Beleidsplan Privacy

Dr. Nassau College

Assen, 14 februari 2018

Projectgroep AVG

Judith Bordewijk, Chris Knol en Wouter van der Weerd

Versie 2

Inhoud

Bron:
saMBO-ICT
Kennisnet

1. Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze ontwikkelingen brengen nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van de bescherming van persoonsgegeven (privacy).

1.1 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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. Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doel het garanderen van de privacy van leerlingen, ouders en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen. Dit beleid is erop gericht om de beveiliging van zowel digitaal als niet-digitaal opgeslagen persoonsgegevens te optimaliseren. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers, leerlingen en ouders, wordt gerespecteerd en dat het Dr. Nassau College voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het privacy beleid binnen het Dr. Nassau College geldt voor alle medewerkers, leerlingen, ouders/verzorgers, bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid valt alle geautoriseerde toegang niet alleen fysiek (deuren, sloten, kasten) maar ook alle devices waarmee toegang tot het schoolnetwerk verkregen kan worden.

- De nadruk van het beleid ligt op die informatiesystemen, die vallen onder de verantwoordelijkheid van het Dr. Nassau College. Het beleid heeft betrekking op gecontroleerde informatie die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het beleid van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het Dr. Nassau College waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan het Dr. Nassau College persoonsgegevens verwerkt.

- Dit beleid is van toepassing op geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van het Dr. Nassau College, op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is nadrukkelijk ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- Het privacy-beleid binnen het Dr. Nassau College heeft 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
    - ICT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
    - Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers
    - Beleid inzake aanschaf en gebruik van digitale leermiddelen
    - Informatiemanagement; beleid op het gebied van opslag, beheer, bewerken van digitale gegevens in de systemen van het Dr. Nassau College en bij aanschaf van nieuwe systemen

3. Uitgangspunten

De belangrijkste beleidsuitgangspunten bij het Dr. Nassau College zijn:

- De beveiliging van de persoonsgegevens dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming.

- De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van het Dr. Nassau College om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.

- Binnen het Dr. Nassau College is het veilig en betrouwbaar omgaan met persoonsinformatie 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 fysieke documenten.

- De school 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 leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van persoonsgegevens.

- Het Dr. Nassau College sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt bij voorkeur gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en het bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis. Indien geen gebruik gemaakt wordt van het eerder genoemde convenant wordt de bewerkersovereenkomst voorgelegd aan een jurist. De kosten voor het toetsen van het afwijkende model bewerkersovereenkomst komt ten laste van het betreffende project.

- Er dient een gedragscode geformuleerd, vastgesteld en geïmplementeerd te worden waar alle medewerkers, leerlingen, bezoekers en externe relaties dienen zich te houden.

- Privacy is bij het Dr. Nassau College een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij het Dr. Nassau College vanaf de start rekening gehouden met de bescherming van persoonsgegevens.

3.1 Vijf vuistregels met betrekking tot privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij het Dr. Nassau College zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat persoonsgegevens niet langer worden bewaard dan noodzakelijk.
4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde privacy-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal het Dr. Nassau College aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4. Wet- en regelgeving

Het Dr. Nassau College voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur VO
- Wet bescherming persoonsgegevens (Wbp)
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

5. Organisatie

De organisatie van de bescherming van persoonsgegevens 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.

Dit hoofdstuk beschrijft hoe privacy in het Dr. Nassau College is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben.

5.1 Rollen (functies) rondom de bescherming van persoonsgegevens

Om privacy gestructureerd en gecoördineerd op te pakken worden bij het Dr. Nassau College een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.2 Richtinggevend

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor de bescherming van persoonsgegevens en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het privacy-beleid wordt op basis van regelmatige rapportages geëvalueerd.

5.3 Sturend

Functionaris voor Gegevensbescherming (FG)
De FG houdt binnen het Dr. Nassau College toezicht op de toepassing en naleving van de Wbp/AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG heeft regelmatig overleg met de informatiemanager en het hoofd ICT. De FG is ook de contactpersoon voor klachten, vragen en incidenten

Informatiemanager
De informatiemanager organiseert de interne en externe informatiestromen en stemt het beleid informatiemanagement jaarlijks af met het privacy-beleid.

Hoofd ICT
Het hoofd ICT organiseert de informatiebeveiliging binnen het Dr. Nassau College.

Directeuren en vestigingsmanagers
Op de locaties zien de directeur of de vestigingsmanager erop toe dat het privacy-beleid wordt nageleefd en wordt omgezetnaar werkinstructies. Zij zijn ervoor verantwoordelijk dat medewerkers in de scholen zich gedragen conform afspraken. De directeuren en vestigingsmanagers hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Medewerkers hebben verantwoordelijkheid met betrekking tot beveiliging van persoonsgegevens in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Van medewerkers wordt gevraagd om actief betrokken te zijn bij privacy. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

Leidinggevende
Naleving van het privacy-beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het privacy-beleid;
- toe te zien op de naleving van het privacy-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde privacy-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de FG.

6. Controle en rapportage

Dit beleidsplan privacy wordt jaarlijks getoetst en bijgesteld door het cmt. Hierbij wordt rekening gehouden met:

- De status van de bescherming persoonsgegevens (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent het Dr. Nassau College een jaarlijkse planning en control cyclus voor privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het privacybeleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van de bescherming van persoonsgegevens.
- **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van het Dr. Nassau College.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij het Dr. Nassau College 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, ouders en gasten. Verhoging van het beveiligingsbewustzijn inzake privacy is een verantwoordelijkheid van de FG met het College van Bestuur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij het Dr. Nassau College heeft alle informatie waarde, daarom worden alle gegevens waarop het privacy-beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang zijn voor de bescherming van persoonsgegevens.

6.3 Incidenten en datalekken

Alle incidenten met betrekking tot persoonsgegevens worden gemeld bij de projectgroep AVG (Judith Bordewijk, Chris knol en Wouter van der Weerd). De projectgroep draagt zorg voor de afhandeling van deze incidenten in nauw overleg met de bestuurder en volgt hiertoe een gestructureerd proces, dat voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 Controle en naleving

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van de processen waarbij gebruik gemaakt wordt van persoonsgegevens. Van belang hierbij is dat leidinggevenden en directeuren en vestigingsmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij het Dr. Nassau College wordt actief aandacht besteed aan privacy bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de FG een belangrijke rol. De FG wordt aangesteld door het College van Bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement.

Bij het Dr. Nassau College is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol. Het is in het belang van het Dr. Nassau College en van alle medewerkers dat alle lekken van persoonsgegevens, hoe klein ook, worden gemeld. Alleen dan kan de projectgroep herhaling voorkomen en het lek of het incident toetsten op ernst en omvang en tijdig de juiste maatregelen treffen om de schade voor zowel de getroffen personen als de school te beperken.