zone college

# Informatiebeveiligings- en privacybeleid

Stichting Groen Onderwijs Oost Nederland

## Inhoudsopgave

## Verantwoording en richtlijnen

### Het belang van informatiebeveiliging en privacy

Het onderwijs 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, met name ook van minderjarigen[1]. 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

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 volledig, juist en actueel zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, boetes 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*[2].

### Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens

[1] Oranje woorden worden in bijlage 1 (Verklarende woordenlijst) toegelicht

[2] Artikel 4, lid 2 van de AVG.

noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één geheel: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen Zone.college te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

**Doel**
Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie Zone.college persoonsgegevens verwerkt, te weten: medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing).
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (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 wordt gerespecteerd en Zone.college voldoet aan relevante wet- en regelgeving.

**Reikwijdte**

- Het IBP-beleid binnen Zone.college geldt voor alle betrokkenen.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Zone.college. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken (b.v. uitspraken van medewerkers en studenten in discussies, op (persoonlijke pagina's van) websites en of sociale media). Onder dit beleid vallen ook alle apparaten van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk geautomatiseerde en systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Zone.college 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 Zone.college raakvlakken met:
    - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
    - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
    - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen.
    - *Medezeggenschap* van studenten, hun ouders/verzorgers en

medewerkers.

**Concretisering**

Zone.college hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het **College van Bestuur** van Zone.college 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. Zone.college voldoet aan alle **relevante wet- en regelgeving**.
3. Bij Zone.college 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 Zone.college om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming in- en herzien.
4. Zone.college 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, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens.
5. Zone.college legt alle **verwerkingen van persoonsgegevens** vast in een dataregister en zal dit register up-to-date houden. Zone.college voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.
6. Binnen Zone.college is het **veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder**. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. Zone.college is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het **eigendom** (auteursrecht) **toebehoort aan derden**. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Zone.college **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. Zone.college sluit met **alle leveranciers van digitale onderwijsmiddelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.
10. Zone.college verwacht van alle **medewerkers, studenten, (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. Zone.college heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. **Informatiebeveiliging en privacy is bij Zone.college een continu kwaliteitsproces**, waarbij regelmatig (minimaal jaarlijks) wordt ge-audit of een self assessment wordt uitgevoerd en wordt gekeken of een aanpassing gewenst dan wel noodzakelijk is.
12. Zone.college kijkt bij **wijzigingen** (denk ook aan uitfasering) 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. Zone.college neemt **passende organisatorische of 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.
14. Zone.college zal alle **beveiligingsincidenten en** datalekken vastleggen, volgens een vast protocol afhandelen en indien nodig melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.
15. Zone.college kiest ten aanzien van informatiebeveiliging (**autorisatie en authenticatie**) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten" in plaats van de zwakkere regel "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

## Compliance

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 Educatie en Beroepsvorming (WEB)
- Branche code Goed Bestuur MBO, MBO Raad
- Wet Inspectietoezicht
- Algemene Verordening Gegevensbescherming (AVG en uAVG)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

Het internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen. Zone.college hanteert het Toetsingskader Informatiebeveiliging en Privacy dat ontwikkeld is door saMBO-ICT, Kennisnet en SURF onder verantwoordelijkheid van de regiegroep IBP in het mbo.

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

- *Doelbepaling en doelbinding*: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
- *Grondslag*: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
- *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 (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
- *Transparantie*: de school legt aan betrokkenen (studenten, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
- *Data-integriteit*: er zijn maatregelen getroffen om te waarborgen dat de te

verwerken persoonsgegevens volledig, juist en actueel zijn.

**Ondersteunende richtlijnen en procedures**
Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

**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 de verantwoordelijke IBP-manager, de FG, en/of de Security- en Privacy Officer(s) met het College van Bestuur als eindverantwoordelijke.

**Classificatie en risicoanalyse**
Alle gegevens en informatiesystemen waarop dit beleid van toepassing is worden 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 kwaliteitscriteria 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. Hiervoor worden DPIA's uitgevoerd (Data Protection Impact Assessment; gegevensbeschermingseffectboordeling). 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. 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 kunnen worden gemeld bij een door Zone.college bepaald contactpunt.

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

Ook aan studenten en externen is gecommuniceerd op welke manier zij kwetsbaarheden en incidenten dienen te melden.

**Planning en controle**
Dit IBP-beleid wordt jaarlijks gereviewed en eventueel bijgesteld door het College van 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 Zone.college een jaarlijks verbeterplan voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Eén en ander leidt tot een jaarplan IBP.

**Naleving en sancties**
De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Naleving van ons IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen Zone.college. Daarboven nemen de leidinggevenden en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP-zaken bij de aanstelling, tijdens functioneringsgesprekken, d.m.v. een instelling brede gedragscode, d.m.v. periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

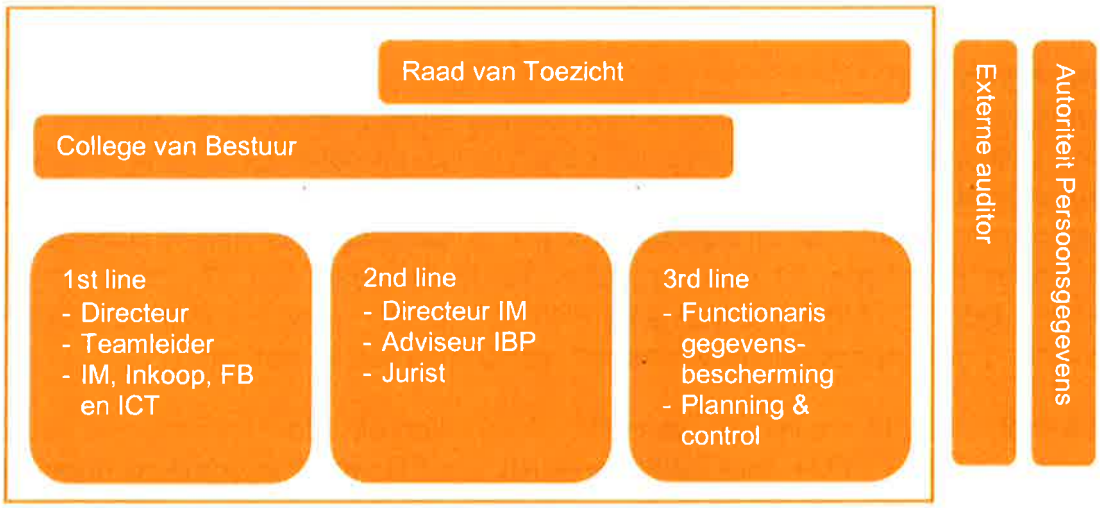
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Zone.college de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

**Logging en monitoring**
Door middel van logging en monitoring worden gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (pogingen tot) ongeautoriseerde toegang tot het netwerk. Zone.college beoordeelt deze logbestanden met regelmaat.

## Governance

**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. Voor een optimaal IBP-beleid moet dit goed ingeregeld zijn, de governance moet op orde zijn.

Zone.college hanteert hierbij (bijvoorbeeld) het 'three lines of defense'-model. De eerste lijn binnen dit model is cruciaal, immers de directeuren en teamleiders moeten erop toezien dat de AVG wordt nageleefd. Daartoe zijn alle leidinggevenden geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld IBP-beleid. Schematisch als volgt weergegeven.




**De first line of defense: directeur, teamleider, Informatiemanagement (IM), Inkoop, Facilitair bedrijf (FB), ICT**
De eerste lijn bewaakt het privacybeleid binnen het eigen organisatorische onderdeel (bijvoorbeeld het onderwijs). Directeuren, teamleiders, IM, Inkoop, FB en ICT vormen de first line of defense als het gaat om de bescherming van persoonsgegevens. Directeuren, teamleiders, IM, Inkoop, FB en ICT voeren de daarbij horende operationele taken uit, zoals:

- toetsen dat geen andere verwerkingen plaatsvinden als vastgelegd in de dataregisters voor studenten, medewerkers en relaties,
- toetsen dat er geen gegevens door externe verwerkers worden verwerkt of aan externe partijen worden overgedragen zonder een wettelijke grondslag dan wel een geldige overeenkomst (verwerkersovereenkomst of een gezamenlijk verantwoordelijkenovereenkomst),
- beoordelen van incidenten rond persoonsgegevens en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek.

Directeuren en teamleiders voeren bovendien de volgende operationele taken uit:

- toetsen dat hun medewerkers voldoende geschoold zijn in het kader van de AVG,
- vastleggen van de extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen.

**De second line of defense: IBP-organisatie van Zone.college**
Experts op het gebied van informatiebeveiliging en privacybescherming monitoren de toepassing en naleving van het informatiebeveiligings- en privacybeleid. Zij adviseren, gevraagd en ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunen de first line, bijvoorbeeld bij het afsluiten van overeenkomsten met derde partijen

De IBP-organisatie ontwikkelt beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit voorgenomen beleid vast. De medewerkers van de IBP-organisatie (IBP-manager, Security Officer of Privacy Officer) vormen daarmee de second line of defense als het gaat om de bescherming van persoonsgegevens.

**De third line of defense: de FG en de (interne) auditfunctie**

a) De Functionaris voor gegevensbescherming

- Zone.college heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld: de functionaris voor de gegevensbescherming (hierna: "FG"). De FG zal door Zone.college tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen Zone.college. Zone.college heeft de FG aangemeld bij de nationale toezichthoudende autoriteit, de Autoriteit Persoonsgegevens.
- De taken van de FG houden in:
    - het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG,
    - het toezien op de naleving van de AVG en andere relevante privacywetgeving,
    - het toezien op de naleving van dit privacy beleid door Zone.college,
    - het toezien op de inzet en uitvoering van Data Protection Impact Assessments,
    - het behandelen van klachten over de toepassing van het privacyreglement,
    - fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) (Interne) audit

- Op basis van het Toetsingskader IB (en daarmee de ISO27001 norm), aangevuld met de plusclusters 7 (privacy) en 8 (examinering), vindt minimaal jaarlijks een interne beoordeling plaats door middel van een self-assessment, peer-review en/of interne audit. Ook kunnen externe controles worden uitgevoerd door onafhankelijke accountants.

**De taken van de medewerkers**
(❶, ❷, ❸, ❹ en ❺ zijn volgordelijke stappen):

| | 1st line of defence | 2nd line of defence | 3rd line of defence |
|---|---|---|---|
| **Autorisaties** | Management[3] brengt autorisaties in kaart (SOLL) en toetst dit bij de Functioneel beheerders (IST). ❶ (stap 1) | De IBP-organisatie controleert of het SOLL en IST autorisatie vergelijk is uitgevoerd. ❷ (stap 2) | De FG controleert of de autorisaties zijn ingericht op basis van *need-to-know* en *least privilege*. ❸ (stap 3) |
| **Beleids-documenten** | Directeur, teamleider, IM, Inkoop, FB en ICT zien er op toe dat de goedgekeurde kaders en richtlijnen uit de beleidsdocumenten worden uitgevoerd. ❷ | De IBP-organisatie schrijft en evalueert de beleidsdocumenten en bespreekt deze met alle stakeholders en de FG'er en dient ze in bij het CvB ter goedkeuring. ❶ | De FG toetst de kwaliteit van het beleid en de werking van het door het CvB goedgekeurde beleid. ❸ |
| **Bewaartermijn** | Directeur, teamleider en FB zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP). ❶ | De IBP-organisatie adviseert aan de hand van de het Documentair StructuurPlan (DSP) de 1st line over de geldende bewaartermijnen. ❷ | De FG ziet er op toe dat de bewaartermijnen worden nageleefd. ❸ |
| **Bewustwording** | Management voert het opleidingsplan van de stafdienst Informatiemanagement uit of stelt een afgeleid opleidingsplan vast. ❶ | De IBP-organisatie stelt een opleidingsplan op voor IBP-scholings- en awareness plannen en faciliteert ook centrale trainingen. ❷ | De FG toetst het gewenste kennisniveau aan de scholings- en awareness plannen en komt eventueel met aanbevelingen. ❸ |
| **DPIA's** | Directeur, teamleider, IM, Inkoop, FB, ICT en projectleiders voeren een pré DPIA uit bij ieder nieuw ICT project. ❶<br>Directeur, teamleider, IM, FB, ICT en projectleider voeren een DPIA uit op in opdracht van de FG. ❹ | De IBP-organisatie komt op basis van de pré DPIA, uitgevoerd door de 1st line, tot een voorstel om al dan niet een DPIA uit te voeren en wordt betrokken bij de uitvoering van de DPIA. ❷ | De FG besluit op basis van het voorstel van de stafdienst Informatiemanagement of er een DPIA moet worden uitgevoerd en adviseert gevraagd of ongevraagd over de DPIA. ❸<br>De DPIA wordt slechts vastgesteld na goedkeuring van de FG. ❻ |
| **Datalekken** | Medewerkers melden zelf intern een datalek via een registratiesysteem. Het management draagt zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers. ❶ | De FG informeert de IBP-organisatie over de gemelde datalekken. ❸ | De FG besluit, na overleg met het CvB, om al dan niet het datalek bij de AP en/of de betrokkenen te melden. ❷ |
| **Dataregisters centraal** | De aangewezen verantwoordelijke directeuren (broneigenaren) voor de Dataregisters bewaken de actualiteit van het dataregister. ❶ | De IBP-organisatie adviseert en controleert op volledigheid, juistheid en actualiteit van de Dataregisters. ❷ | De FG toetst of het dataregister voldoet aan wet- en regelgeving. ❸ |
| **Door het management aangewezen uitvoerders** | Het management wijst de deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.). ❶ | De IBP-organisatie toetst het toegewezen eigenaarschap aan de autorisatie. ❷ | De FG toetst of het eigenaarschap beschreven is. ❸ |
| **Rechten van de betrokkenen** | Het management ontvangt het verzoek van de FG en neemt deze in behandeling (controle door afdeling Studentzaken of afdeling Personele Zaken). ❷ | De FG informeert de IBP-organisatie over het aantal verzoeken. ❸ | De FG is het eerste aanspreekpunt en volgt de vastgestelde procedure. ❶ |
| **Verwerkers-overeenkomsten** | De betrokken directeur, teamleider, Inkoop, FB en ICT zorgt dat er altijd een verwerkersovereenkomst is opgesteld en kan de IBP-organisatie hiervoor advies vragen. De directeur, teamleider, Inkoop, FB en ICT stuurt de verwerkersovereenkomst ter goedkeuring aan de FG. ❶ | De IBP-organisatie adviseert bij verwerkersovereenkomsten op verzoek van de first line. ❷ | De FG toetst de verwerkersovereenkomst op rechtmatigheid en volledigheid. Het College van Bestuur tekent na akkoord van de FG. ❸ |
| **Vragen van medewerkers betreffende IBP gerelateerde onderwerpen** | Het management is het eerste aanspreekpunt voor vragen inzake privacy en security, medewerkers kunnen de IBP-organisatie ook zelf benaderen. ❶ | De IBP-organisatie adviseert de manager en/of medewerker. ❷ | De FG controleert de gestelde vragen en de oplossingen. ❸ |

[3] Met management worden directeuren en teamleiders bedoeld.

**Implementatie beleid**
Het College van Bestuur is verantwoordelijk voor de verwerkingen van persoonsgegevens binnen Zone.college. Het College van Bestuur wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de wet AVG. De verantwoordelijkheid houdt kort samengevat in:

- dat de persoonsgegevens verwerkt worden in overeenstemming met de vastgestelde doelen van de verwerking, dat die doelen gerechtvaardigd zijn en dat de verwerking zorgvuldig gebeurt,
- dat hierover verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van Zone.college uitgevoerd. Het is niet één instituut of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die Zone.college verwerkt. Er is een onderscheid tussen centrale verwerkingen, waarvoor de stafdiensten verantwoordelijk zijn en aanvullend daarop, decentrale verwerkingen, waarvoor het onderwijsteam of dienst zelf verantwoordelijk is.

**Verdeling van de verantwoordelijkheden**
Zone.college onderscheidt een viertal soorten verwerkingen van persoonsgegevens met daarbij benoemde broneigenaren:

- De studentenadministratie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen die bij Zone.college onderwijs volgen. De studentenadministratie is verantwoordelijk voor het Dataregister met studentgegevens,
- De personeelsadministratie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen die in opdracht van Zone.college, zowel centraal als decentraal, werk verrichten. De personeelsadministratie is verantwoordelijk voor het Dataregister van medewerkers,
- De dienst Marketing en Communicatie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen waarmee Zone.college centraal een relatie onderhoudt, zoals belangstellenden, oud-werknemers, contactpersonen van de stage verlenende organisaties en leveranciers, prospects en alumni. Deze dienst is verantwoordelijk voor het dataregister van deze relaties,
- De dienst Financiën is verantwoordelijk voor de verwerking van alle persoonsgegevens van debiteuren en crediteuren,
- De opdrachtgever van onderzoek (broneigenaar) dat Zone.college uitvoert, zowel centraal als decentraal, is verantwoordelijk voor de verwerkingen van persoonsgegevens in het kader van dat onderzoek. Een onderzoeksvoorstel wordt altijd voorgelegd aan de IBP-organisatie en getoetst door de FG.

Er worden geen persoonsgegevens verwerkt buiten de verantwoordelijkheid van een van bovengenoemde broneigenaren, tenzij dit met toestemming van de FG gebeurt. De FG bepaalt op welke manier deze verwerkingen worden gedocumenteerd.

**Inpassing in de instellingsgovernance en afstemming met aanpalende beleidsterreinen**
Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp informatiebeveiliging en privacy op verschillende niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt voorbereid door de stafdienst Informatiemanagement.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld door de IBP-organisatie.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door diverse rollen: directeur, teamleider, IM, Inkoop, FB en ICT, zowel op centraal als decentraal niveau.

**Bewustwording en training**
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om het bewustzijn voortdurend aan te scherpen, zodat bij Zone.college de bewustwording van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn trainingen voor medewerkers en regelmatig terugkerende bewustwordingscampagnes gericht op medewerkers, studenten en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door het de IBP-organisatie.

**Controle en naleving**
Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de 2nd line en de interne auditfunctie de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Deze externe controles worden gepland en geformuleerd in een nauwe samenspraak met de interne auditfunctie van Zone.college.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten Zone.college maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

## Bijlage 1: Verklarende woordenlijst

| | |
|---|---|
| AVG | Algemene Verordening Gegevensbescherming. |
| Beleid | Beleid met betrekking tot het verwerken van persoonsgegevens door Zone.college. |
| Betrokkene | Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft. |
| Broneigenaar | Aangewezen directeur die verantwoordelijk is voor persoonsgegevens van één of meerdere categorieën van Betrokkenen. De Broneigenaar voert de persoonsgegevens in en zorgt voor de vernietiging. In de tussentijd leent hij ze uit aan de organisatorische eenheden binnen Zone.college. De organisatorische eenheden mogen dan de persoonsgegevens verrijken. |
| Datalek | Een inbreuk in verband met persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke inbreuken onder. |
| Dataportabiliteit | Het recht om persoonsgegevens en informatie over te dragen aan een nieuwe verwerker zonder technische problemen. |
| Dataregister | De AVG spreekt van het Register van Verwerkingsactiviteiten, dit is een overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag daarvoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens. Zone.college heeft drie centrale registers: dat voor studentgegevens, voor medewerker gegevens en voor relatiegegevens. Het dataregister is het Register van Verwerkingsactiviteiten aangevuld met de BIV-classificatie en de autorisatie matrix op hoofdlijnen. |
| DPIA | Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment. |
| Functionaris voor Gegevensbescherming | Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG. |
| Minderjarigen | Voor de AVG geldt iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt uiteraard jonger als 18 jaar. |

| | |
|---|---|
| Niet-geautomatiseerde verwerking | Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), et cetera. |
| Persoonsgegeven | Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon. |
| Privacy by Default | Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt. |
| Privacy by Design | Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. |
| Verwerker | Een door Zone.college ingeschakelde (derde) partij die ten behoeve van Zone.college, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt, e.e.a. vastgelegd in een verwerkersovereenkomst. |
| Verwerking | Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens. |
| Verwerkingsverantwoordelijke | College van Bestuur van Zone.college dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt. |