



Grotius College

Privacybeleid

Bewerkt door:

Privaty B.V.

Versie	Status	Datum	Auteur	Omschrijving
1.0	Gereed	April 2019	R. van Son	

Vastgesteld door Grotius College

Versie	Datum	Naam	Functie
1.0	April 2019	Dhr. W.A. van den Bosch MBA	Directie-bestuurder

Inhoud

1	Inleiding	5
2	Beginselen verwerken van persoonsgegevens	6
3	Rechtmatigheid van verwerkingen	6
3.1	Grondslagen	6
3.2	Toestemming.....	7
3.3	Vrijelijke toestemming	7
3.4	Het verwerken van bijzondere persoonsgegevens.....	7
4	Transparantie van de verwerkingen.....	7
4.1	Algemene openheid van zaken.....	7
4.2	Reageren op verzoeken.....	8
4.3	Kosten	8
4.4	Het verzamelen van persoonsgegevens bij de betrokkene	8
4.5	Het verzamelen van persoonsgegevens bij anderen dan de betrokkene (n)	8
5	De rechten van betrokkenen	9
5.1	Informatieplicht	9
5.2	Recht op overdraagbaarheid	9
5.3	Recht op bezwaar.....	9
6	Verantwoordelijkheid passende maatregelen	9
7	Privacy by design en Privacy by default	10
8	Schriftelijke afspraken met derden.....	10
9	Verwerkersovereenkomsten	11
10	Het verwerkingsregister.....	11
10.1	Het opstellen van een register.....	11
10.2	Verwerkersregister	11
10.3	Samenwerking met de AP.....	11
11	Passende waarborgen gegevensbescherming.....	12
11.1	Organisatorische en technologische maatregelen.....	12
11.2	Risico's minimaliseren	12
11.3	Meldplicht datalekken	12
11.4	De uitvoerig van een DPIA bij gevoelige gegevens.....	12
12	De rol van de Functionaris Gegevensbescherming	13
12.1	Aanstellen FG.....	13
12.2	Onafhankelijke positie FG	13
12.3	Wettelijke taken van een FG (art. 39 AVG)	13

13	Aantoonbare naleving.....	13
13.1	Uitwerking in procedures.....	13
13.2	Voorlichting en bewustzijn.....	13
13.3	Planning en controle.....	14
13.4	Naleving en sancties.....	14

1 Inleiding

Dit is het privacybeleid van Grotius College. Dit document heeft betrekking op het verwerken van persoonsgegevens in het kader van het verlenen van onderwijs en de (interne) bedrijfsvoering van Grotius College.

De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door ontwikkelingen op het gebied van ICT en digitalisering. 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.

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.

Grotius College is als onderwijsorganisatie verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming. Dit is zo omdat Grotius College het doel en de middelen bepaalt voor de verwerking van de persoonsgegevens die zij ontvangt. Dit privacybeleid beschrijft de wijze waarop Grotius College als verwerkingsverantwoordelijke met persoonsgegevens omgaat. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd in dit beleid. De uitgangspunten van dit beleidsdocument zijn verder uitgewerkt in procedés en interne gedragscodes zodat aan de vereisten van de Algemene verordening gegevensbescherming ('AVG') en alle relevante wetgeving wordt voldaan, waaronder:

- Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Reikwijdte en doel van dit privacybeleid

Het privacybeleid van Grotius College geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (in-huur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk van Grotius College verkregen kan worden. Dit beleid heeft betrekking op alle verwerkingen van persoonsgegevens binnen Grotius College. Hetzelfde geldt voor

verwerkingen die worden gedaan in toepassingen die vallen onder de verantwoordelijkheid van Grotius College en op verwerkingen die worden gemaakt en bestemd zijn om aan die toepassingen te worden toegevoegd.

De volgende doelen dienen met de uitvoering van dit beleid te worden bereikt:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Grotius College persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

2 Beginselen verwerken van persoonsgegevens

Het verwerken van persoonsgegevens door Grotius College gebeurt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Met andere woorden: de verwerking moet voldoen aan de wet en bekend zijn bij de betrokkenen. Daarom verwerken wij persoonsgegevens alleen als sprake is van:

- vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en die persoonsgegevens mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze verwerkt worden;
- een minimale gegevensverwerking: Grotius College en haar medewerkers werken alleen met persoonsgegevens die noodzakelijk zijn om de vooraf bepaalde doelen te dienen;
- Grotius College stelt alles in het werk om er voor te zorgen dat alleen actuele en juiste persoonsgegevens verwerkt worden, gegevens die onjuist zijn of niet langer nodig zijn om te worden gebruikt door Grotius College zullen gerectificeerd of verwijderd worden;
- een verwerking die transparant is: de verwerking heeft duidelijke en specifieke doelen en deze zijn op een begrijpelijke, tijdige en ondubbelzinnige wijze bekend gemaakt;
- verder zorgt Grotius College voor een nauwkeurige verwerking van alle persoonsgegevens, voor een passend veiligheidsbeleid en passende organisatorische maatregelen om de persoonsgegevens te beschermen, voor beleid omtrent het veilig verwijderen van persoonsgegevens die niet langer nodig zijn.

De hierna volgende bepalingen zijn gebaseerd op deze beginselen en de eisen uit de AVG (artikel 5 AVG).

3 Rechtmatigheid van verwerkingen

3.1 Grondslagen

Grotius College verwerkt alleen persoonsgegevens wanneer sprake is van een rechtmatige grondslag. Dit betekent dat een verwerking alleen plaatsvindt als:

- er toestemming is van de betrokkene; of
- de verwerking is noodzakelijk voor het uitvoeren van een overeenkomst met de betrokkene; of
- Grotius College moet voldoen aan een wettelijke verplichting; of

- de verwerking is noodzakelijk om ter bescherming van de vitale belangen van de betrokkene; of
- de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de Grotius College of van een derde, tenzij het recht op privacy van de betrokkene zwaarder weegt, zeker in het geval het leerlingen betreft.

3.2 Toestemming

Wanneer Grotius College toestemming vraagt voor het verwerken van persoonsgegevens wordt het verzoek in een gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal gepresenteerd. Wanneer Grotius College in één keer toestemming vraagt voor meerdere doeleinden wordt in het verzoek om toestemming duidelijk het onderscheid tussen de verschillende verwerkingen en doeleinden aangegeven. Als verwerkingsverantwoordelijke wijzen we de betrokkene er op dat hij of zij elk moment zijn toestemming kan intrekken. Grotius College heeft een proces ingericht waarbij het geven van toestemming net zo eenvoudig is als intrekken ervan.

Grotius College verzamelt vooral gegevens van minderjarigen onder de 16 jaar. De procedure om toestemming te vragen is daarom gericht op het verkrijgen van toestemming van de ouders.

3.3 Vrijelijke toestemming

Grotius College is zich er bewust van dat toestemming vrijelijk, in begrijpelijke taal en ondubbelzinnig gegeven moet worden. Er wordt alleen toestemming gevraagd als de verwerking niet past binnen de vooraf bepaalde doelen in het kader van de uitvoering van een overeenkomst of het voldoen aan een wettelijke verplichting. De uitvoering van de overeenkomst kan daarom niet afhangen van het al dan niet geven van toestemming van de betrokkene.

3.4 Het verwerken van bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Ook de verwerking van genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van die persoon evenals gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn bijzondere persoonsgegevens.

Grotius College kan in het kader van haar dienstverlening gegevens over gezondheid verzamelen als dit noodzakelijk is voor het welzijn van de leerlingen die zij onder haar hoede heeft. Dit doet Grotius College alleen als daar toestemming voor is gegeven door de ouders of wanneer ouders deze informatie zelf openbaren.

4 Transparantie van de verwerkingen

4.1 Algemene openheid van zaken

Als verwerkingsverantwoordelijke heeft Grotius College de plicht om passende maatregelen te nemen en zo transparant mogelijk te zijn als het om de verwerking van persoonsgegevens gaat. Alle communicatie over het gebruik van persoonsgegevens,

reacties op verzoeken van betrokkenen en meldingen aan betrokkenen worden in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal gedaan. Er is om die reden een privacyverklaring gepubliceerd op de website van Grotius College en alle andere punten waar persoonsgegevens de organisatie binnen kunnen komen.

4.2 Reageren op verzoeken

Het verstrekken van persoonsgegevens aan de betrokkene indien daarom wordt verzocht vindt alleen plaats als de betrokkene op een juiste wijze kan worden geïdentificeerd. Reacties op verzoeken zoals bedoeld in artikel 4 van dit privacy beleid worden binnen een maand gegeven. Deze termijn kan eventueel met twee maanden worden verlengd, mits Grotius College de verzoeker hier binnen een maand van op de hoogte brengt. Voorwaarde is dat de verlenging noodzakelijk is afhankelijk van de complexiteit van het verzoek of het aantal verzoeken. Wanneer wordt besloten om geen gevolg te geven aan een verzoek van een betrokkene wordt dit met reden omkleed aan de betrokkene binnen één maand medegedeeld. De betrokkene wordt tegelijkertijd gewezen op de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

4.3 Kosten

Grotius College brengt als verwerkingsverantwoordelijke geen kosten in rekening voor het verstrekken van informatie over het gebruik van persoonsgegevens. In uitzonderingsgevallen waarbij verzoeken van betrokkene kennelijk ongegrond zijn of wanneer buitensporige verzoeken worden gedaan kan Grotius College besluiten om:

- een redelijke vergoeding te vragen voor de gemaakte administratieve kosten of getroffen redelijke maatregelen;
- of geen vervolg te geven aan het verzoek of de verzoeken.

In beide gevallen zal Grotius College de ongegronde of buitensporige aard van het verzoek of verzoeken aantonen.

4.4 Het verzamelen van persoonsgegevens bij de betrokkene

Bijna alle persoonsgegevens die Grotius College ontvangt over betrokkenen worden bij de persoon zelf verzameld. Bij het verkrijgen van de gegevens zorgt Grotius College er voor dat de persoon die ze overhandigt over alle relevantie informatie beschikt betreffende de gegevensverwerking.

Deze informatie verstrekt Grotius College via haar privacy verklaring wat op haar website is gepubliceerd.

4.5 Het verzamelen van persoonsgegevens bij anderen dan de betrokkene (n)

In de gevallen dat Grotius College persoonsgegevens ontvangt van anderen dan waarop de persoonsgegevens betrekking hebben worden de betrokkenen hierover geïnformeerd. De informatie bevat dezelfde gegevens als genoemd in artikel 3.4, aangevuld met de bron waarvan de persoonsgegevens afkomstig zijn. Deze informatie wordt binnen een maand aan de betrokkene verstrekt. Als Grotius College een besluit neemt ten aanzien van betrokkene dat informeert zij de betrokkene over het ontvangen van zijn of haar persoonsgegevens voordat het besluit wordt genomen of bekend wordt gemaakt.

5 De rechten van betrokkenen

In artikel 3 van dit beleidsdocument wordt het recht op informatie uitgebreid beschreven, net als de procedure om op verzoeken te reageren. In dit artikel worden alle overige soorten verzoeken, de uitoefening van de rechten van betrokkenen, waar Grotius College op dient te reageren benoemd:

- Recht op rectificatie: de betrokkenen hebben het recht om te verzoeken dat onjuiste of onvolledige persoonsgegevens onverwijld worden gerectificeerd door de verwerkingsverantwoordelijke;
- recht op gegevenswissing: de betrokkene heeft het recht dat zijn of haar persoonsgegevens onder bepaalde voorwaarden worden verwijderd;
- Betrokkenen hebben het recht op beperking van de verwerking. Dit betekent dat de persoonsverwerking stil komt te liggen. De persoonsgegevens blijven bewaard maar worden niet bewerkt, doorgegeven of verwijderd.

Grotius College zorgt voor procedures om tijdig en op een juiste wijze op deze verzoeken te kunnen reageren.

5.1 Informatieplicht

Als verwerkingsverantwoordelijke hebben we de plicht om elke derde ontvanger van de persoonsgegevens op de hoogte te brengen van elke rectificatie, wissing of beperking. Als de betrokkene meer informatie wil over de ontvangers dan verstrekt Grotius College deze.

5.2 Recht op overdraagbaarheid

Als verwerkingsverantwoordelijke zorgen wij er voor de betrokkene zijn of haar persoonsgegevens, die aan ons zijn verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij of zij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen als. Als het technisch mogelijk is heeft de betrokkene er recht op dat de persoonsgegevens rechtstreeks naar de andere verwerkingsverantwoordelijke worden verzonden.

5.3 Recht op bezwaar

De betrokkenen heeft het recht bezwaar te maken tegen de verwerking wanneer Grotius College als verwerkingsverantwoordelijke van mening is dat de verwerking kan worden gebaseerd op het gerechtvaardigde belang van de organisatie. Als verwerkingsverantwoordelijke zorgt Grotius College voor een begrijpelijke en kenbare argumentatie waarom het gerechtvaardigde belang van de organisatie boven het recht op privacy van de betrokkene zou moeten prevaleren.

6 Verantwoordelijkheid passende maatregelen

Als verwerkingsverantwoordelijke zorgt Grotius College voor passende technische en organisatorische maatregelen om te waarborgen en aan te kunnen tonen dat alle verwerkingen in overeenstemming met de AVG plaatsvinden.

Om te bepalen of een maatregel passend is worden de volgende aspecten overwogen:

- de aard, de omvang, de context en het doel van de verwerking en;

- de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen.

Deze maatregelen zullen periodiek geëvalueerd worden en als dit nodig blijkt geactualiseerd. Grotius College voert hierbij een gegevensbeschermingsbeleid waarin de genomen maatregelen worden beschreven. Onderdeel van deze maatregelen kan zijn het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 AVG of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 AVG. Dit draagt bij aan de aantoning dat aan de AVG is voldaan.

7 Privacy by design en Privacy by default

Als verwerkingsverantwoordelijke zorgen we ervoor dat al onze verwerkingen van begin af zo min mogelijk inbreuk maken op de privacy van de betrokkenen. Dit doen wij rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden. Op basis daarvan treft Grotius College passende technische en organisatorische maatregelen om aan de basisbeginselen van de AVG te kunnen voldoen, zoals een minimale gegevensverwerking en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van onze klanten en leerlingen.

Grotius College treft ook passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.

8 Schriftelijke afspraken met derden

Grotius College werkt met diverse partijen samen. In dat kader kunnen persoonsgegevens worden uitgewisseld. Wanneer persoonsgegevens worden uitgewisseld tussen partijen is dit tussen een verantwoordelijke en een verwerker, of tussen meerdere medeverantwoordelijken.

- Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Wanneer hier sprake van is zorgt Grotius College voor duidelijke afspraken tussen de verantwoordelijke partijen zodat duidelijk is voor de betrokkene waar hij of zij zijn rechten kan uitoefenen en wie verantwoordelijk is voor het informeren van de betrokkene. De betrokkene heeft het recht om deze afspraken in te zien en kan ongeacht deze afspraken bij alle verantwoordelijken een verzoek indienen.
- Een verwerker verwerkt namens Grotius College persoonsgegevens waarvoor het doel en de middelen van de verwerking door Grotius College worden bepaald. Het is de plicht van de verwerkingsverantwoordelijke om alleen met verwerkers die passende maatregelen hebben genomen om aan de AVG te voldoen.

- De verwerker mag niet zonder toestemming van Grotius College voor zichzelf verwerkers inschakelen. Na gegeven toestemming mag de verwerker wijzigingen aanbrengen in de door haar ingeschakelde sub-verwerkers, als verwerkingsverantwoordelijke kunnen we hier bezwaar tegen maken.
- De verwerker is verantwoordelijk voor het opleggen van dezelfde afspraken zoals die tussen Grotius College en de verwerker zijn gemaakt aan de subverwerker.

9 Verwerkersovereenkomsten

De afspraken tussen Grotius College en haar verwerkers zijn vastgelegd in een verwerkersovereenkomst. Grotius College zorgt voor een standaard overeenkomst waarin deze afspraken aan een verwerker kunnen worden opgelegd. Indien een verwerker zelf een correcte overeenkomst aanbiedt kunnen de afspraken daarin worden vastgelegd. Bij aangaan van overeenkomsten met leveranciers of dienstverleners dient telkens op voorhand te worden ingeschat of een verwerkersovereenkomst dan wel een geheimhoudingsverklaring nodig is om de persoonsgegevens van Grotius College te beschermen. In elk geval dient tijdens het inkoopproces stil te worden gestaan bij de mogelijkheid dat een verwerkersovereenkomst verplicht is. De privacy officer of de FG adviseren over de inhoud van een externe verwerkersovereenkomst voordat deze wordt getekend.

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.

10 Het verwerkingsregister

10.1 Het opstellen van een register

Grotius College streeft aantoonbare naleving van de AVG na. In dat kader wordt een verwerkingsregister bijgehouden door Grotius College. Hierin staan alle verwerkingen waarvoor de verwerkingsverantwoordelijke verantwoordelijk is. Dit register moet periodiek worden geëvalueerd en worden bijgewerkt indien nodig.

10.2 Verwerkersregister

Grotius College treft op dit moment niet op als verwerker voor een andere verwerkingsverantwoordelijke. Mocht dit veranderen dan stelt Grotius College ook een register op met alle verwerkingen die voor andere verantwoordelijken wordt uitgevoerd.

10.3 Samenwerking met de AP

De registers van Grotius College zijn interne stukken maar kunnen ter beschikking worden gesteld aan de toezichthouder. Op elk vlak waar in het kader van gegevensbescherming samen kan worden gewerkt met de toezichthouder zal dit worden gedaan. Aan verzoeken van de toezichthouder om samen te werken of inlichtingen te verstrekken wordt altijd voldaan.

11 Passende waarborgen gegevensbescherming

11.1 Organisatorische en technologische maatregelen

Ter bescherming van alle onder haar verantwoordelijkheid vallende persoonsgegevens heeft Grotius College passende organisatorische en technische maatregelen genomen. Deze maatregelen zijn opgenomen in het ICT/veiligheidsbeleid en worden rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen vastgesteld. Het veilig en betrouwbaar omgaan met informatie is 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. Grotius College verwacht van alle medewerkers, leerlingen, (geregistreeerde) 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 imagooverlies. Grotius College heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

11.2 Risico's minimaliseren

Het beveiliging is gericht op het minimaliseren van risico's. Bij de beoordeling of de beveiliging van een passend niveau is wordt rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig. Grotius 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.

11.3 Meldplicht datalekken

Als verwerkingsverantwoordelijke zorgen wij voor een adequaat protocol dat in werking treedt wanneer een beveiligingsincident geconstateerd wordt waar mogelijk persoonsgegevens bij betrokken zijn. Deze incidenten worden geregistreerd en, indien nodig, gemeld aan de toezichthouder en/of betrokkenen. Een uitgebreide beschrijving van de procedure is te vinden in het protocol. De Functionaris Gegevensbescherming is bij de uitvoering betrokken.

11.4 De uitvoerig van een DPIA bij gevoelige gegevens

Wanneer een nieuwe verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voeren wij als verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden. De toezichthouder heeft voorwaarden opgesteld

en een DPIA voor bepaalde soorten verwerkingen verplicht gesteld. Grotius College heeft dit in haar ICT/veiligheidsbeleid opgenomen.

12 De rol van de Functionaris Gegevensbescherming

12.1 Aanstellen FG

Als verwerkingsverantwoordelijk heeft Grotius College een FG aangesteld. Omdat de FG makkelijk bereikbaar moet zijn voor alle betrokkenen en de toezichthouder worden de contactgegevens vermeld op onze website en privacyverklaringen.

12.2 Onafhankelijke positie FG

De FG wordt, om zijn of haar taken naar behoren te kunnen vervullen, tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. In dat kader kan hem of haar toegang worden verschaft tot alle benodigde persoonsgegevens en worden alle beschikbare middelen ter beschikking gesteld om haar taken uit te voeren. Hierbij ontvangt de FG geen instructies van de verantwoordelijke, is de FG gebonden aan vertrouwelijkheid en mag de FG geen andere functies die tot een belangenconflict kunnen leiden.

12.3 Wettelijke taken van een FG (art. 39 AVG)

Een FG heeft een aantal wettelijke taken. Grotius College stelt alle middelen ter beschikking aan de FG om deze taken naar behoren uit te voeren:

de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de AVG en het eigen gegevensbeschermingsbeleid en toezien op de naleving hiervan. Tevens is de FG contactpersoon voor de toezichthouder en alle betrokkenen.

13 Aantoonbare naleving

13.1 Uitwerking in 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.

13.2 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, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

13.3 Planning en controle

Dit IBP-beleid wordt minimaal elk jaar geëvalueerd door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Grotius College 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 hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

13.4 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 leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met 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 de verwerkingsverantwoordelijke, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement. Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Grotius College de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.