Privacybeleidsplan
NHL Stenden Hogeschool

Emmen, november 2019
Versienummer: 1.1

Colofon

Error! Reference source not found.

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

Deze versie is gebaseerd op het Gezamenlijk product van de SURF Projectgroep 'Voorbereiding Implementatie Algemene Verordening Gegevensbescherming' en SURFibo (nu SCIPR). Aan de oorspronkelijke versie werkten mee Frans Pingen (Wageningen University), Bart van den Heuvel (Maastricht University) Sedat Capkin (SURFsara), Ronja Meijer (Wageningen University) Jaap Gall (Hogeschool Arnhem Nijmegen) Chloë Baartmans (SURFnet).
Voor NHL Stenden Hogeschool is deze versie bewerkt, aangepast en aangevuld door Willem Bakker, Functionaris voor Gegevensbescherming

Versie 2.0 maart 2018

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

NHL STENDEN hogeschool

Inhoudsopgave

1. Inleiding

In een datagedreven maatschappij waarin de technologie vrijwel onbeperkte mogelijkheden biedt om gegevens te verzamelen, op te slaan, te analyseren en te verspreiden, is de bescherming van persoonsgegevens van het allergrootste belang. Privacy is een grondrecht[1] dat in onze maatschappij meer dan ooit bescherming verdient. Dat is de achtergrond van de Algemene verordening gegevensbescherming die in heel Europa vanaf 25 mei 2018 wordt toegepast.

Voor een kennisinstelling zoals NHL Stenden Hogeschool is de bescherming van persoonsgegevens een topprioriteit. Een hogeschool is immers een ware 'gegevensfabriek'. Kennis, gegevens en persoonsgegevens zijn ons bedrijfskapitaal.

Los van de grote materiële en immateriële risico's[2] die een onzorgvuldige omgang met persoonsgegevens met zich meebrengen, kent NHL Stenden Hogeschool daarom een zeer hoge prioriteit toe aan de bescherming van de persoonsgegevens van studenten, medewerkers en alle andere betrokkenen. De juiste omgang met persoonsgegevens door de hogeschool is – ook volgens de wet – in laatste instantie de verantwoordelijkheid van het college van bestuur.

Met de maatregelen beschreven in dit beleidsdocument geeft NHL Stenden Hogeschool invulling aan die verantwoordelijkheid. Dit beleid beoogt de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren. Met dit beleid en de correcte uitvoering daarvan voldoet NHL Stenden Hogeschool aan de privacywetgeving.

1.1. Definities

Avg: Algemene Verordening Gegevensbescherming[3].

Beleid: dit beleid met betrekking tot het verwerken van persoonsgegevens door NHL Stenden Hogeschool.

Betrokkene: een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft. NHL Stenden Hogeschool onderscheidt de volgende categorieën betrokkenen: medewerkers in loondienst, medewerkers niet in loondienst, studenten, cursisten, leads, alumni, externe relaties, gasten van het Stenden Hotel en onderzoekssubjecten.

Verwerkingsverantwoordelijke: het college van bestuur van NHL Stenden Hogeschool, dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Verwerker: een door NHL Stenden Hogeschool ingeschakelde (derde) partij die ten behoeve van NHL Stenden Hogeschool, en op basis van schriftelijke instructies, persoonsgegevens verwerkt.

Verwerking: elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.

---

[1] Zie Artikel 9 van de Grondwet en Artikel 12 van de Universele Verklaring van de Rechten van de Mens

[2] Al naar gelang de aard van de overtreding bedragen de maximale boetes 10 of 20 miljoen euro of, als dat meer is, respectievelijk 2 of 4% van de jaaromzet. Maar reputatieschade door een schandaal van enige omvang is naar verwachting voor een instelling voor hoger onderwijs waarvan de financiering afhankelijk is van de studenteninstroom mogelijk nog erger.

[3] De Algemene Verordening Gegevensbescherming is op 25 mei 2016 in werking getreden en per 25 mei 2018 van kracht. In het Engels: General Data Protection Regulation (GDPR).

Derde: ieder ander - niet zijnde de betrokkene, de verwerkingsverantwoordelijke of de verwerker, of enig persoon die onder rechtstreeks gezag valt van de verwerkingsverantwoordelijke of de verwerker - die gemachtigd is om persoonsgegevens te verwerken.

Datalek: een inbreuk op de beveiliging van persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hieronder vallen zowel opzettelijke als onopzettelijke datalekken.

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: Het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van betrokkenen. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling): Een beoordeling die helpt bij het identificeren van privacyrisico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

Profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Minderjarige: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.

1.2. Reikwijdte en doelstelling van het Beleid

Het Beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen NHL Stenden Hogeschool waaronder in ieder geval alle medewerkers (inclusief inhuur/outsourcing), studenten, gasten, bezoekers en externe relaties vallen, alsmede op andere betrokkenen waarvan NHL Stenden Hogeschool persoonsgegevens verwerkt.

In het beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van NHL Stenden Hogeschool alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het Beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij NHL Stenden Hogeschool wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.
Het Beleid van NHL Stenden Hogeschool heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamentele recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij NHL Stenden Hogeschool.

Dit Beleid heeft de volgende doelstellingen:

- Het bieden van een kader: het Beleid biedt een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde ‘best practice’ of norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- Het stellen van normen: de basis voor de beveiliging van persoonsgegevens is ISO 27001[2]. Maatregelen worden genomen op basis van ‘best practices’ in het hoger onderwijs en op basis van ISO 27002[3]. Voor de vraag welke persoonsgegevens door wie mogen worden verwerkt zijn de dataregisters (zie § 6.5) de norm.
- Het SURF Juridisch Normenkader (Cloud)services[4] wordt gehanteerd als best practice voor cloud services en andere outsource-contracten.
- Het nemen van de verantwoordelijkheid: het college van bestuur legt hiermee de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast voor de hele organisatie/ NHL Stenden Hogeschool.
- Daadkrachtige implementatie van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- Compliance met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen wil deze beleidsnotitie ook bijdragen aan de bewustwording op het gebied van privacy. Naleving van de wet lukt alleen als iedereen in de organisatie zich bewust is van de noodzaak van een zorgvuldige omgang met persoonsgegevens en een goede bescherming daarvan.

---

[2]Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[3]Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[4]SURF juridisch Normenkader (Cloud)services, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014 en geüpdatet in 2016, te vinden via https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html.

2. Beleidsprincipes Verwerking persoonsgegevens

2.1. Beleidsuitgangspunt en -principes

Het algemene beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van NHL Stenden Hogeschool om persoonsgegevens te verwerken en het belang van betrokkene die recht heeft op de eerbiediging van zijn persoonlijke levenssfeer en die zoveel mogelijk regie moet hebben over zijn eigen persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 6 van de Avg (“rechtmatigheid”).
- persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Informatie hierover moet eenvoudig toegankelijk zijn en begrijpelijk (“behoorlijkheid en transparantie”).
- persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hier om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven voordat men begint met de verwerking. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (“doelbinding”).
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (“minimale gegevensverwerking”).
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (“minimale gegevensverwerking”).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn (“juistheid”).
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (“integriteit en vertrouwelijkheid”).
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden van de verwerking. Hierbij worden de van toepassing zijnde bewaar- en vernietigingstermijnen in acht genomen (“opslagbeperking”).

3. Wet- en regelgeving

Bij NHL Stenden Hogeschool wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

3.1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

NHL Stenden Hogeschool heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (niet-)wetenschappelijk personeel nageleefd en toegepast.

3.2. Algemene verordening gegevensbescherming

NHL Stenden Hogeschool heeft de wettelijke vereisten geïmplementeerd door middel van dit Beleid. Daaronder vallen het rechtmatig en zorgvuldig verwerken van persoonsgegevens en het nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens.

3.3. Archiefwet

NHL Stenden Hogeschool houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

4. Rollen en verantwoordelijkheden met betrekking tot Verwerking persoonsgegevens

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken hanteert NHL Stenden Hogeschool de volgende rolverdeling.

4.1. College van Bestuur

Het college van bestuur is de verwerkingsverantwoordelijke en daarmee de eindverantwoordelijke voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen NHL Stenden Hogeschool. Het cvb stelt hiervoor het beleid, de maatregelen en de procedures vast.

4.2. Portefeuillehouder beveiliging persoonsgegevens

De portefeuillehouder beveiliging persoonsgegevens is het bestuurslid dat privacy in portefeuille heeft. Hij is eindverantwoordelijk voor de bescherming van persoonsgegevens binnen NHL Stenden Hogeschool.

4.3. Functionaris voor gegevensbescherming

NHL Stenden Hogeschool heeft overeenkomstig Artikel 37 van de Avg een 'Functionaris voor gegevensbescherming' aangesteld (hierna: FG). De FG is aangemeld bij de Autoriteit Persoonsgegevens. De FG wordt door NHL Stenden Hogeschool tijdig betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken. Hij informeert en adviseert over de naleving van de privacywetgeving en houdt daar toezicht op[4]. De FG heeft een onafhankelijke positie binnen de hogeschool.

De FG heeft de volgende taken. Hij:

- informeert en adviseert alle betrokken partijen over hun verplichtingen onder de Avg;
- ziet toe op de naleving van de Avg en andere relevante privacywetgeving;
- ziet toe op de naleving van dit privacybeleid door NHL Stenden Hogeschool;
- ziet toe op de uitvoering van Data Protection Impact Assessments (DPIA's);
- werkt samen met de Autoriteit persoonsgegevens en is daarvoor het eerste aanspreekpunt binnen de organisatie.

4.4. Systeemeigenaar

Iedere applicatie heeft een systeemeigenaar die ervoor verantwoordelijk is dat het systeem doet wat het moet doen en dat dit gebeurt binnen de kaders van dit Beleid. De systeemeigenaar zorgt ervoor dat de applicatie, zowel nu als in de toekomst, blijft beantwoorden aan de eisen en wensen van de gebruikers enerzijds en aan wet- en regelgeving anderzijds.

4.5. Directeur

De directeur is verantwoordelijk voor de naleving van dit beleid binnen zijn Academie, Dienst of Verbindingseenheid. Hij ondersteunt en faciliteert de Data Protection Counselor (zie § 4.6). De directeur heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het Beleid;

[4] Artikel 39 van de Avg noemt expliciet beide rollen: informeren en adviseren enerzijds en toezicht houden anderzijds.

- toe te zien op de naleving van het Beleid door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

4.6. Data Protection Counselor

De Data Protection Council (DPC) van NHL Stenden Hogeschool is een overleg- en adviesorgaan voor het beleid op het gebied van privacy (bescherming persoonsgegevens) en security (informatiebeveiliging). De DPC is samengesteld uit vertegenwoordigers van alle Academies, verbindingseenheden en afdelingen. De leden van de Regiegroep Informatiebeveiliging maken qualitate qua deel uit van de DPC. De leden van de DPC worden Data Protection Counselors genoemd.
Het dagelijks bestuur van de DPC wordt gevormd door de Functionaris Gegevensbescherming en de Security Officer, die beiden deel uit maken van de Bestuursstaf. De bijeenkomsten worden geleid door de FG.

Profiel van de Data Protection Counselor

De Data Protection Counselor
- heeft kennis van de aandachtsgebieden privacy en security[5];
- maakt deel uit van het managementteam van de academie, afdeling of eenheid die hij/zij vertegenwoordigt (hierna kortweg aangeduid als 'afdeling') of heeft de positie om direct invloed uit te oefenen op de uitvoering van het beleid op dit gebied;
- is in vaste dienst van NHL Stenden Hogeschool;
- ondersteunt de uitvoering van dit beleid binnen de afdeling, met name maar niet uitsluitend als het gaat om de naleving van de dataregisters, het afsluiten van verwerkersovereenkomsten, het beleggen van Data Protection Impact Assessments, het bijdragen aan de bewustwording van privacy en security binnen de afdeling, het uitwerken van concrete werkinstructies binnen de afdeling en het faciliteren van de rechten van de betrokkenen;
- is het eerste aanspreekpunt binnen de afdeling op het gebied van privacy en security;
- signaleert aandachtspunten op het gebied van privacy en security binnen de afdeling: de Data Protection Counselor heeft dienaangaande een meldingsplicht aan de FG;
- geeft binnen de DPC aan welke knelpunten, behoeftes en suggesties er vanuit de afdeling zijn op het gebied van privacy en security;
- doet zijn/haar uiterste best alle bijeenkomsten van de DPC bij te wonen – in uitzonderlijke gevallen kan hij/zij zich laten vervangen.

Een jaarlijkse gezamenlijke scholing maakt deel uit van de activiteiten van de Data Protection Council.

4.7. Privacy Officer

De Privacy Officer[6] ondersteunt de Academies, afdelingen en verbindingseenheden bij de uitvoering van het privacybeleid. Hij doet dat vanuit het Ster-team.

[5] Een jaarlijkse, gezamenlijke scholing maakt deel uit van de activiteiten van de Data Protection Council.

[6] Momenteel is deze rol nog niet ingevuld.

4.8. Medewerkers en studenten

Medewerkers en studenten zijn niet alleen degenen van wie persoonsgegevens worden verwerkt en die als zodanig bepaalde rechten hebben, maar zij hebben als medewerker en als student ook hun plichten waar het gaat om de omgang met persoonsgegevens in het kader van hun werk of van hun studie. Zowel medewerkers als studenten zijn gehouden aan dit Beleid. Zij dienen in alle gevallen zorgvuldig met persoonsgegevens om te gaan en zijn gehouden mogelijke datalekken of kwetsbaarheden onmiddellijk te melden via het meldpunt datalekken of bij de Functionaris Gegevensbescherming.

Voor medewerkers zijn binnen hun Academie, verbindingseenheid of afdeling zo nodig protocollen en werkinstructies beschikbaar. Studenten worden door NHL Stenden Hogeschool op hun rechten en plichten gewezen, onder meer via het Studentenstatuut.

Medewerkers kunnen door het cvb een sanctie opgelegd krijgen, wanneer hun verwijtbaar gedrag kan worden verweten in verband met de omgang met persoonsgegevens van collega's, studenten of andere betrokkenen.

De sancties die aan studenten kunnen worden opgelegd wanneer hun verwijtbaar gedrag kan worden verweten in verband met de omgang met persoonsgegevens van andere studenten, medewerkers of andere betrokkenen van NHL Stenden Hogeschool, worden beschreven in het Studentenstatuut.

In §1.1 staat welke andere betrokkenen NHL Stenden Hogeschool onderscheidt.

5. Implementatie Beleid

Het college van bestuur van NHL Stenden Hogeschool is verantwoordelijk voor Verwerkingen van persoonsgegevens waarvan het college het doel en de middelen vaststelt. Het cvb is daarom de **Verwerkingsverantwoordelijke** in de zin van de Avg. De feitelijke verwerking van persoonsgegevens wordt echter in alle lagen van NHL Stenden Hogeschool uitgevoerd.
Een goede governance-structuur maakt het mogelijk dat de hogeschool de naleving van de privacywetgeving mogelijk maakt en dat de betrokkenen weten dat er zorgvuldig en binnen de kaders van de wet wordt omgegaan met hun persoonsgegevens. Die structuur maakt het ook mogelijk dat de betrokkenen hun rechten kunnen uitoefenen (zie § 8).

5.1. Verdeling van de verantwoordelijkheden

- Het zorgvuldig verwerken van persoonsgegevens dient gezien te worden als **een lijnverantwoordelijkheid**. Dat betekent dat de directeuren van academies, diensten en verbindingseenheden de primaire verantwoordelijk dragen voor een zorgvuldige verwerking van persoonsgegevens binnen hun afdeling. Dat doen zij binnen de in dit Beleid afgesproken kaders. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen.

- Het zorgvuldig omgaan met persoonsgegevens is **ieders verantwoordelijkheid**. Er wordt van medewerkers en studenten verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van NHL Stenden Hogeschool of van individuen. Het is daarom wenselijk dat er gedragscodes worden opgesteld en geïmplementeerd[7]. Het nemen van die verantwoordelijkheid is ook de taak van de resultaatverantwoordelijke teams.

5.2. Inpassing in de instellingsgovernance / 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 privacy op verschillende niveaus.

Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacy. Het strategisch niveau wordt ingevuld in het college van bestuur en in het hogeschoolberaad.

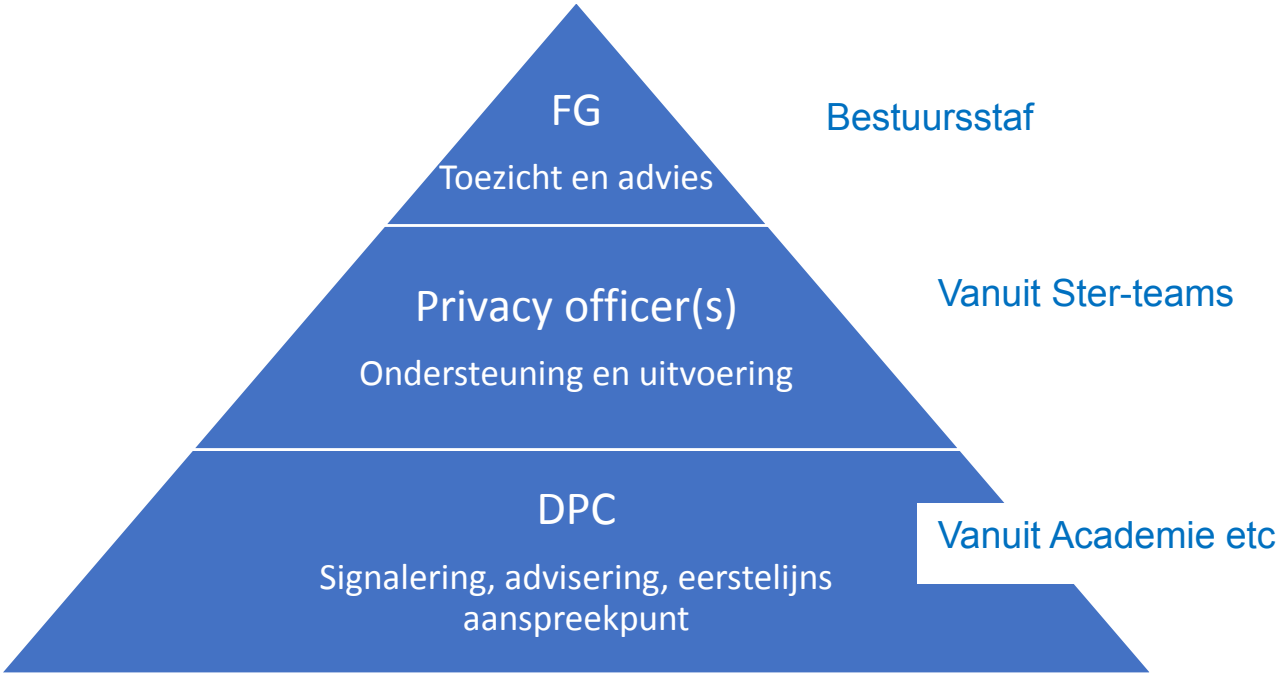
Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld in de Data Protection Council (zie § 4.6) en in de managementteams van de Academies, diensten en verbindingseenheden,

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Het operationele niveau wordt ingevuld in de Regiegroep Informatiebeveiliging (afstemming tussen de uitvoering van privacy en informatiebeveiliging) en in alle resultaatverantwoordelijke teams.

[7] De gedragscode voor medwerkers van NHL Stenden Hogeschool was op het moment van vaststelling van dit beleidsstuk nog niet beschikbaar. Dat geldt eveneens voor de Acceptable Use Policies voor medewerkers en studenten.

De Bestuursstaf adviseert op het strategische niveau, houdt toezicht op het tactische niveau (door middel van audits) en informeert desgevraagd op het operationele niveau.

Toegespitst op wat er op privacygebied moet gebeuren voor een goede naleving van de Avg, onderscheiden wij drie niveaus:



5.3. 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 bij NHL Stenden Hogeschool het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het Beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Deze campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met andere beveiligingscampagnes. Verhoging van het bewustzijn is een gezamenlijke verantwoordelijkheid van de Functionaris Gegevensbescherming en de Security Officer.

5.4. Controle en naleving

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. Vanuit de Bestuursstaf initiëren de FG en de Security Officer de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk geïntegreerd in de normale Planning & Controlcyclus. Peer-reviews in het kader van de SURFaudit maken onderdeel uit van de externe controles van NHL Stenden Hogeschool.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan NHL Stenden Hogeschool de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

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

6. Rechtmatige en zorgvuldige Verwerking van persoonsgegevens

NHL Stenden Hogeschool verwerkt persoonsgegevens in overeenstemming met de principes zoals uitgewerkt in paragraaf 2.1 van dit Beleid. Ter uitwerking van deze principes treft NHL Stenden Hogeschool de in dit hoofdstuk genoemde maatregelen.

6.1. Grondslag

NHL Stenden Hogeschool verwerkt slechts persoonsgegevens als er sprake is van een van de wettelijke gronden zoals beschreven in artikel 6 van de Avg:

a. *Toestemming van de Betrokkene.*
b. *Noodzakelijk voor de uitvoering van een overeenkomst met de Betrokkene.*
c. *Noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.*
d. Noodzakelijk om de vitale belangen van de Betrokkene of een ander natuurlijk persoon te beschermen.
e. Noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag.
f. *Noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.*

In de praktijk gaat het dan meestal om een van de schuingedrukte grondslagen, waarbij aangetekend moet worden dat ‘toestemming’ in afhankelijkheidsrelaties (zoals die tussen een werkgever en een werknemer, of tussen een hogeschool en een student) in het algemeen geen valide grondslag is[8]. De grondslagen voor de verschillende verwerkingen staan vermeld in de dataregisters (zie § 6.5).

6.2. Privacyverklaring

NHL Stenden Hogeschool verwerkt persoonsgegevens op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat NHL Stenden Hogeschool aan de betrokkene inzichtelijk maakt in hoeverre en op welke manier diens persoonsgegevens verwerkt worden. Bij het verzamelen van de persoonsgegevens zal NHL Stenden Hogeschool door middel van een privacyverklaring de betrokkene inlichten. Inlichting zal plaatsvinden voorafgaand aan de verwerking, tenzij dit redelijkerwijs niet mogelijk is. De dataregisters voor de verschillende categorieën bevatten een op die categorie toegespitste privacyverklaring. De website(s) van NHL Stenden Hogeschool bevatten een overkoepelende privacyverklaring. Zie ook paragraaf 8.1 van dit Beleid.

[8] Toestemming dient in volledige vrijheid gegeven worden, je moet weten waar je precies toestemming voor geeft en de toestemming moet expliciet zijn.

6.3. Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt, in overeenstemming met het uitgewerkte bewaarbeleid van NHL Stenden Hogeschool. NHL Stenden Hogeschool zal de persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren. De bewaartermijnen staan vermeld in de dataregisters.

6.4. Passende beveiligingsmaatregelen

NHL Stenden Hogeschool draagt zorg voor een adequaat beveiligingsniveau en brengt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen. NHL Stenden Hogeschool heeft een intern beveiligingsbeleid geïmplementeerd waarin maatregelen zijn uitgewerkt die werknemers van NHL Stenden Hogeschool hanteren.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van NHL Stenden Hogeschool.

6.5. Documentatieplicht

NHL Stenden Hogeschool heeft meerdere maatregelen getroffen om aantoonbaar te voldoen aan de wettelijke eisen van de Avg, waaronder de implementatie van het onderhavige Beleid.

NHL Stenden Hogeschool houdt overeenkomstig Artikel 30 van de Avg een ‘register van verwerkingsactiviteiten’ bij. NHL Stenden geeft daaraan invulling met integrale, overzichtelijke ‘dataregisters’ voor de verschillende categorieën van betrokkenen (methode Cuijpers). Er zijn dataregisters voor:

- studenten
- cursisten
- medewerkers in loondienst
- medewerkers niet in loondienst
- leads
- alumni
- externe relaties
- hotelgasten (van het Stenden University Hotel).

Voor de laatste categorie ‘onderzoekssubjecten’ (mensen die in het kader van een onderzoek worden ondervraagd, variërend van de bachelorthesis tot het onderzoek van een lector) wordt een aangepaste vorm van de documentatieplicht ontworpen. De FG wordt betrokken bij het opstellen van de dataregisters en hij houdt toezicht op de naleving ervan. Voor ieder ‘dataregister’ is een van de directeuren gemandateerd verantwoordelijk (zie bijlage 10.1 voor een overzicht).

Tevens voert NHL Stenden Hogeschool structureel Data Protection Impact Assessments (DPIA’s) uit, in ieder geval bij (grotere onderzoeks)projecten, infrastructurele wijzigingen binnen de informatiearchitectuur of de aanschaf van nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Als hieruit blijkt dat de verwerking een hoog risico zou inhouden indien NHL Stenden Hogeschool geen maatregelen neemt om het risico te beperken, raadpleegt NHL Stenden Hogeschool voorafgaand aan de verwerking, de toezichthoudende autoriteit.

De hierboven bedoelde DPIA’s worden – voor zover van toepassing - standaard na drie jaar herhaald.

Ook voor de introductie van nieuwe apps, binnen bijvoorbeeld een Academie, wordt standaard een ‘quick DPIA’ uitgevoerd.

De FG en de Security Officer adviseren over de vraag of een DPIA verplicht, aanbevolen of niet nodig is.

6.6. Privacy by Design en Privacy by Default

NHL Stenden Hogeschool hanteert bij de implementatie van iedere Verwerking de principes “Privacy by Design” en “Privacy by Default”.

Vanwege de aanzienlijke materiële risico’s is de risicoanalyse op privacybescherming en informatiebeveiliging onderwerp van de accountantscontrole en van een jaarlijkse bespreking in de Raad van Toezicht.

6.7. Geheimhouding

Bij NHL Stenden Hogeschool worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Iedereen behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

6.8. Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij een van de wettelijke uitzonderingen uit de Avg van toepassing is, zoals ‘uitdrukkelijke toestemming van de Betrokkene’ of een ‘zwaarwegend algemeen belang’. Tevens gelden zwaardere eisen voor de beveiliging van deze bijzondere persoonsgegevens. Daar waar de basisbescherming niet voldoende is, moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere persoonsgegevens vallen de volgende gegevens:
- gegevens waaruit ras of etnische afkomst blijkt;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- gegevens waaruit lidmaatschap van een vakbond blijkt;
- genetische gegevens met het oog op de unieke identificatie van een persoon;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Voor twee soorten persoonsgegevens geldt dat zij niet onder de categorie bijzondere persoonsgegevens vallen, maar dat de Verwerking en beveiliging ervan wel aan vergelijkbare strenge eisen zijn gebonden:

a) Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mag slechts onder toezicht van de overheid of binnen Europese of nationale wetgeving.

b) Onder de Nederlandse wetgeving mag een nationaal identificatienummer (het BSN of het onderwijsnummer) alleen worden verwerkt als dat wettelijk is bepaald.

6.9. Doorgifte persoonsgegevens

6.9.1. Uitbesteden van Verwerking aan een Verwerker

Indien NHL Stenden Hogeschool persoonsgegevens laat verwerken door een *Verwerker*, wordt de uitvoering van Verwerkingen geregeld in een verwerkersovereenkomst, tussen NHL Stenden Hogeschool, de Verwerkingsverantwoordelijke, en deze Verwerker.

6.9.2. Doorgifte persoonsgegevens binnen de Europese Economische Ruimte (hierna ‘EER’)

NHL Stenden Hogeschool verstrekt persoonsgegevens alleen aan een Verwerker gevestigd binnen de EER, als de verwerking is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 of artikel 9 Avg en als de Verwerker voldoet aan de wettelijke vereisten uit de Avg.

6.9.3. Doorgifte persoonsgegevens buiten de EER

NHL Stenden Hogeschool verstrekt persoonsgegevens alleen aan Verwerkers die zich bevinden in een land buiten de EER, indien aan een van de volgende voorwaarden is voldaan:

1. Het derde land, gebied, welbepaalde sector in een derde land, of de internationale organisatie in kwestie biedt volgens de Europese Commissie een passend beschermingsniveau.

   Als passend beschermingsniveau hanteert NHL Stenden Hogeschool:
   - De algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[7];

- Het Privacy Shield voor bedrijven in de Verenigde Staten, gepubliceerd door de Europese Commissie in samenwerking met de US Department of Commerce[8].

2. Doorgifte vindt plaats op basis van **passende waarborgen** uit de Avg, artikel 46 en 47. Doorgifte van persoonsgegevens naar de International Branch Campuses van NHL Stenden Hogeschool vindt plaats op grond van Europese standaardbepalingen ('model clauses'). Deze standaardbepalingen zijn ondertekend door alle vier de IBC's.

3. Doorgifte vindt plaats op basis van een van de **wettelijke uitzonderingen** uit artikel 49 van de Avg. Op grond van Artikel 30, lid 2a van de (Nederlandse) Uitvoeringswet Algemene verordening gegevensbescherming van 16 mei 2018, geeft NHL Stenden Hogeschool van studenten die op Grand Tour™ gaan met het oog op hun eigen veiligheid, met hun medeweten én alleen indien noodzakelijk, medische gegevens door, zoals allergie-informatie of medicatie.

6.10. Vragen- en klachtenprocedure

6.10.1. Melding en registratie

Vragen of klachten in verband met (de verwerking van) persoonsgegevens kunnen gemeld worden bij de Functionaris voor gegevensbescherming. Van vragen of klachten met een (potentiële) significante impact, zal een register bijgehouden worden.

Alle betrokkenen, alle verwerkers van NHL Stenden Hogeschool en alle derden kunnen een klacht of een vraag indienen.

6.10.2. Zwakke plekken in de beveiliging

Werknemers zijn gehouden potentiële datalekken onmiddellijk te melden bij het meldpunt Datalekken persoonsgegevens (https://datalekken.nhlstenden.com of op https://privacy.nhlstenden.com). Het kan dan bijvoorbeeld gaan om verlies of diefstal van gegevensdragers of mobiele devices, om waargenomen zwakke plekken in systemen of diensten, om vermoedens van inbreuk op de beveiliging of om aanwijzingen dat persoonsgegevens op een verkeerde plek zijn terechtgekomen. Van alle meldingen betreffende zwakke plekken in de beveiliging wordt een register bijgehouden.

6.10.3. Afhandeling

Vragen, klachten en zwakke plekken in de beveiliging worden doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures zo snel mogelijk afgehandeld.
Als de persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van NHL Stenden Hogeschool ernstig in gevaar zijn, worden in ieder geval het college van bestuur en de FG op de hoogte gesteld.

6.10.4. Evaluatie

Het is van belang om te leren van de feedback die via de vragen- en klachtenprocedure wordt verkregen. Registratie van significante vragen, klachten en zwakke plekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportages hierover maken daarom een vast onderdeel uit van de jaarrapportage van het college van bestuur en van de FG.

---

[6] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of bij formele studieresultaten, maar ze kunnen ook zijn vastgelegd door NHL Stenden Hogeschool, b.v. in een overeenkomst tussen NHL Stenden Hogeschool en de Betrokkenen.
[7] Deze kunt u vinden via de volgende link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
[8] Deze kunt u vinden via de volgende link https://www.privacyshield.gov/list.

7. Datalekken

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van een Datalek of het vermoeden van een Datalek in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1. Datalek

Van een Datalek is sprake als er een inbreuk op de beveiliging van persoonsgegevens plaatsvindt, die leidt tot enige ongeoorloofde Verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om een diefstal van een laptop, een in de trein vergeten usb-stick of een e-mail die naar de verkeerde persoon is verstuurd. Ernstige datalekken moeten worden gemeld bij de Autoriteit Persoonsgegevens binnen 72 uur na ontdekking daarvan en in sommige gevallen ook bij de Betrokkene, dus bij degene(n) van wie persoonsgegevens zijn gelekt.

7.2. Melding en registratie

Een Datalek kan bij NHL Stenden Hogeschool zowel binnen de eigen organisatie ontstaan, maar ook bij een door NHL Stenden Hogeschool ingeschakelde Verwerker. De volgende situaties moeten hierbij worden onderscheiden:

a. *Medewerker*: medewerkers moeten, indien zij een (mogelijk) Datalek waarnemen, of vermoeden zelf onderdeel te zijn van een Datalek, contact opnemen met het meldpunt datalekken persoonsgegevens via https://datalekken.nhlstenden.com (of via https://privavy.nhlstenden.com) of in uitzonderlijke gevallen bij de vertrouwenspersoon of Functionaris Gegevensbescherming van NHL Stenden Hogeschool.
b. *Verwerker:* het is ook mogelijk dat er een Datalek plaatsvindt bij een door NHL Stenden Hogeschool ingeschakelde Verwerker. De Verwerker zal overeenkomstig de afgesloten verwerkersovereenkomst het Datalek melden aan NHL Stenden Hogeschool.
c. *Andere personen:* indien een ander dan een medewerker of een Verwerker een (mogelijk) Datalek waarneemt of zelf onderdeel is van een Datalek, dient contact opgenomen te worden met het meldpunt datalekken persoonsgegevens via https://datalekken.nhlstenden.com (of via https://privavy.nhlstenden.com) of met de Functionaris Gegevensbescherming.

7.3. Afhandeling

Een vermoeden van een datalek dient onmiddellijk te worden gemeld via het daarvoor bestemde online-formulier. Daarin wordt onder meer vermeld:

- Wie de melding doet;
- Hoe het incident zich heeft gemanifesteerd;
- Of er persoonsgegevens in het spel zijn en zo ja, wat voor gegevens, en van hoeveel personen.

Een team van specialisten (het ‘triageteam’) krijgt na een dergelijke melding per omgaande een e-mail dat er een mogelijk datalek is. Het triageteam neemt de melding zo snel mogelijk in behandeling en stelt aan de hand van de Handleiding van de Autoriteit Persoonsgegevens vast of het inderdaad een datalek is (of een eenvoudig beveiligingsincident), of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens (dat hoeft namelijk niet altijd) en ten slotte of het datalek ook gemeld moet worden aan de betrokkene(n). Deze afwegingen worden vastgelegd in het online registratiesysteem. Een eventuele melding aan de Autoriteit Persoonsgegevens en aan de

betrokkenen wordt gedaan door het college van bestuur, geholpen door de Functionaris Gegevensbescherming. Dit gebeurt conform de wet binnen 72 uur na ontdekking. Melding aan de betrokkenen gebeurt door de Academie, afdeling of verbindingseenheid waar het datalek is opgetreden, met ondersteuning van Corporate Communicatie en de FG.

Het triageteam bestaat uit twee vertegenwoordigers van de Digitale Leer- en WerkOmgeving (Operational Security Officer en Informatiearchitect) en twee vertegenwoordigers van de Bestuursstaf (Corporate Security Officer en FG). De FG neemt op deze wijze kennis van alle (mogelijke) datalekken. Zo nodig doet het triageteam beroep op een collega van de afdeling Juridische Zaken,

Het cvb wordt geïnformeerd over alle als zodanig geïdentificeerde datalekken, dus ook over de datalekken die niet aan de Autoriteit Persoonsgegevens zijn gemeld.

7.4. Besluitvorming

Het triageteam *adviseert* over het al dan niet melden van een datalek aan de Autoriteit Persoonsgegevens en eventueel aan de betrokkene. Het *besluit* om al dan niet te melden wordt genomen door het cvb. Ook de melding zelf gebeurt officieel door het cvb. Indien het cvb in tegenstelling tot het advies van het triageteam besluit om het datalek niet te melden, neemt de FG dat besluit met de daaraan ten grondslag liggende overwegingen op in zijn jaarverslag.

7.5. Evaluatie

Het is van belang om te leren van Datalekken om de waarschijnlijkheid van toekomstige Datalekken te verkleinen. Registratie van Datalekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage over Datalekken met betrekking tot persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van het college van bestuur en van de FG.

.

[10] Beleidsregels meldplicht datalekken van de Autoriteit persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf.
[11] Vergelijkbaar met het CSIRT-team: Computer Security Incident Response Team.

8. Rechten van Betrokkenen

De Avg geeft Betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun persoonsgegevens. Een verzoek kan schriftelijk worden ingediend bij het daarvoor bestemde loket[9].

Voor alle in dit hoofdstuk uitgewerkte rechten van Betrokkenen gelden de volgende punten:

- **Melding aan Betrokkene**

NHL Stenden Hogeschool draagt er zorg voor dat de informatie en communicatie op een beknopte, toegankelijke en in duidelijke en eenvoudige taal wordt verstrekt aan Betrokkene. De taal zal worden afgestemd op de doelgroep. Per doelgroep (categorie van betrokkenen) heeft NHL Stenden een dataregister opgesteld waarin vermeld staat welke persoonsgegevens waar, waartoe en op welke wettelijke grondslag worden verwerkt. Ieder dataregister bevat een privacystatement toegespitst op de desbetreffende categorie.

- **Termijn**

Op een verzoek van een Betrokkene wordt zo spoedig mogelijk, doch uiterlijk binnen vier weken na indiening schriftelijk gereageerd. Hierbij zal de Betrokkene in ieder geval in kennis worden gesteld over het gevolg dat aan het verzoek is gegeven. Indien de termijn van vier weken redelijkerwijs niet haalbaar is, zal Betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. NHL Stenden Hogeschool zal in dat geval binnen twee maanden na het verstrijken van de eerste termijn gevolg geven aan het verzoek van de Betrokkene.

- **Identiteit Betrokkene**

NHL Stenden Hogeschool draagt bij het verstrekken van de betreffende informatie zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Hiertoe kan NHL Stenden Hogeschool extra informatie verzoeken.

- **Minderjarigen**

Een verzoek tot uitoefening van een van de rechten zoals uitgewerkt in dit hoofdstuk door een Betrokkene, zijnde Minderjarig, onder curatele gesteld of ten behoeve van wie een bewind of mentorschap is ingesteld, geschiedt door diens wettelijk vertegenwoordiger. Een reactie door NHL Stenden Hogeschool zal ook naar deze wettelijke vertegenwoordiger worden verstuurd.

8.1. Recht op informatie

De Betrokkene heeft het recht om door NHL Stenden Hogeschool te worden geïnformeerd over bepaalde aspecten van de Verwerking van zijn persoonsgegevens. NHL Stenden Hogeschool informeert de Betrokkene kosteloos over de Verwerking van diens persoonsgegevens, zowel in de situatie waarin de persoonsgegevens direct bij de Betrokkene zijn verzameld, als wanneer ze langs een andere route zijn verkregen.

A. Verkrijging direct van Betrokkene

NHL Stenden Hogeschool verstrekt de Betrokkene voorafgaand aan de verzameling van de gegevens, tenminste de volgende informatie indien de gegevens direct bij de Betrokkene worden verzameld:

- De identiteit en contactgegevens van de Verwerkingsverantwoordelijke en, in voorkomend geval, de FG.
- De specifieke doeleinden van Verwerking waarvoor de persoonsgegevens zijn bestemd alsook de rechtsgrond voor de verwerking.

[9] Moet nog worden ingericht.

- De gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of Derde als de Verwerking is gebaseerd op de rechtsgrond ‘gerechtvaardigd belang’.
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de persoonsgegevens door te geven aan een derde land, welk land dit is en op welke grond de persoonsgegevens daarnaartoe worden verstuurd.
- De periode gedurende welke de persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen.
- Het bestaan van het recht om de Verwerkingsverantwoordelijke te verzoeken om inzage, rectificatie of wissen van de persoonsgegevens, beperking van de hem betreffende verwerking, alsmede het recht tegen de Verwerking bezwaar te maken en het recht op dataportabiliteit.
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
- De ontvangers of categorieën van ontvangers van de persoonsgegevens.
- Indien de Verwerking is gebaseerd op de grondslag ‘toestemming’, het recht van de Betrokkene om die toestemming te allen tijde in te trekken.
- Of de persoonsgegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting.
- Of de persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de te verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.

B. Verkrijging niet direct van Betrokkene

Als de persoonsgegevens niet direct bij de Betrokkene zelf zijn verzameld maar langs een andere route, zal aan de Betrokkene, in aanvulling op de hiervoor genoemde punten, de volgende informatie worden verstrekt:

- De categorieën van persoonsgegevens.
- De bron waar de persoonsgegevens vandaan komen.

Bovenstaande informatie is bij NHL Stenden Hogeschool vastgelegd in de dataregisters en – voor zover het onderzoek betreft – in het pakket SmartPIA.

De dataregisters zijn voor alle categorieën betrokkenen beschikbaar vanaf het eerste contact dat ze met NHL Stenden Hogeschool hebben. Studenten, cursisten en medewerkers worden bij de aanvang van hun studie of bij het afsluiten van de arbeidsovereenkomst actief over de dataregisters geïnformeerd.

8.2. Recht op inzage

- *Verzoek*

Iedere Betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt en, als dat het geval blijkt, het recht op inzage in hem betreffende verwerkte persoonsgegevens.

- *Mededeling*

Met het verstrekken van het dataregister informeert NHL Stenden Hogeschool de betrokkene over:

- Een omschrijving van de doeleinden van de Verwerking.
- De categorieën van gegevens waarop de Verwerking betrekking heeft.
- Categorieën van ontvangers.
- Beschikbare informatie over herkomst van de gegevens.
- De termijn van bewaring van gegevens of indien dat niet mogelijk is, de criteria om die termijn te bepalen.
- Het recht van Betrokkene om de Verwerkingsverantwoordelijke te verzoeken om rectificatie of wissen van gegevens, beperking of bezwaar van Verwerking alsmede het recht op dataportabiliteit.
- Het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.
- Alle beschikbare informatie over de bron van de gegevens, als de gegevens niet bij de Betrokkene zijn verzameld.

- De passende waarborgen die zijn getroffen, indien de gegevens worden doorgegeven aan een derde land.

- *Kopie*

De Betrokkene kan om een kopie van alle persoonsgegevens verzoeken. Deze kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of de Betrokkene expliciet om een papieren kopie verzoekt.

- *Kosten*

Iedere eerste kopie kan kosteloos worden aangevraagd. Per additionele kopie zal NHL Stenden Hogeschool echter een vergoeding van administratieve kosten a € 15 in rekening brengen aan de Betrokkene.

- *Rechten en vrijheden van anderen*

NHL Stenden Hogeschool zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

8.3. Recht op dataportabiliteit

- *Gronden voor verzoek*

Iedere Betrokkene kan een verzoek indienen bij NHL Stenden Hogeschool om (kosteloos) zijn gegevens te verkrijgen in een gestructureerde, gangbare en machineleesbare vorm dan wel deze rechtstreeks aan een andere Verwerkingsverantwoordelijke over te laten dragen (dataportabiliteit), zonder daarbij te worden gehinderd door NHL Stenden Hogeschool, indien is voldaan aan de volgende voorwaarden:

1. De Verwerking door NHL Stenden Hogeschool berust op de grondslag ‘toestemming’ dan wel ‘uitvoering van een overeenkomst met de Betrokkene’.
2. De Verwerking in kwestie is geheel geautomatiseerd.

- *Rechten en vrijheden van anderen*

NHL Stenden Hogeschool zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

- *Verwijderen van gegevens*

Indien een Betrokkene zijn recht van dataportabiliteit heeft uitgeoefend in het kader van een Verwerking ter uitvoering van een overeenkomst, mag NHL Stenden Hogeschool niet besluiten de gegevens te wissen. Na het verstrijken van de bewaartermijn, dient NHL Stenden Hogeschool de gegevens echter alsnog te wissen.

Indien het recht is uitgeoefend in het kader van een Verwerking op grond van toestemming van de Betrokkene, mag NHL Stenden Hogeschool wel besluiten om de gegevens te wissen na uitoefenen van het recht.

8.4. Recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking

- *Verzoek tot rectificatie, aanvulling, verwijdering of beperking*

Iedere Betrokkene kan met betrekking tot over hem opgenomen persoonsgegevens bij NHL Stenden Hogeschool van deze gegevens verzoeken die te corrigeren, aan te vullen, te verwijderen of de Verwerking te beperken. Bij het recht op beperking worden de persoonsgegevens tijdelijk afgeschermd en niet meer verwerkt door NHL Stenden Hogeschool. De beperking wordt duidelijk in het bestand aangegeven.

- *Kennisgeving*

Indien blijkt dat de opgenomen persoonsgegevens van de Betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de Verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, zal de gegevensbeheerder (dat kan zowel de functioneel beheerder als de Verwerker zijn) deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken.

Bovendien worden Derden aan wie de gegevens, voorafgaand aan de rectificatie, aanvulling, verwijdering dan wel beperking, zijn verstrekt hiervan in kennis gesteld, tenzij dit redelijkerwijs niet mogelijk of gezien de omstandigheden niet relevant is. De verzoeker mag opgave verzoeken van degene aan wie NHL Stenden Hogeschool deze mededeling heeft gedaan.

- *Termijn voor uitvoering*

De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De uitvoering hiervan geschiedt kosteloos voor de Betrokkene.

8.5. Recht van bezwaar

- *Gronden voor bezwaar*

Voor Betrokkenen bestaan er twee gronden om bezwaar te maken tegen een Verwerking:

1. In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar maken tegen Verwerking bij NHL Stenden Hogeschool als deze Verwerking plaatsvindt op grond van de behartiging van het gerechtvaardigd belang van NHL Stenden Hogeschool of van een Derde aan wie de gegevens worden verstrekt. Zie voor een beschrijving van de grondslagen, paragraaf 6.1.

   NHL Stenden Hogeschool zal bij bezwaar de verdere Verwerking in beginsel staken. Indien NHL Stenden Hogeschool kan aantonen dat zijn dwingende gerechtvaardigde belangen zwaarder wegen dan de belangen of grondrechten en de fundamentele vrijheden van de Betrokkene, zal de Verwerking worden voortgezet. Indien het bezwaar gerechtvaardigd is, treft NHL Stenden Hogeschool (kosteloos) maatregelen die nodig zijn om de persoonsgegevens voor de betreffende doeleinden niet meer te verwerken.

2. Bij een Verwerking met het doel ‘direct marketing’, heeft een betrokkene te allen tijde het recht om bezwaar te maken. NHL Stenden Hogeschool zal bij bezwaar de verwerking voor doeleinden van direct marketing onmiddellijk (kosteloos) staken en niet hervatten.

8.6. Geautomatiseerde besluitvorming

Gronden

Betrokkenen hebben het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde Verwerking gebaseerd besluit, waaraan voor hem rechtsgevolgen zijn verbonden. Onder een ‘besluit gebaseerd op een geautomatiseerde Verwerking’ wordt verstaan een besluit dat is gemaakt zonder menselijke tussenkomst. Hieronder valt onder andere Profilering.

NHL Stenden Hogeschool neemt nooit besluiten over personen op grond van een uitsluitend geautomatiseerde verwerking van persoonsgegevens.

8.7. Rechtsbescherming

- *Algemene klachten*

Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit reglement jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij de Functionaris voor Gegevensbescherming: fg@nhlstenden.com. Een klacht over de Functionaris Gegevensbescherming kan worden ingediend bij de vertrouwenspersoon of bij de Autoriteit Persoonsgegevens.

- *Overige bezwaarmogelijkheden*

Naast de algemene interne klachtenprocedure zoals hierboven beschreven, heeft de Betrokkene de volgende mogelijkheden als hij het idee heeft dat NHL Stenden Hogeschool een hem rakende overtreding van de Avg heeft begaan:

A. Verzoekschriftprocedure bij de kantonrechter

Indien NHL Stenden Hogeschool afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of NHL Stenden Hogeschool heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van NHL Stenden Hogeschool ingediend te worden bij de kantonrechter. Indien NHL Stenden Hogeschool niet binnen de gestelde termijn heeft geantwoord op het verzoek van Betrokkene, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend. Indiening van het verzoekschrift hoeft niet door een advocaat te geschieden.

B. Bezwaar en beroep

Indien NHL Stenden Hogeschool afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of NHL Stenden Hogeschool heeft het verzoek van de Betrokkene afgewezen, en het besluit van NHL Stenden Hogeschool is aan te merken als een besluit van een bestuursorgaan in de zin van artikel 6 lid 4 van de Awb, heeft de Betrokkene de mogelijkheid een bezwaarschriftprocedure te starten. Een bezwaarschriftprocedure moet altijd gestart worden binnen 6 weken na bekendmaking van een besluit van NHL Stenden Hogeschool. Tegen de beslissing op bezwaar, staat beroep open bij de rechtbank.

C. Verzoek tot handhaving bij toezichthoudende autoriteit

Indien NHL Stenden Hogeschool afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of NHL Stenden Hogeschool het verzoek van de Betrokkene heeft afgewezen, heeft de Betrokkene de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit, dan wel om een belangenorganisatie namens hem op te laten treden.

9. Tot slot

Dit beleid is tot stand gekomen na advies van

- De bestuursstaf, in het bijzonder de afdeling Juridische Zaken
- De Data Protection Council van NHL Stenden Hogeschool
- Het hogeschoolberaad.

Het is vastgesteld door het CvB van NHL Stenden Hogeschool d.d. 1 oktober 2019, na instemming van de HMR d.d. 24 september 2019.

Een review van het beleid maakt onderdeel uit van de tweejaarlijkse plan-do-check-act cyclus van NHL Stenden Hogeschool. Daarin is ook een controle op de effectiviteit van de maatregelen opgenomen.

Aanpassingen van dit beleid worden aangekondigd via intranet. De meest recente versie staat gepubliceerd op een internetpagina van de instelling.

Voor vragen of opmerkingen met betrekking tot dit beleid kunt u terecht bij de FG.

10. Bijlagen

10.1. De dataregisters: welke persoonsgegevens, waar en waarom?

Artikel 30 van de Avg verplicht ons tot het opstellen en onderhouden van een ‘register van verwerkingsactiviteiten’. Daarmee laat een organisatie zien welke persoonsgegevens onder haar verantwoordelijkheid worden verwerkt. NHL Stenden Hogeschool geeft invulling aan deze verplichting met een dataregister[10] voor iedere doelgroep (in de termen van de Avg: ‘categorie van betrokkenen’).

NHL Stenden heeft dataregisters opgesteld voor de volgende groepen. Tussen haakjes de gemandateerd verantwoordelijke directeuren (situatie van november 2018).

- Studenten (Angela Schat)
- Cursisten (Soon Hee Santema)
- Leads (Rob Koning)
- Alumni (Rob Koning)
- Medewerkers in loondienst (Alette Hospers)
- Medewerkers niet in loondienst (Alette Hospers)
- Externe relaties (Rob Koning)
- Gasten van het Stenden University Hotel (Thulani Xhali)

Voor ieder dataregister heeft het cvb een gemandateerd verantwoordelijke aangewezen, een directeur die verantwoordelijk is voor de naleving en het onderhoud van het dataregister. Hun namen staan hierboven tussen haakjes[11].

Het dataregister is in de kern een matrix waarin een uitputtende opsomming van de verwerkte persoonsgegevens wordt afgezet tegen de plekken waar deze persoonsgegevens ‘wonen’: bij externe verwerkingsverantwoordelijken, zoals de Belastingdienst, bij verwerkers zoals Youforce Raet en bij de verschillende organisatieonderdelen van NHL Stenden Hogeschool.

De naleving van de dataregisters maakt deel uit van de door de Bestuursstaf uitgevoerde privacyaudit die tweemaal per jaar wordt uitgevoerd. Voorts zijn de dataregisters nadrukkelijk onderwerp van gesprek in de rapportagegesprekken met alle directeuren.

De leden van de Data Protection Council hebben binnen hun Academie, Dienst of Verbindingseenheid een signalerende en informerende taak als het om de dataregisters gaat.

Alle dataregisters zijn te vinden via https://privacy.nhlstenden.com/

10.2. Procedure 'Hoe kunnen betrokkenen hun rechten uitoefenen?'

Betrokkenen die hun rechten willen uitoefenen kunnen zich aanmelden bij een daartoe ingericht online loket[12]. Als het om een verzoek om inzage gaat, ontvangen ze per omgaande het voor hen geldende dataregister. Als de betrokkene meer wil weten dan *welke* gegevens van hem worden verwerkt en bij andere verzoeken, vindt binnen twee weken een gesprek plaats met een vertegenwoordiger van de Data Protection Council[13]. Tijdens dat gesprek moet de betrokkene zich kunnen identificeren. Het doel van het gesprek is tweeledig: de-escalatie en specificatie. Als vervolgens duidelijk is wat de betrokkene precies wil, gaat het verzoek (bijvoorbeeld een verzoek om inzage) naar de

[10] Het instrument is ontwikkeld onder leiding van Ludo Cuijpers van Leeuwenborg Opleidingen en wordt onder meer ook gebruikt bij Fontys Hogescholen en de Open Universiteit. De Autoriteit Persoonsgegevens heeft zich waarderend over het instrument uitgelaten.
[11] Situatie op 1 september 2018.
[12] Zolang dat loket niet is ingericht, worden de verzoeken rechtstreeks aan het College van Bestuur gericht.
[13] Actie: per locatie iemand aanwijzen die dit wil doen.

gemandateerde verantwoordelijke van het betreffende dataregister. Die zorgt ervoor dat de betrokkene binnen vier weken gebruik heeft kunnen maken van zijn recht en – in dit voorbeeld – inzage heeft gekregen in zijn gegevens. Zie Hoofdstuk 8 voor de rechten van de betrokkene.

Verzoeken om gegevenswissing van leads en alumni worden op basis van een check op het e-mailadres zonder nader onderzoek ingewilligd.

Alle verzoeken alsmede de afhandeling daarvan worden gedocumenteerd en gedurende twee jaar bewaard in een centraal register.

Betrokkenen die niet tevreden zijn over de manier waarop hun verzoek is afgehandeld, kunnen contact opnemen met de FG. De FG houdt toezicht op het bestaan, de opzet en de werking van deze procedure.

10.3. Procedure Data Protection Impact Assessments

Een Data Protection Impact Assessment is een systematische beoordeling van de noodzaak en de risico's van een (voorgenomen) verwerking van persoonsgegevens. De Avg schrijft de DPIA met name voor als er sprake is van

a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking (…)

b) een grootschalige verwerking van bijzondere categorieën van persoonsgegevens (…)

c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.[14]

De voorschriften van de Autoriteit Persoonsgegevens lijken een breder gebruik van de DPIA te impliceren. Een DPIA is altijd aanbevelenswaardig en levert nuttige informatie voor het dataregister, voor de eventueel af te sluiten verwerkersovereenkomst en voor het vereiste niveau van informatiebeveiliging.

Binnen NHL Stenden Hogeschool wordt de DPIA daarom uitgevoerd

- voor alle grote, essentiële verwerkingen van persoonsgegevens (herhaling om de drie jaar)
- voor alle nieuwe systemen of processen
- voor alle apps en andere op Academie- of afdelings- of opleidingsniveau ingezette digitale toepassingen
- voor onderzoeksprojecten waarin persoonsgegevens worden verwerkt wordt een DPIA uitgevoerd als een of meer van de volgende criteria van toepassing zijn.
    - internationaal;
    - samenwerking met andere instellingen;
    - verwerking van bijzondere persoonsgegevens;
    - verwerking van gegevens van meer dan 1000 respondenten;
    - master- of PhD-onderzoek.

Het Initiatief voor een DPIA wordt genomen door de systeemeigenaar en/of leidinggevende en/of hoofdonderzoeker. De uitvoering vindt plaats onder leiding van de Corporate Security Officer. De uitkomsten worden gedocumenteerd, evenals de opvolging van de daaruit voortvloeiende adviezen.

De controle op de naleving van de uitvoering van DPIA maakt deel uit van de pricacy-audit die tweemaal per jaar wordt uitgevoerd. Het onderwerp wordt geagendeerd in de rapportagegesprekken die de directeuren met het cvb voeren. De leden van de DPC hebben binnen het Academie, Dienst of Verbindingseenheid een signalerende en informerende rol als het om de DPIA's gaat. De rapportage over het uitvoeren van de DPIA's maakt deel uit van het jaarverslag van de FG.

Er wordt jaarlijks een algemene voorlichtingsbijeenkomst over het instrument van de DPIA gehouden.

[14] Avg, Artikel 35, lid 3a.

10.4. Procedure Privacy by design

'Gegevensbescherming door ontwerp (*privacy by design*) houdt in dat de voor verwerking gebruikte mechanismen zo zijn ontworpen dat ze zoveel mogelijk rekening houden met de privacy van de betrokkenen en de vereisten uit de Avg. Een systeem dat hieraan voldoet zou dus bijvoorbeeld knoppen ingebouwd kunnen hebben waarmee betrokkenen inzage in hun persoonsgegevens kunnen krijgen. Ook andere maatregelen, gericht op bijvoorbeeld het minimaliseren van de hoeveelheid persoonsgegevens en het zo spoedig mogelijk pseudonimiseren van persoonsgegevens vallen hieronder'[15].

Privacy by Design is vanuit NHL Stenden Hogeschool een ontwerpvereiste voor systemen en processen en een randvoorwaarde bij inkoop en aanbesteding.

Privacy by Design sluit op voorhand bepaalde informatie of gegevens uit, selecteert alleen relevante personen en gegevens, verwijdert (deel)informatie die niet langer nodig is en vernietigt persoonsgegevens zodra ze niet langer nodig zijn[16].

Concrete voorbeelden van privacy by design zijn :

- Een knop 'Mijn gegevens'
- Een goede autorisatiestructuur
- De mogelijkheid om gegevens geautomatiseerd en gedifferentieerd te verwijderen (aan het einde van de bewaartermijn bijvoorbeeld)
- Mogelijkheid voor gedetailleerde logging
- De juiste informatie op het juiste scherm (indien bijvoorbeeld het BSN-nummer gebruikt *moet* worden in het systeem, zit dat diep verborgen en is het alleen zichtbaar voor die gebruikers voor wie het zichtbaar moet zijn)

De dienst DLWO zorgt voor een technische uitwerking van de ontwerpeisen die voortvloeien uit Privacy by Design en voor een jaarlijkse update daarvan.

De afdeling Inkoop is verantwoordelijk voor het opnemen van de eis van privacy by design in het inkoop- een aanbestedingsproces.

De leden van de DPC hebben binnen hun Academie, Dienst of Verbindingseenheid een signalerende en informerende rol als het om Privacy by Design gaat.

De FG en de SO verzorgen jaarlijks een voorlichtingsbijeenkomst over Privacy by Design.

Privacy by Default (gegevensbescherming door standaardinstellingen) is een verwant begrip: standaard moeten de keuzemogelijkheden op de meest privacyvriendelijke manier zijn ingesteld. Dit is binnen NHL Stenden Hogeschool met name een aandachtspunt binnen de omgeving van Office365.

De dienst DLWO is verantwoordelijk voor de privacyvriendelijke instelling van de binnen de hogeschool gebruikte systemen en voor de voorlichting daarover.

[15] Engelfriet, Meij en Kager (2017), p. 119.
[16] Onleend aan een presentatie van Dr. Jaap-Henk Hoepman op Stenden Hogeschool op 15 februari 2017.

10.5. Procedure Verwerkersovereenkomsten[17]

Overeenkomstig Artikel 28 lid 3 van de Avg sluit NHL Stenden Hogeschool verwerkersovereenkomsten af met verwerkers, partijen die ten behoeve van ons persoonsgegevens verwerken.

De verantwoordelijkheid voor het afsluiten en het beheer van de verwerkersovereenkomsten ligt bij de afdeling Inkoop of, bij contracten onder €50.000, bij de budgethouder.

NHL Stenden Hogeschool hanteert in principe de modelovereenkomst die is ontwikkeld door SURF. Kleine door de leverancier gewenste afwijkingen worden ter beoordeling voorgelegd aan de FG. Substantiële afwijkingen worden voorgelegd aan de privacy-jurist van de Bestuursstaf. De verwerkersovereenkomsten worden ondertekend door het cvb of – bij contracten onder €50.000 – door de budgethouder.

De controle op de naleving van de verplichting om verwerkersovereenkomsten te sluiten maakt deel uit van de privacyaudit die twee maal per jaar wordt uitgevoerd door de Bestuursstaf. Die controle vindt plaats aan de hand van de overzichten uit de dataregisters.

De FG organiseert in samenwerking met de privacyjurist jaarlijks een informatiebijeenkomst over verwerkersovereenkomsten.

De verwerkersovereenkomsten komen nadrukkelijk aan de orde in de rapportagegesprekken van de directeur Finance, Procurement & Control met het cvb.

10.6. Vergroting awareness

De bescherming van persoonsgegevens zit in informatiesystemen, die ontworpen zijn volgens de eisen van Privacy by Design, in procedures en mechanismes zoals onder meer beschreven in de dataregisters, maar vooral in het menselijk handelen. Als medewerkers en andere betrokkenen zich onvoldoende bewust zijn van het belang van privacy, is het opstellen van privacybeleid dweilen met de kraan open.

In de aanloop naar de fusie is de awareness-site http://datacare.nhlstenden.com gelanceerd. In 2018 hebben de SO en de FG gezamenlijk minstens vijfentwintig workshops en voorlichtingsbijeenkomsten gegeven. Dat aanbod is deels opgenomen in het programma van de ProfessionaliseringsAcademie. Scholing vindt plaats op drie niveaus:

- Open inschrijving voor zowel onderwijzend als ondersteunend personeel
- Training voor teams
- Scholing van de leden van de Data Protection Council. Deze scholing straalt uit naar de Academies, Diensten en Verbindingseenheden die zij vertegenwoordigen. Het uitdragen van het belang van een zorgvuldige omgang met persoonsgegevens en de voorlichting daarover is een belangrijke taak van de leden van de DPC.

Een module ‘privacy en security in een data-gedreven maatschappij’ wordt onder verantwoordelijkheid van de Dienst HRM opgenomen in de management-development-trajecten. De aandacht voor de bescherming van persoonsgegevens is een expliciet punt van aandacht in de rapportagegesprekken van alle directeuren met het cvb.

Via intranet zal de komende twee jaar minimaal één maal per maand aandacht gevraagd worden voor het thema privacy.

[17] Mandatering en procedure waren op het moment van indienen van dit plan nog niet vastgesteld.

De bewustwordingscampagne richt zich op alle categorieën betrokkenen, waarbij de medewerkers en de studenten het eerst aan de beurt komen.

Deze campagne wordt ondersteund door de dienst Marketing en Communicatie.

10.7. Privacy en internationalisering

De privacywetgeving stelt strenge eisen aan de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Regio.

De Avg is van toepassing op alle Europese studenten en medewerkers van NHL Stenden Hogeschool, waar die zich ook bevinden. De Avg is eveneens van toepassing op studenten van buiten de EER die in Nederland studeren, zoals de zogenaamde '60 EC students'.

Overeenkomstig artikel 46, lid 2c baseert NHL Stenden Hogeschool de doorgifte van persoonsgegevens naar de landen waarin onze International Branch Campuses zijn gevestigd op 'passende waarborgen', in het bijzonder op de 'standaardbepalingen inzake gegevensbescherming die door de (Europese) Commissie (…) zijn vastgesteld'. Met alle vier de IBC's heeft NHL Stenden Hogeschool deze zogenaamde modelcontracten of 'model clauses' afgesloten. Daarmee heeft de doorgifte van persoonsgegevens in het kader van de Grand Tour™ een wettelijke grondslag[18].

De doorgifte van persoonsgegevens naar landen buiten de EER in het kader van stages of exchange wordt gebaseerd op het nakomen van een in het belang van de betrokkene afgesloten overeenkomst (Artikel 49, lid 1).

De terugkoppeling van gegevens van aangemelde internationale studenten naar agenten buiten de EER, vindt zijn grondslag in de toestemming die deze studenten hiervoor hebben gegeven.

Hoewel de International Branch Campuses juridisch gezien hun eigen verantwoordelijkheid hebben en zich aan de voor hen van toepassing zijnde wetgeving dienen te houden, ligt het in de rede om, los van de onderscheiden verantwoordelijkheden en verschillende wettelijke regiems, binnen de 'NHL Stendengroep' wereldwijd op dezelfde manier met persoonsgegevens om te gaan. Met het oog daarop heeft NHL Stenden Hogeschool een Privacy Guideline, als een interne gedragscode voor de omgang met persoonsgegevens op en tussen de sites (zie bijlage 10.9).

De verantwoordelijkheid voor het naleven van de Europese modelcontracten ligt bij het cvb. Deze verantwoordelijkheid is gemandateerd aan de Directeur International Affairs.

De verantwoordelijkheid voor naleven van de Privacy Guideline ligt bij de General Managers van de IBC's.

De FG ziet toe op de afstemming van de Privacy Guideline op de Avg en bevordert de awareness op de International Branch Campuses.

10.8. Privacy en onderzoek

Binnen een instelling voor hoger onderwijs zoals NHL Stenden Hogeschool wordt veel onderzoek gedaan. In veel gevallen worden in het kader van dat onderzoek persoonsgegevens van de onderzoekssubjecten verwerkt. Omdat ieder onderzoek verschillend is, leent de categorie onderzoekssubjecten zich niet voor een dataregister, zoals die is opgesteld voor de andere

[18] Hieraan ligt onder meer een uitvoerig advies van Duthler Associates ten grondslag *Doorgifte persoonsgegevens aan derde landen* van 17 augustus 2017.

doelgroepen. Voor het in kaart brengen van de in het kader van de diverse onderzoeken verwerkte persoonsgegevens wordt het instrument SmartPIA ingezet.

NHL Stenden Hogeschool ontwikkelt met gebruikmaking van goede voorbeelden van elders zo spoedig mogelijk een privacy-gereedschapskist voor onderzoek.

Die kist bevat idealiter de volgende gereedschappen:

- Een beknopt privacyprotocol voor de verschillende typen onderzoekers, van de bachelorstudent tot de PhD.
- Een ethische commissie, eventueel in samenwerking met een of meer andere onderwijsinstellingen.
- Een veilige, door NHL Stenden ter beschikking gestelde tool voor het doen van online onderzoek
- Een repository voor onderzoeksdata, eventueel in samenwerking met een of meer andere onderwijsinstellingen.
- Een platform voor het uitzetten van en meedoen aan intern onderzoek onder studenten en medewerkers.
- Een stappenplan onderzoek.

De verantwoordelijkheid van de naleving van de privacyregels voor onderzoek ligt bij de Directeur R&D Onderwijs en Onderzoek.

De ontwikkeling van de privacy-gereedschapskist is de taak van de daarvoor in het leven geroepen commissie Onderzoek en Privacy.

10.9. International Privacy guideline NHL Stenden

Privacy guideline NHL Stenden University of Applied Sciences

Purpose
By issuing this guideline NHL Stenden University shows how it acts in accordance with the legal requirements and protects the personal data of members of staff, students and third parties. The guideline describes the approach we take to privacy and is based on Dutch law.

Scope
The guideline covers the processing of all personal data by or on behalf of NHL Stenden University (all locations).

Definitions
Personal data: all data concerning an identified or identifiable natural person.

Processing of personal data: all actions or series of actions related to personal data, including in all cases the collection, registration, classification, storage, editing, amendment, retrieval, viewing, usage, issue by means of forwarding, distribution or any other form of provision, uniting, placing in mutual relation, as well as the protection, exchange or destruction of data.

Controller: the natural person, legal person or any other person who or administrative body that, acting alone or in association with others, lays down the purpose and the means of processing personal data.

Processor: the person who processes the personal data for the controller, without being subject to the controller's direct authority.

Data subject: the person to whom the personal data relates.

Data protection officer (DPO): The position of the DPO is laid down by law. He oversees the processing of personal data and can make recommendations to improve how the personal data is processed.

PCP network: This network serves as a sounding board for the Data Protection Officer (DPO) of Stenden and has three functions: to inform, identify and advise. The network comprises representatives of the staff departments, all service groups, the examination committees' platform and all Schools. The Information Security Officer and the Information Manager are members of the PCP network in that capacity.

Privacy governance
Data processing carried out by or on behalf of Stenden University is reported to the Data Protection Officer and published on the intranet.
The adopted Stenden policy forms the framework for this. The key terms are transparency and purpose limitation. We say what we do and we do only what is necessary.
Privacy issues are communicated via the privacy portal at iStenden.

How do we obtain the data?
Data is only collected:

- directly or indirectly (via Studielink, agents, social media) from the data subject through the channels provided for by law.

What do we do with the data?
Personal data is processed exclusively:
- if necessary for education or research, in particular to facilitate education for students;
- if necessary for the purpose of the employer-employee relationship;
- if it has been given to the DPO (stating the legal grounds);
- if the data subject has given explicit consent for this to be done;
- if the vital interests of the data subject are at stake.

What are our general principles?
The personal data processed by NHL Stenden University is correct and relevant and is legitimately and legally processed.
NHL Stenden does not collect any more data than what is necessary (data minimisation).
Employees of NHL Stenden are asked to provide a copy of their passport when they join the organisation; on no occasions other than that.
NHL Stenden does not keep data for longer than necessary. This is based on the Selection List for Universities of Applied Sciences (*Selectielijst hogescholen*).
NHL Stenden collects data only for a precisely defined purpose that is related to the institution's social mandate (purpose limitation);
NHL Stenden never passes on data to third parties unless:
- it is legally obliged to do so;
- the data subject has given explicit consent for this to be done.

A supporting document or copy of the diploma is only issued to or on the request of the data subject, for example. E-mail details of students or members of staff are issued to the research agencies for quality surveys (National Student Survey (NSE), staff satisfaction survey).
To the extent that NHL Stenden has personal data processed by third parties (processors), a processor's agreement is entered into with the processors laying down responsibility for data breaches.
NHL Stenden never sells personal data and does not make it available for commercial purposes in any way whatsoever.
NHL Stenden effectively protects the personal data in accordance with the current state of technology. Personal data is encrypted where necessary and possible.

Special categories of personal data
NHL Stenden does not process any special personal data other than
- nationality (in connection with the internationalisation policy);
- religion (exclusively for the Education in Primary Schools programme in connection with assigning the placements by denomination);
- medical data (if necessary for assistance in the context of the Study and Disability scheme and for the safety of students during the Grand Tour™.

Forwarding of data to third countries
NHL Stenden Netherlands does not exchange personal data with the international branch campuses unless:
- this is necessary for educational purposes;
- there is no alternative owing to the obligations under the employment contract;
- the vital interests of the data subject are at stake.

Rights and obligations of data subjects
Data subjects have the right to view and correct their data. They can also object to the registration of certain data.
For matters concerning the protection of their personal data they can lodge a complaint with the DPO. Students can also lodge a complaint via ELF (single point of contact facility).
All persons at Stenden are obliged to report possible personal data protection breaches to the DPO (responsible disclosure).
Managerial staff and members of the PCP network are obliged to report the processing of personal data to the DPO.

To conclude
If in doubt, the DPO should be consulted.
The Data Protection Officer of NHL Stenden University of Applied Sciences is Willem Bakker.
willem.bakker@stenden.com | ✆ +31 6 15 31 95 03

10.10. Gevolgen implementatie van dit beleid

Extra kosten in of vanaf 2019		Beleidsplan	Ten laste van
Personeel			
Facilitering DPC	Ca. 1,5 fte	Eerstelijns privacyzorg op de werkvloer	Academies en afdelingen
Privacy officer	0,5 fte	Tweedelijns ondersteuning	Bestuursstaf
Rechtenloket	0,1 fte	Facilitering rechten betrokkenen	Bestuursstaf
Data management support	0,4 fte	Ondersteuning bij invullen SmartPIA	Mediatheek
Materieel			
Awareness medewerkers en studenten	N.t.b.	Kosten promotiecampagnes	CvB
Informatiebeveiliging	N.t.b.	Tooling	DLWO
Privacy by design	N.t.b.	Vervanging legacysystemen	DLWO
Onderzoek	N.t.b.	Tooling	DLWO
Internationalisering	N.t.b.	Reis- en verblijfkosten	Internationalisering

Personele inzet te realiseren door interne verschuivingen, gesteund en geïnitieerd door het cvb. Materiële inzet te bekostigen uit de reguliere begroting van de meest in aanmerking komende afdeling of verbindingseenheid. Indien nodig stelt het cvb hiervoor maximaal € 75.000 ter beschikking.

Zonder de hierboven voorgestelde, minimale implementatie en de daarmee gemoeid zijnde kosten (personeel en materieel, incidenteel en structureel), zal de **accountant** in 2019/2020:
a) kritische vragen stellen in hoeverre de materiële risico's die het niet naleven van de Avg met zich meebrengen zijn afgedekt[19]. Het cvb is in de zin van de Avg immers de verwerkingsverantwoordelijke, die het doel en de middelen van de verwerkingen onder paraplu van NHL Stenden Hogeschool vaststelt;
b) vragen stellen hoe uit governance, bestedingspatronen en aanwezige maatregelen en procedures blijkt dat privacy voor NHL Stenden een 'topprioriteit' is (zie § 1 van het beleidsplan);
c) aandacht vragen voor het feit dat veel collega-hogescholen op dit terrein aanzienlijk grotere uitgaven en inspanningen doen.

Wat als	*Geen kostenverhogende implementatie*	*Implementatie zoals hier voorgesteld*
Geen majeure incidenten	Alleen lastige vragen accountant, HMR en RvT	'Goed bezig': de privacy hoeft ons in ieder geval niet wakker te houden.
Wel majeure incidenten	Serieus probleem, onder vergrootglas AP, mogelijk een waarschuwing of een boete, veel negatieve publiciteit, vertrouwensbreuk met stakeholders, mogelijk een dip in de instroom.	Probleem, maar wij hebben een duidelijk verhaal: beleid is aanwezig of in opbouw, het cvb kan adequaat reageren en een vertrouwensbreuk voorkomen. De publiciteit heeft geen of maar een beperkte negatieve impact.

[19] Meest recente boete (nog onder de 'oude' wetgeving!): €600.000 voor Uber. De naleving van de privacywetgeving zal in toenemende mate een onderwerp worden voor accountants, medezeggenschapsraad en Raad van Toezicht.

Actielijst

1. Het **cvb** pakt zijn rol als verwerkingsverantwoordelijke proactief op (privacy & security als onderwerp op vergaderingen, in plangesprekken en in het overleg met RvT en HMR).
2. Het **cvb** vraagt de directeuren om hun vertegenwoordigers in de DPC te faciliteren met minimaal 0.1 fte op jaarbasis.
3. Het **cvb** stelt vanuit het eigen budget in 2019 een bedrag beschikbaar voor niet personele out-of-pocketkosten voor privacy van maximaal €75.000.

4. **DLWO** plant en spreidt de uitgaven voor de aanpassing of uitbreiding voor systemen in verband met de eisen van privacy by design over 2019 en 2020 en verder.
5. **DLWO** draagt zorg voor encryptie, monitoring, logging en mobile devicemanagement (conform eerdere besluiten van de cvb's van NHL en Stenden).

6. De **mediatheek** zorgt voor een structurele hulplijn voor de invulling van SmartPIA (datamanagement support).

7. De **bestuursstaf** stelt een privacy officers aan voor maximaal 0,5 fte (assisteert bij ontwikkeling werkinstructies en protocollen, functioneel beheer SmartPIA, meewerkend voorman of –vrouw bij deelprojecten gerelateerd aan implementatie privacybeleid (autorisaties, bewaartermijnen en facilitering rechten betrokkenen).
8. De **bestuursstaf** verzorgt in 2019 een inventariserende audit op het gebied van de naleving van de dataregisters, overige privacywetgeving en securityvoorschriften.
9. De **bestuursstaf** rapporteert in R4, R8 en R12 aan het cvb over de voortgang van bovenstaande actiepunten.