van proceseigenaren en uitvoerders van het IBP beleid, waaronder continue- en cyclische taken, is een voorwaarde om het implementatietraject IBP succesvol te kunnen laten verlopen. Dit wordt stelselmatig gevraagd als eis bij vele normen.  
Zonder deze benoeming en het consistent uitvoeren van cyclische taken, monitoring en handhaving kan de organisatie niet op het volwassenheidsniveau 3 geraken.
- ❖ Wanneer bewustwordingsactiviteiten onvoldoende is ingebed in de organisatie, vanaf onboarding inclusief training, aantoonbaarheid en registratie van behaalde certificaten, zal het volwassenheidsniveau achter blijven op de doelstelling.
- ❖ Het Register van verwerkingen is nog niet compleet, mede door het ontbreken van proceseigenaren en uitvoerders. De procesbeschrijvingen van de groepsverwerkingen zijn merendeel nog niet beoordeeld of aangepast.
- ❖ De BIV-classificatie (het beoordelen van gegevens op basis van *beschikbaarheid, integriteit en vertrouwelijkheid*) is volledig doorgevoerd bij alle bedrijfsmiddelen. Dit is nodig om het passende beveiligingsniveau te kunnen bepalen en beoordelen.



# Aanbevelingen

- ❖ Gebruik structureel het GRC-systeem (PCC) voor het creëren van inzicht, overzicht en het zorgen van de aantoonbaarheid van verantwoordelijkheden en uitvoering van essentiële taken.
- ❖ Benoem proceseigenaren, die verantwoordelijk zijn voor een proces of afdeling en daarmee ook voor het nakomen van het IBP beleid. Geef ook aan wie de uitvoerenden zijn, conform de tabel behorende bij norm OR.01.
- ❖ Betrek de FG 'preventief' bij wijzigingen van processen of een migratie bij aanschaf vervangend systeem/leverancier of een uit te voeren DPIA. Waarschijnlijk speelt IBP bij meer dan 80% van alle bedrijfsprocessen.
- ❖ Voor iedereen binnen PPO moet het duidelijk zijn welke route bewandeld moet worden bij een Changeproces. Zorg preventief voor een juiste aanpak bij het wijzigingen en het veilig in gebruik kunnen nemen van nieuwe applicaties, processen of verwerkingen. Alleen dan kan er tijdig, aan de voorkant, een risico assessment uitgevoerd worden, zodat er ook tijdig een no-go uitgesproken kan worden of dat er met de juiste mitigerende maatregelen er een goedkeuring kan komen.
- ❖ Stel een proceseigenaar aan en uitvoerder voor het register van verwerkingen, conform norm OR.01.  
Vanuit een up-to-date register van verwerkingen is controle en beheer mogelijk. Er is nu onvoldoende uitvoering van de verplicht gestelde risicoassessments (DPIA's), retentieperiode (data opschonen), leverancierscontrole en interne audits. Deze taken kunnen vanuit PCC vrij eenvoudig worden opgepakt, gepland en na uitvoering geregistreerd worden voor de aantoonbaarheid.



**PRIVATY**  
SECURITY EN BESCHERMING  
VAN PRIVACYGEGEVENS

# Bijlagen

## Toelichting op begrippen & kaders

1. Privacy en het verschil met Informatiebeveiliging
2. Volwassenheidsniveaus – Capability Maturity Model
3. Kaderbegrippen Informatiebeveiliging
4. Kaderbegrippen Privacy



# Privacy en Informatiebeveiliging

- ❖ Privacy: betreft een mensenrecht. Wetgeving stelt eisen aan het gebruik, het respecteren en nakomen van rechten van betrokkenen en de beveiliging en bescherming van *persoonsgegevens*.
- ❖ Informatiebeveiliging: het geheel aan maatregelen om betrouwbaarheid van (*bedrijfs-*)*informatie en processen* te waarborgen. Informatiebeveiliging wordt onderverdeeld naar 'beschikbaarheid, integriteit, vertrouwelijkheid' en het benodigd beveiligingsniveau wordt geduid naar LAAG-MIDDEN-HOOG per onderdeel. Onderstaande tabel is een indeling van een *BIV-classificatie*, welke in de GRC tool wordt gebruikt onder [Governance - Bedrijfsmiddelen].

Beschikbaarheid	Integriteit	Vertrouwelijkheid	Algeheel niveau
Niet nodig	Niet zeker	Openbaar	Laag
Belangrijk	Beschermd	Intern	Midden
Noodzakelijk	Hoog	Vertrouwelijk	Hoog
Essentieel	Absoluut	Geheim	Kritiek

- ❖ Privacy gaat ook om *andere waarborgen* voor het gebruik van persoonsgegevens dan alleen informatiebeveiliging. Een rechtmatige verwerking houdt in dat alleen de noodzakelijke persoonsgegevens verwerkt mogen worden voorzien van een duidelijk '*doeleinde en een grondslag*'. Toepassen van Privacy by design en het inrichten van een veilige en betrouwbare verwerking is een vereiste. Zo hebben alle persoonsgegevens binnen de organisatie een levenscyclus, er geldt altijd een retentieperiode.



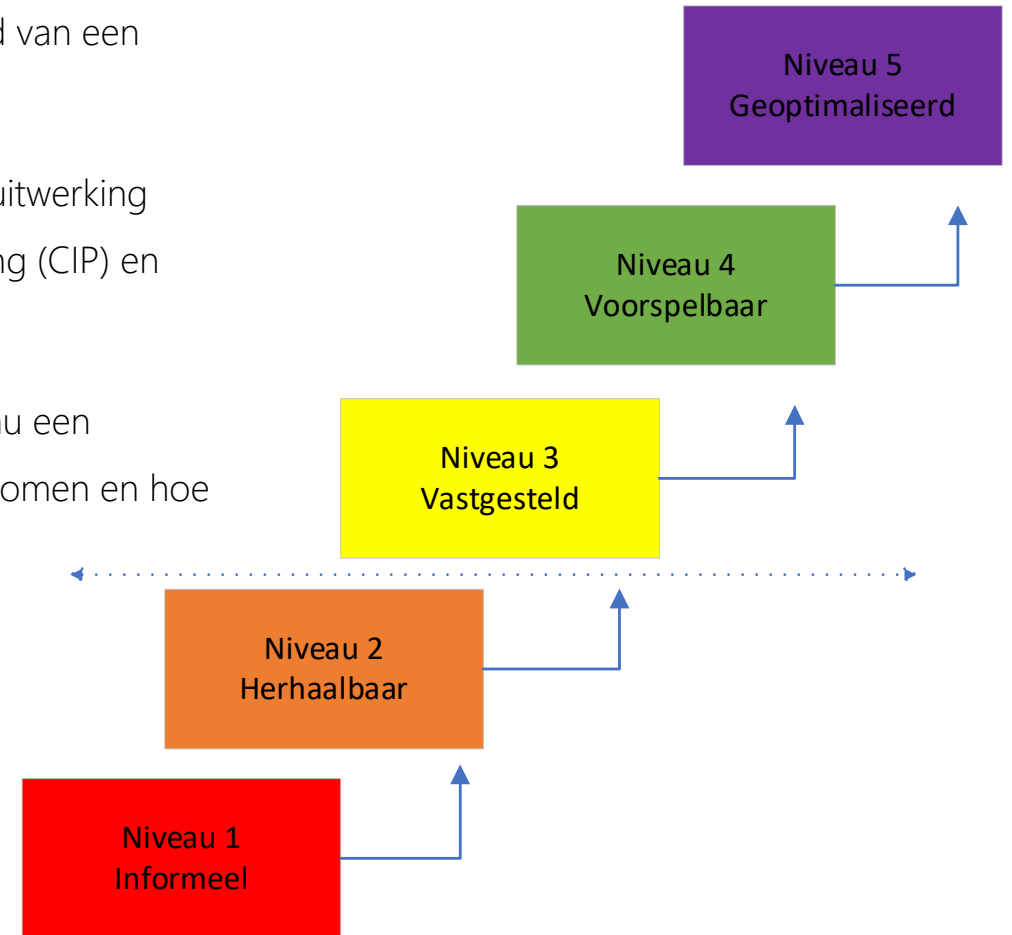
# Volwassenheidsniveaus 1/2

De volwassenheidsniveaus voor IBP zijn per onderdeel bepaald aan de hand van een vijfpuntsschaal, van 1 (informeel) tot 5 (geoptimaliseerd).

Deze vijfpuntsschaal is gebaseerd op het 'Capability Maturity Model' en de uitwerking daarvan door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) en Norea, de beroepsorganisatie voor IT-auditors.

De volwassenheidsniveaus zijn bedoeld om te kunnen bepalen op welk niveau een organisatie zich bevindt, bepaald op basis van hoe beslissingen worden genomen en hoe de processen daarvoor zijn vormgegeven. Het model is primair bedoeld als 'richtinggevend' om een organisatie te laten groeien in volwassenheid.

De AVG stelt dat maatregelen met betrekking tot informatiebeveiliging en privacybescherming aantoonbaar moeten zijn, dat geldt vanaf niveau 3.





## Volwassenheidsniveaus 2/2

Niveau	Beschrijving	Criteria
1	Initieel	<ul style="list-style-type: none"><li>• Niet of beperkt gedefinieerd en geïmplementeerd</li><li>• Informeel en inconsistentie, geen standaardisatie</li><li>• Uitvoering afhankelijk van individu</li></ul>
2	Herhaalbaar	<ul style="list-style-type: none"><li>• Grotendeels gedefinieerd</li><li>• Informeel en meer consistent en standaard</li><li>• Aantoonbaarheid beperkt</li></ul>
3	Vastgesteld / Gedefinieerd	<ul style="list-style-type: none"><li>• Volledig gedefinieerd en vastgesteld</li><li>• Formeel, aantoonbaar, consistent en standaard</li><li>• Verantwoordelijkheden en taken eenduidig toegewezen</li></ul>
4	Voorspelbaar / Beheerst en meetbaar / Gemanaged	<ul style="list-style-type: none"><li>• Volledig geïmplementeerd</li><li>• Periodieke control, evaluatie en opvolging (PDCA-cyclus)</li><li>• Risico-assessment en rapportage aan management</li></ul>
5	Geoptimaliseerd / Continu verbeteren	<ul style="list-style-type: none"><li>• Self-assessment, gap en oorzaak analyses</li><li>• Real time monitoring, continu evalueren</li><li>• Inzet automated tooling (GRC-system)</li></ul>



# Kaderbegrippen Informatiebeveiliging

Onderdeel	Beschrijving
Beleid	Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-) partners en er mede voor zorgt dat de kritieke bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.
Organisatie	Beheren van de informatiebeveiliging binnen de organisatie.
Objecten van beheer	Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.
Personele eisen	Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten waaronder informatie te verminderen.
Fysieke beveiliging	Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.
Beheersprocessen	Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.
Logische toegangsbeveiliging	Beheersen van de toegang tot informatie. Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang.
Ontwikkeling/aanschaf van systemen	Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.
Incidentmanagement	Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.
Continuïteitsmanagement	Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritieke bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
Naleving	Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.



# Kaderbegrippen Privacy 1/2

Onderdeel	Beschrijving
Beleid	Het beleid en de procedures worden op organisatieniveau eenduidig vastgesteld, formeel vastgesteld en organisatiebreed gebruikt. De juistheid en de eenduidigheid van de beleidsbeslissingen wordt in een procedure organisatiebreed formeel bewaakt. Ontwikkelingen in relevante wet- en regelgeving worden actief door de organisatie gevolgd, zodat de impact op het beleid bekend is voordat de wet- en regelgeving wordt vastgesteld. De kwaliteit (zoals actualiteit en bruikbaarheid) van het beleid en het beleidsproces is meetbaar en inzichtelijk op ieder niveau. Het hoogste management stuurt (waar nodig bij) op de kwaliteit van het beleid en de beleidsprocessen.
Organisatie	De rapportagelijnen worden organisatiebreed vastgelegd en formeel vastgesteld. Ontwikkelingen in relevante wet- en regelgeving worden actief door de organisatie gevolgd, zodat de impact op de organisatie en de benodigde middelen tijdig bekend is. Relevante externe ontwikkelingen worden direct verwerkt in de organisatorische inrichting van de organisatie. Het hoogste management wordt geïnformeerd over de effectiviteit en efficiëntie van de organieke inbedding en stuurt (waar nodig) bij.
Risicomanagement, Privacy by Design en de GEB	De opzet van de GEB-en wordt organisatiebreed op elkaar afgestemd en gestandaardiseerd. Het toepassen van Privacy by Design in de ontwerpstappen wordt organisatiebreed op elkaar afgestemd en gestandaardiseerd. De GEB wordt onderdeel van een formeel vastgestelde risicomanagement aanpak. De plannen voor het mitigeren van de risico's worden meegenomen in de plan- en control-cyclus van de organisatie. Het hoogste management wordt geïnformeerd over het effect van de risico's op de bedrijfsvoering en stuurt (waar nodig) bij.
Doelbinding gegevensverwerking	Alle doeleinden, rechtvaardigingsgronden en afwegingen worden, welbepaald en uitdrukkelijk omschreven en op één plaats vastgelegd, zodat de rechtvaardigingsgronden eenvoudig en tijdig aantoonbaar zijn. Organiseatiebreed wordt bewaakt en afgedwongen dat er dataminimalisatie wordt toegepast. Het hoogste management wordt geïnformeerd over de doeleneinden en de gehanteerde rechtvaardigheidsgronden en stuurt (waar nodig) bij.
Verwerkingsregister	De vastgelegde informatie geeft inzicht in de complete samenhang tussen de gegevens, verwerkingen, processen, organisatie en technische systemen. De vastgelegde informatie wordt meegenomen in de beslissingen om te komen tot veranderingen in de gegevensverwerking. De compleetheid en kwaliteit (zoals actualiteit en bruikbaarheid) van vastgelegde informatie is meetbaar en inzichtelijk. Het hoogste management zet de vastgelegde informatie over de verwerkingen in bij de beslissingen om privacy te borgen in de gegevensstrategie van de organisatie.
Kwaliteitsmanagement	De mogelijkheden persoonsgegevens te (laten) corrigeren en overgedragen te krijgen worden meegenomen in de Privacy by Design processen. Door het inzetten van deze mogelijkheden en de juistheid van persoonsgegevens te bewaken, stuurt het hoogste management op het leveren van klantvriendelijke diensten.
Beveiligen van de verwerking van persoonsgegevens	Er wordt een informatiebeveiligingsmanagementsysteem (ISMS) ingezet, dat onderdeel wordt gemaakt van de plan- en control-cyclus van de organisatie. (Potentiële) inbreuken worden gemonitord en ontwikkelingen omtrent de beschouwing van risico's en passende maatregelen gevolgd en gedeeld. Het hoogste management wordt door middel van prestatie-indicatoren en een dashboard geïnformeerd over de effectiviteit van de informatiebeveiliging en stuurt (waar nodig) bij.



# Kaderbegrippen Privacy 2/2

Onderdeel	Beschrijving
Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	Bij het opstellen van de informatie wordt rekening gehouden met het gebruik in de branche. De klanttevredenheid wordt gemeten en gebruikt om desgewenst bij te sturen. Het informeren van de betrokkenen maakt integraal onderdeel uit van de organisatiebrede communicatiestrategie voor het informeren van klanten/betrokkenen over de dienstverlening. De verstrekte informatie bij de verzameling van persoonsgegevens wordt consequent en actueel in lijn gehouden met de doelstellingen van de organisatie.
Bewaren van persoonsgegevens	Bij het bepalen van de bewaartermijnen wordt gekeken naar het gebruik binnen de branche. Bij het bepalen van de wijze van vernietigen wordt gekeken naar het gebruik binnen de branche. Het tijdig en gecontroleerd vernietigen van persoonsgegevens en de doelstelling waarvoor de opslag plaatsvindt wordt meegenomen in het ontwerp van de verwerking. De bewaartermijnen worden aantoonbaar in lijn gebracht met de privacydoelstellingen van de organisatie.
Doorgifte persoonsgegevens	Er wordt blijvend bewaakt of de doorgiften aan de vereisten voldoen. Voor het maken van de onderlinge afspraken en de afdoende garanties wordt de kennis en ervaring van de branche benut. Of de doorgiften aan de vereisten voldoen wordt meetbaar gemaakt. De organisatie evalueert op periodieke basis of de doorgiften en de gedeelde gegevens noodzakelijk zijn voor de bedrijfsvoering, of ze passen in de outsourcingstrategie en of de gehanteerde vereisten adequaat zijn.
Intern toezicht	Bij het rapporteren over en het aantonen van de rechtmatigheid wordt gekeken naar het gebruik in de branche. Bewaking van de rechtmatigheid wordt integraal onderdeel gemaakt van de managementprocessen. Het effectief mogelijk maken van toezicht wordt meegenomen in het ontwerp van de gegevensverwerking. Er wordt een FG aangesteld. Het hoogste management stuurt op het inzetten van toezicht als instrument voor het leveren van klantvriendelijke diensten door de organisatie. De FG heeft door middel van een dashboard een actueel beeld van de rechtmatigheid van de verwerkingen. De mate van compliancy en de ambities daarin worden meegenomen in zijn of haar externe uitingen.
Toegang gegevensverwerking voor betrokkenen	De organisatie stelt richtlijnen op om de efficiëntie van de toegang te waarborgen. Bij het bepalen van de wijze van toegang wordt door een FG rekening gehouden met het gebruik binnen de branche. Organisationsbreed vindt bewaking van de wijze van toegang plaats, bijvoorbeeld door het mee te nemen in de architectuurprocessen. De FG krijgt door middel van een dashboard een actueel beeld van de aangevraagde en verleende toegangen of de rechtmatigheid van de verwerkingen. Het hoogste management stuurt op klantvriendelijke diensten door het bieden van toegang, waarmee de betrokkene zijn rechten kan uitoefenen.
Meldplicht datalekken	De processen volgens welke datalekken moeten worden gemeld, zijn vastgelegd en zijn integraal onderdeel van het informatiebeveiligings-managementsysteem (ISMS). (Potentiele) inbreuken op de gegevensverwerking worden gemonitord, zodat datalekken worden voorkomen. Kennis omtrent de behandeling en preventie van datalekken wordt ook buiten de eigen organisatie gevolgd en gedeeld. De effectiviteit van de behandeling en preventie van datalekken wordt door middel van prestatie-indicatoren bewaakt en gebruikt om te sturen op uitvoerings-/afdelingsniveau. Het voorkomen en kunnen signaleren van datalekken maakt onderdeel uit van het ontwerpproces/Privacy by Design. Het hoogste management wordt door middel van prestatie-indicatoren en een dashboard geïnformeerd over de effectiviteit van de behandeling en preventie van datalekken en stuurt (waar nodig) bij. Het hoger management is in staat desgewenst bij te sturen, doordat prestatie-indicatoren en een dashboard over het voorkomen en omgaan met datalekken worden gehanteerd.