

Datum 27 mei 2025
Auteur Linda Dijkstra
Versie 2.1
Status definitief

Privacybeleid HvHL



Inhoud

1.	Inleiding	5
1.1	Reikwijdte	5
1.2	Privacy	6
1.3	Instellingsplan	6
1.4	Doelstellingen	7
2.	Uitgangspunten	9
2.1	Grondslag en doelbinding	9
2.2	Rechtmatigheid, behoorlijkheid, transparantie	9
2.3	Dataminimalisatie	10
2.4	Juistheid	10
2.5	Bewaartermijn	10
2.6	Integriteit en vertrouwelijkheid	10
3.	Aangrenzende gebieden	11
3.1	Security	11
3.2	Wet- en regelgeving	11
3.3	Beleid	14
4.	Governance en organisatorische borging gegevensbescherming	15
4.1	Basisregels	15
4.2	3 lines model	15
4.3	Rollen en verantwoordelijkheden	16
4.4	P&C cyclus	18
5.	Rechtmatige en zorgvuldige verwerking van persoonsgegevens	19
5.1	Rechtmatige en zorgvuldige verwerking	19
5.2	Organisatorische maatregelen	19
5.2	Technische maatregelen	20
5.3	Herkennen van situaties en risico's	20
5.4	Supporten van privacybewust gedrag	21
5.5	Privacybewust handelen en gedrag	21
5.6	Privacybeleid en -reglement	21



6.	Datalekken	23
7.	Rechten van Betrokkenen	24
7.1	Melding aan Betrokkene	24
7.2	Termijn	24
7.3	Identiteit Betrokkene	24
7.4	Minderjarigen	24
8.	Implementatie beleid	25
8.1	Verdeling van de verantwoordelijkheden	25
8.2	Gegevensbescherming in de organisatie	25
8.3	Data Protection Office (DPO)	26
8.4	Privacy/Security overleg	26
8.5	Bewustwording en training	26
8.6	Controle en naleving	26
9.	Uitvoering van beleid	27



1. Inleiding

Het op een juiste, transparante en veilige wijze verwerken van persoonsgegevens is de eindverantwoordelijkheid van het College van Bestuur (CvB) van HvHL. HvHL verwerkt voortdurend en in grote hoeveelheden persoonsgegevens. Die verwerking is met name noodzakelijk in verband met het verzorgen van het onderwijs en de daarbij behorende (bedrijfs)processen. Onzorgvuldig gebruik en misbruik van persoonsgegevens kan schade berokkenen aan studenten en medewerkers (hogeschoolgemeenschap) en relaties, en daarmee ook aan HvHL zelf.

Met het stellen van regels, het hanteren van procedures, het verzorgen van scholing en voorlichting wordt vorm en inhoud gegeven aan die verantwoordelijkheid. Het werken met veilige systemen en het hanteren van een up-to-date verwerkingenregister leveren samen met privacy bewuste medewerkers en studenten een bijdrage aan de bescherming van de rechten en vrijheden van de hogeschoolgemeenschap en haar relaties.

De wijze waarop HvHL persoonsgegevens verwerkt is vastgelegd in dit privacybeleid, een gedragscode voor de digitale werkomgeving en een gedragscode voor gegevensbescherming. Het privacybeleid is het kader waarin is aangegeven aan welke principes HvHL zich houdt.

Afkortingen

Afkorting	Omschrijving
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
CvB	College van Bestuur
DPO	Data Protection Office
ESG	European Sustainable Goals
IT	Informatie Technologie
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek

1.1 Reikwijdte

Dit beleid heeft betrekking op het verwerken van de persoonsgegevens van alle betrokkenen binnen HvHL, zoals studenten, medewerkers, relaties (inhuur/outsourcing), partners en bezoekers, alsmede op alle andere betrokkenen van wie HvHL persoonsgegevens verwerkt.

Complementair aan de bescherming van persoonsgegevens (privacy) is het beleidsterrein van de informatieveiligheid, waarbij het gaat om de beschikbaarheid, integriteit en vertrouwelijkheid van data. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het CvB en de medewerkers van HvHL spelen een belangrijke rol bij het waarborgen van de privacy. Het management van HvHL laat met de uitvoering en navolging van dit beleid zien dat

zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van HvHL.

1.2 Privacy

Binnen HvHL wordt privacy als volgt gedefinieerd:

Privacy is een grondrecht en een voorwaarde om vrij te zijn in wie je bent en wat je doet. Privacy gaat erover dat mensen regie houden over hun gegevens. Privacy beschermt personen of groepen af van bespieding en beïnvloeding.

Informatieprivacy is het recht om enige controle te hebben over hoe uw persoonlijke informatie wordt verzameld en gebruikt.

HvHL omarmt privacy op een gestructureerde wijze om daarmee te voldoen aan wet- en regelgeving. Hiervoor is het HvHL privacy management framework geïmplementeerd.



Figuur 1: Privacy management framework

1.3 Instellingsplan

In het instellingsplan staat beschreven hoe HvHL de toekomst in gaat. Aan de missie en visie levert Privacy haar eigen bijdrage. In de houding en het gedrag van de medewerkers, zoals die verwoord zijn in de kernwaarden speelt het beschermen van de Privacy van betrokkenen een belangrijke rol.

Missie

Bijdragen aan de wereld van morgen

Het waarborgen van privacy in een steeds meer digitaliserende samenleving is veel breder dan alleen het beschermen van persoonsgegevens. Privacy kan ook in het gedrang komen in praktijksituaties waar geen persoonsgegevens worden gebruikt. Denk hierbij aan het gebruik van big data, waarbij vaak geen persoonsgegevens worden gebruikt, maar wel door de uitgestrektheid van de data zo veel inzicht is in de profielen en bewegingen van individuen dat het gebruik grote gevolgen kan hebben.



Door verantwoord om te gaan met digitalisering kunnen we de kansen die digitalisering biedt aan en dragen wij er zorg voor dat we de privacy van betrokkenen kunnen waarborgen.

Visie

Experts in duurzame transitie

Door het toenemende energieverbruik door de toepassing van IT en het gebruik van schaarse materialen voor apparatuur, wordt de milieu-impact van de digitale transitie vergroot. Daarom vinden wij het belangrijk om spaarzamer met digitale data om te gaan en maximale efficiency na te streven bij digitale toepassingen. Zo weinig mogelijk data verzamelen en verspreiden verkleint niet alleen de kans op het in gedrang komen van de privacy, maar draagt ook bij aan duurzaamheid.



Figuur 2: ESG en Privacy

1.4 Doelstellingen

Betrokkenen moeten erop kunnen vertrouwen dat HvHL zorgvuldig en veilig met persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve digitale voorzieningen, globalisering en de digitalisering stellen andere eisen aan de bescherming van persoonsgegevens en privacy. HvHL is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Dit privacybeleid heeft als doel de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

De gegevens die betrekking hebben op een betrokkene dienen beschermd te worden tegen onrechtmatig en ongeautoriseerd gebruik, en tegen misbruik. De rechten en vrijheden van betrokkenen met betrekking tot de verwerking van persoonsgegevens zijn fundamentele

rechten. Dat brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig behoren te zijn bij HvHL.

- **Bieden van een kader:**

Dit 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.

- **Stellen van normen:**

De basis voor de beveiliging van persoonsgegevens zijn ISO 27001¹, ISO 27002.² en ISO 27701³. Het SURF Juridisch Normenkader (Cloud)services³ wordt gehanteerd als best practice voor cloud services en andere outsource-contracten. Bijstellingen in deze normstellingen worden periodiek doorgevoerd.

- **Borgen van de verantwoordelijkheid:**

Door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor de hele organisatie, en door implementatie van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen. Zodoende kan het CvB daadwerkelijk zijn eindverantwoordelijkheid nemen.

- **Voldoen aan wet- en regelgeving**

Door de Nederlandse en Europese wet- en regelgeving als uitgangspunt te nemen en te respecteren.

- **Bewustwording**

Belangrijk doel is het creëren van het besef in de organisatie dat de bescherming van (persoons)gegevens belangrijk en noodzakelijk is en dat daarbij naleving van de relevante wet- en regelgeving voorop moet staan. Onwetendheid of onbekwaamheid brengt grote risico's met zich mee. Die risico's zijn niet beperkt tot een enkel individueel lid van de hogeschoolgemeenschap maar strekken zich uit tot heel HvHL met het CvB als eindverantwoordelijke.

¹ Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging

² Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging

³ Voluit: NEN-ISO/IEC 27701: Uitbreiding op ISO 27001 met maatregelen voor de bescherming van privacygevoelige informatie



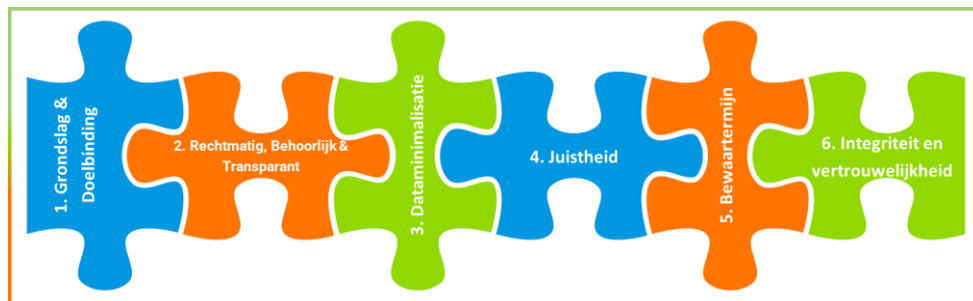
2. Uitgangspunten

HvHL gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. HvHL houdt zich daarbij aan de uitgangspunten die hierna staan beschreven. Deze uitgangspunten zijn verder uitgewerkt in de “Gedragscode voor de digitale werkomgeving”, de “Gedragscode voor gegevensbescherming” en de “Procedure rechten van betrokkenen”.

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij wordt een goede balans aangebracht tussen het belang van HvHL om persoonsgegevens te verwerken en het belang van betrokkenen om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

Om hieraan te voldoen hanteert HvHL de volgende principes:

1. Grondslag en doelbinding;
2. Rechtmatig, behoorlijk en transparant;
3. Dataminimalisatie;
4. Juistheid;
5. Bewaartermijn;
6. Integriteit en vertrouwelijkheid.



Figuur 3: Principes voor de verwerking van persoonsgegevens

2.1 Grondslag en doelbinding

HvHL zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

2.2 Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Met dit privacybeleid, de gedragscode voor gegevensbescherming, de gedragscode voor de digitale werkomgeving, de privacyverklaring en het register van verwerkingsactiviteiten beoogt HvHL duidelijkheid te geven over de wijze waarop ze met persoonsgegevens omgaat.



De inbreuk op de belangen van de betrokkene moet in verhouding zijn met het doel van de verwerking (toereikend, ter zake dienend en niet bovenmatig).

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokkenen zoveel mogelijk beperkt.

2.3 Dataminimalisatie

HvHL verwerkt de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

2.4 Juistheid

De (persoons)gegevens die HvHL verwerkt zijn nauwkeurig en worden waar nodig actueel gehouden.

2.5 Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens is nodig om de taken van HvHL goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Zie hiervoor ook het bewaarbeleid.

2.6 Integriteit en vertrouwelijkheid

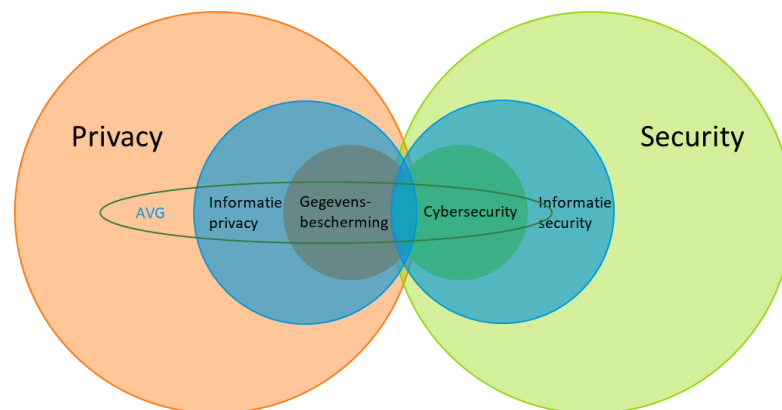
HvHL gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt HvHL voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

In het geval van samenwerking met externe partijen, waarbij sprake is van verwerking van persoonsgegevens, maakt HvHL afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan wet- en regelgeving.



3. Aangrenzende gebieden

Privacy staat niet op zichzelf, het is een onderdeel van de gegevensbescherming binnen HvHL. Gegevensbescherming wordt gevormd door de samenwerking tussen privacy en security met bijbehorend beleid, wet- en regelgeving.



Figuur 4: Samenwerking Privacy & Security

3.1 Security

Security omvat elk aspect van beveiliging, van fysiek (bijv. gebouwen, laptops, persoonlijke veiligheid, etc.) tot logisch (bijv. cyberbeveiliging). In het informatiebeveiligingsbeleid worden de regels beschreven waaraan HvHL en haar medewerkers moeten voldoen m.b.t. security.

3.1.1 Informatie security

Informatie security staat voor de bescherming van gegevens of informatiebronnen in elk formaat, d.w.z. fysiek (bijv. papier) en elektronisch (bijv. op een computer).

3.1.2 Cybersecurity

Cybersecurity is de bescherming van elke elektronische vorm van gegevens of informatie, ongeacht de context van de levenscyclus van gegevens.

3.2 Wet- en regelgeving

Op het privacybeleid is de volgende wet- en regelgeving van toepassing.

3.2.1 Grondwet (GW)

Artikel 10 [eerbiediging van de persoonlijke levenssfeer]

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Artikel 11 [onaantastbaarheid van het lichaam]

Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.

Artikel 13 [brief- telefoon- en telegraafgeheim]

1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

3.2.2 Europees Verdrag voor de Rechten van de Mens (EVRM)**Artikel 8 [eerbiediging van de persoonlijke levenssfeer] Recht op eerbiediging van privé familie- en gezinsleven**

1. Een ieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

3.2.3 Algemene Wet Bestuursrecht (AWB)**Artikel 5:20 [medewerkingsplicht]**

1. Een ieder is verplicht aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Zij die uit hoofde van ambt, beroep of wettelijk voorschrift verplicht zijn tot geheimhouding, kunnen het verlenen van medewerking weigeren, voor zover dit uit hun geheimhoudingsplicht voortvloeit.

3.2.4 Wet op het Hoger Onderwijs en Wetenschappelijk Onderzoek (WHW)

Bij het verzorgen van het onderwijs vormt de WHW het wettelijk kader. HvHL heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd, evenals met gegevens in de personeels- en salarisadministratie. Daarnaast worden gedrags- en integriteitscodes voor medewerkers en studenten nageleefd en toegepast.

3.2.5 AVG en UAVG

HvHL heeft de wettelijke vereisten geïmplementeerd met het privacybeleid. Onderdeel van het beleid zijn een rechtmatige en zorgvuldige verwerking van persoonsgegevens en het nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van persoonsgegevens. Het privacybeleid is in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG).



3.2.6 *Archiefwet*

HvHL houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop moet worden omgegaan met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

3.2.7 *Selectielijst Hogescholen*

HvHL hanteert voor de bewaar- en vernietigingstermijnen van persoonsgegevens in beginsel de Selectielijst Hogescholen uitgebracht door de Vereniging Hogescholen.

3.2.8 *Handvest van de Grondrechten van de Europese Unie (EHRM)*

Artikel 7 [eerbiediging van de persoonlijke levenssfeer] De eerbiediging van het privéleven en van het familie- en gezinsleven

Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

Artikel 8 [bescherming persoonsgegevens] De bescherming van persoonsgegevens

1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.

3.2.9 *ePrivacy Directive/Verordening (ePV)*

De wetgeving rond de ePrivacy Verordening richt zich specifiek op de bescherming van persoonsgegevens rond elektronische communicatie. Onder elektronische communicatie wordt verstaan: 'informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische communicatiedienst'. Denk hierbij aan bijvoorbeeld het versturen van een e-mailadres of telefoonnummer via sociale mediakanalen. Alhoewel de ePrivacy Verordening zich richt op elektronische communicatie, is het toepassingsbereik van de verordening groot. Het geldt onder andere bij online marketing, e-mail en sociale media kanalen, het ophalen van gegevens door middel van het plaatsen van cookies en openbare WiFi-netwerken.

3.2.10 *Telecommunicatiewet (Cookiewet)*

artikel 11.7a

1. Onverminderd de Algemene verordening gegevensbescherming is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:
 - a. is voorzien van duidelijke en volledige informatie overeenkomstig de Algemene verordening gegevensbescherming, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en
 - b. daarvoor toestemming heeft verleend.
2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk

- wordt bewerkstelligd dat via een elektronisch communicatienetwerk informatie wordt opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen informatie.
3. Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:
 - a. met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,
 - b. die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij.
 4. Een handeling als bedoeld in het eerste lid, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren zodat de betrokken gebruiker of abonnee anders behandeld kan worden, wordt vermoed een verwerking van persoonsgegevens te zijn.
 5. De toegang van de gebruiker tot een dienst van de informatiemaatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon wordt niet afhankelijk gemaakt van het verlenen van toestemming als bedoeld in het eerste lid.
 6. Bij of krachtens algemene maatregel van bestuur kunnen in overeenstemming met Onze Minister van Veiligheid en Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten en de in het derde lid genoemde uitzonderingen.

3.3 Beleid

3.3.1 Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is opgesteld door de afdeling IVT en vastgesteld door het CvB. In dit beleid is het systeem beschreven dat ervoor zorgt dat HvHL cybersecuritymaatregelen optimaal identificeert en implementeert om interne en externe dreigingen het hoofd te bieden.

3.3.2 Archiefbeleid

Bewaarregels en bewaartermijnen voor documenten die binnen de Selectielijst vallen worden gehanteerd. Daarnaast is in het beleid een uniforme wijze van archiveren beschreven, zodat het terugvinden van informatie gewaarborgd wordt.

3.3.3 Bewaarbeleid

Het bewaarbeleid beschrijft de verplichtingen van HvHL met betrekking tot het bewaren van persoonsgegevens die door HvHL zijn verzameld in overeenstemming met de AVG.



4. Governance en organisatorische borging gegevensbescherming

HvHL zorgt ervoor – naast de benodigde technische maatregelen – dat alle medewerkers op een rechtmatige wijze persoonsgegevens verwerken. Hoe dit organisatorisch wordt geborgd, wordt in dit hoofdstuk beschreven.

4.1 Basisregels

Alle medewerkers binnen HvHL zijn verantwoordelijk voor een rechtmatige omgang met persoonsgegevens. Daartoe zijn de volgende elf basisregels opgesteld:

1. Gebruik alleen die persoonsgegevens die je nodig hebt voor je doel/activiteit;
2. Zorg dat de persoonsgegevens die je verwerkt juist en actueel zijn;
3. Sla persoonsgegevens op zo min mogelijk plekken op;
4. Deel de persoonsgegevens alleen met collega's die direct betrokken zijn;
5. Laat persoonsgegevens niet onbeheerd achter;
6. Neem de grootste zorgvuldigheid in acht wanneer je bijzondere persoonsgegevens verwerkt;
7. Verwijder de persoonsgegevens na het verstrijken van de bewaartermijn;
8. Neem de grootste zorgvuldigheid en terughoudendheid in acht als het gaat om het verstrekken van persoonsgegevens aan derden;
9. Raadpleeg de Data Protection Office (DPO) bij bijzondere situaties of voor advies;
10. Denk je dat je persoonsgegevens hebt gelekt? Meld dit direct aan de DPO. Stuur buiten kantooruren of in het weekend een SMS.

Deze basisregels vormen ook het kader bij het vaststellen of aanpassen van de diverse werkprocessen binnen de organisatie. Iedere medewerker heeft zijn of haar eigen verantwoordelijkheid voor een rechtmatige omgang met persoonsgegevens.

4.2 3 lines model

Het Three Lines Model wordt door HvHL als instrument ingezet om risico's te beheersen en om aan de buitenwereld te laten zien dat we *'in control'* zijn. Daarbij worden drie 'verdedigingslinies' gebruikt om te voorkomen dat een risico daadwerkelijk een schade wordt voor de organisatie.

De eerste lijn

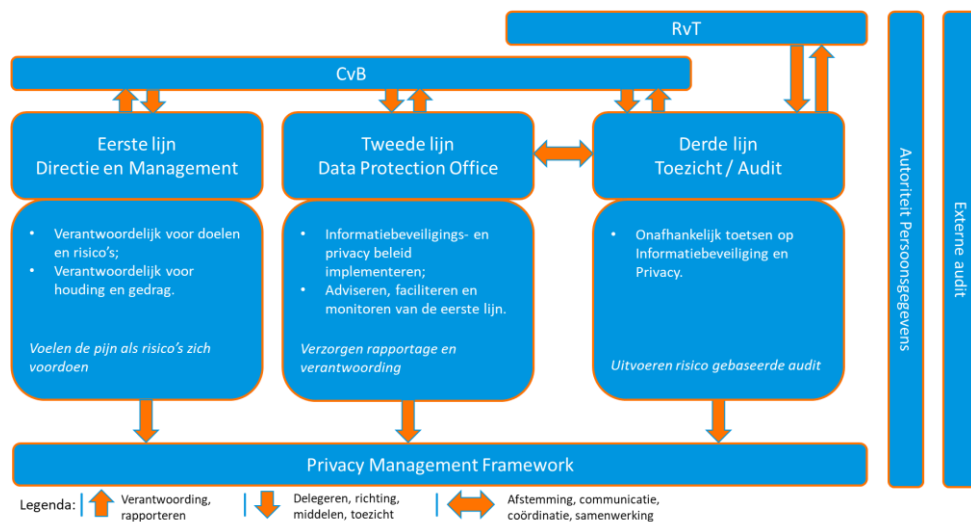
Dit zijn de directeuren en managers die doelen moeten halen, medewerkers aansturen en risico's managen. Risico's kunnen het beste beheerst worden door hen die er belang bij hebben, daarom is de eerste lijn de belangrijkste vorm van risicomanagement.

De tweede lijn

Deze lijn ondersteunt de eerste lijn met betrekking tot risicomanagement met specialistische kennis rondom de risicogebieden Privacy en Security. Ook controleert zij of de controls op orde zijn.

De derde lijn

Dit is de interne audit en analyseert inconsistenties in de opzet en het bestaan en werking van het SURF Audit Toetsingskader Privacy en het SURF Audit Toetsingskader Informatiebeveiliging (IB) en doet bevindingen en aanbevelingen. Zij geeft daarmee een onafhankelijk oordeel en zekerheid (assurance) af over de kwaliteit van sturing en beheersing.



Figuur 5: Three Lines Model

4.3 Rollen en verantwoordelijkheden

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken wordt bij HvHL een aantal rollen onderkend die zijn toegewezen.

4.3.1 Betrokkenen binnen HvHL

Betrokkenen binnen HvHL (studenten, medewerkers, relaties (inhuur/outsourcing)) zorgen ervoor dat zij volgens de basisregels en de daarvoor vastgestelde werkprocessen omgaan met persoonsgegevens. Bij problemen bij het volgen van de werkprocessen informeren zij daarover hun afdelingshoofd en de DPO. Eventuele vragen over de verwerking van persoonsgegevens en over het werkproces voor datalekken, waaronder de vraag of sprake is van een datalek, kunnen gesteld worden aan de DPO.

4.3.2 College van Bestuur (CvB)

Het CvB is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen HvHL en stelt het beleid, de maatregelen en de procedures op het gebied van verwerking vast. Het college wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de AVG.

Portefeuillehouder beveiliging persoonsgegevens

De portefeuillehouder beveiliging persoonsgegevens is het bestuurslid dat integrale veiligheid in portefeuille heeft. De portefeuillehouder is eindverantwoordelijk voor beveiliging van persoonsgegevens binnen HvHL.



4.3.3 *Directeuren en managers van de diensten*

De directeuren Onderwijs en Onderzoek en de managers van de diensten zijn verantwoordelijk ten aanzien van een rechtmatige en zorgvuldige verwerking van persoonsgegevens bij hun organisatieonderdelen. Deze verantwoordelijkheid is aan hen overgedragen door het CvB.

4.3.4 *Leidinggevenden*

Het creëren van bewustwording en de naleving van het beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beleid;
- toe te zien op de naleving van het beleid door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

4.3.5 *Manager Bestuursstaf*

Het beleidsthema privacy / bescherming van persoonsgegevens is belegd bij de manager Bestuursstaf. Deze is namens het CvB verantwoordelijk voor de implementatie, uitvoering, naleving en actualisering van het privacybeleid.

4.3.6 *Functionaris gegevensbescherming (FG)*

HvHL beschikt over een onafhankelijke, interne toezichthouder op de verwerking van persoonsgegevens. Deze toezichthouder is de FG. De FG is aangemeld bij de Autoriteit persoonsgegevens.

Uit de AVG vloeit voort dat de FG samenwerkt met en fungeert als eerste aanspreekpunt voor de Autoriteit persoonsgegevens. De FG adviseert daarnaast de organisatie over haar wettelijke verplichtingen en ziet toe op naleving van de AVG en het privacybeleid. HvHL stelt hem de benodigde middelen ter beschikking voor het vervullen van zijn taken en het in stand houden van zijn deskundigheid.

De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn taken. De FG kan de uitvoering van het beleid bevorderen, maar heeft ook de ruimte om eventuele zorgen over naleving van het privacybeleid aan de manager bestuursstaf als thema-eigenaar (en waar dat naar zijn mening nodig is aan het CvB) kenbaar te maken. De handreiking FG van het Nederlands Genootschap voor Functionarissen Gegevensbescherming (NGFG) wordt gehanteerd als uitgangspunt voor de uitvoering en inbedding van de functie bij HvHL.

De FG wordt tijdig betrokken bij alle aangelegenheden waar persoonsgegevens aan de orde zijn en brengt jaarlijks verslag uit van zijn bevindingen aan het CvB.

4.3.7 *Data Protection Office (DPO)*

De Data Protection Office heeft als taak om ervoor te zorgen dat medewerkers binnen HvHL zich bewust blijven van de rechtmatige omgang met persoonsgegevens, door hen daarover periodiek te informeren, onder meer over de hiervoor beschreven basisregels. Daarbij volgt de DPO het opgestelde communicatieplan. Daarnaast beantwoordt de DPO eventuele vragen van medewerkers over specifieke gegevensverwerkingen. Indien een medewerker een nieuwe



verwerking bij de DPO meldt die nog niet in het verwerkingsregister is opgenomen, voegt de DPO deze toe aan het register.

De rollen, taken en verantwoordelijkheden bij de DPO zijn uitgewerkt in het document “Inrichting Data Protection Office”.

4.3.8 Systeemeigenaarschap en verantwoordelijkheid

Binnen HvHL worden veel en uiteenlopende systemen en applicaties gebruikt voor het verzorgen van het onderwijs en de bedrijfsvoering. De managers dragen de verantwoordelijkheid voor de gang van zaken binnen het onderdeel waaraan zij leiding geven.

De systeemeigenaar is er verantwoordelijk voor dat de applicatie en bijbehorende IVT-faciliteiten een goede ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het beleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu, als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.

Alle aan te schaffen systemen, applicaties, licenties en dergelijke worden in overleg met de afdeling Inkoop & IVT/Contractmanagement ingekocht.

4.4 P&C cyclus

Er zijn bij HvHL drie formele momenten in het jaar waarin gegevensbescherming bij HvHL wordt verantwoord, te weten:

- Beleids-/jaarplan (jaarlijks voor 1 december);
- Halfjaarrapportage (jaarlijks uiterlijk 30 juli);
- Jaarverslag (jaarlijks uiterlijk 15 maart).

In het beleids-/jaarplan geeft HvHL aan wat de doelen/ambities voor het komende jaar zijn. Hierin is de implementatie en naleving van de AVG door HvHL als verwerkingsverantwoordelijke een vast element. In respectievelijk de halfjaarrapportage en het jaarverslag wordt gerapporteerd over de voortgang en eventuele maatregelen die getroffen worden om daadwerkelijk AVG-proof te zijn en te blijven.

De interne controlecyclus, zoals in de vorige paragrafen is beschreven, heeft een frequentie van tweemaal per jaar. Elk half jaar informeert de DPO het CvB.



5. Rechtmatige en zorgvuldige verwerking van persoonsgegevens

HvHL verwerkt persoonsgegevens op een manier die ten aanzien van betrokkenen behoorlijk en transparant is. Om de rechtmatige en zorgvuldige verwerking van persoonsgegevens te waarborgen wordt het 7S-Model van McKinsey gehanteerd, om Privacy op een holistische en effectieve manier te organiseren.

Door dit model toe te passen op de context van het onderwerp privacy, is snel zichtbaar dat alleen het nemen van technische en organisatorische maatregelen niet leidt tot een effectief en integraal ingerichte organisatie.



Figuur 6: 7S-model van McKinsey

5.1 Rechtmatige en zorgvuldige verwerking

Privacy is een gedeelde verantwoordelijkheid, niet alleen van het management, niet alleen van de FG. Dat betekent dat privacy in alle gedeeltes van HvHL structureel een plek moet krijgen.

Incidenten rondom de verwerking van persoonsgegevens zijn niet volledig te voorkomen. Niemand is perfect en menselijk falen is ons allen bekend. Een risico op een incident als een datalek is in elke organisatie aanwezig. Blijvende aandacht voor privacy is een verantwoording waaraan organisaties, dus ook HvHL, niet ontkomen.

5.2 Organisatorische maatregelen

Beleggen aanjagersrollen

Het gaat bij de AVG over veel meer dan het beveiligen van systemen, processen en data, waarbij slechts enkelen verantwoordelijk zijn. Het gaat om het gedrag van medewerkers, dat is



uiteindelijk de allesbepalende factor bij gegevensverwerking. Uiteraard is het CvB verantwoordelijk voor het nakomen van de verplichtingen die voortvloeien uit de AVG. Dat principe ontslaat HvHL echter niet van een collectieve verantwoording om op een juiste wijze met privacy en persoonsgegevens om te gaan. Iedereen heeft daarin een rol én verantwoording. Deze rollen met verantwoordelijkheden zijn in paragraaf 4.2 uitgewerkt.

Documentatieplicht

HvHL heeft meerdere maatregelen getroffen om aan te tonen te voldoen aan de wettelijke eisen uit de AVG, waaronder implementatie van het onderhavige beleid.

Elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens dient gemeld te worden bij de DPO, die de rechtsgeldigheid van de verwerking beoordeelt en toeziet op een adequate documentatie van alle relevante gegevens.

5.2 Technische maatregelen

Passende beveiligingsmaatregelen

HvHL draagt zorg voor een adequaat beveiligingsniveau en legt 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.

Een risicoanalyse op gegevensbescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van HvHL.

Privacy by Design en Privacy by Default

HvHL hanteert bij de implementatie van iedere verwerking de principes Privacy by Design en Privacy by Default. Dat betekent vooral dat bij de ontwikkeling en/of aanschaf van producten en diensten gegevensbescherming altijd voldoende aandacht moet krijgen. Met name bij ICT-producten en -diensten is het van belang dat al in het ontwikkelproces over passende en waar mogelijk privacy verhogende maatregelen wordt nagedacht.

5.3 Herkennen van situaties en risico's

Communicatie

HvHL beschikt over een communicatieplan Gegevensbescherming (privacy en security). Onderdeel van dit plan is een jaarplanning. Dit jaarplan beschrijft de onderwerpen die over de maanden heen onder de aandacht van de hogeschoolgemeenschap gebracht gaan worden.

E-learning

HvHL investeert in de Privacy kernvaardigheden van haar medewerkers en studenten. Hiervoor wordt e-learning beschikbaar gesteld met zowel een vrijwillig als verplicht karakter.

Data Protection Office

De FG, Bedrijfsjurist en CISO vormen de Data Protection Office, waar medewerkers en studenten met hun vragen rondom privacy en security terecht kunnen. De werking van de DPO is beschreven in het document "Inrichting Data Protection Office".



Op intranet is een kennisdatabank te vinden met Privacy gerelateerde onderwerpen. Hier worden ook regelmatig de voortgang, actualiteiten en ervaringen met Privacy gedeeld.

5.4 Supporten van privacybewust gedrag

Leiderschapsvisie

Privacy heeft een plek binnen de leiderschapsvisie van HvHL. Leidinggevend worden getraind om sturing te geven op privacy. Uitgangspunten, risico's en kansen worden door de DPO gedeeld met managers en leidinggevend.

Onboarding

Tijdens de onboarding van nieuwe medewerkers wordt aandacht besteed aan de regels voor de verwerking van privacygevoelige, bedrijfsgevoelige of personeelsvertrouwelijke gegevens gelden binnen HvHL.

Risico-inventarisatie

Bij vernieuwingen, veranderingen en projecten wordt een risico-inventarisatie over privacy gemaakt met de daarbij behorende mitigerende maatregelen.

5.5 Privacybewust handelen en gedrag

Geheimhouding

Bij HvHL worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Eenieder behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Toegang tot gegevens waartoe een medewerker (of andere persoon) geen rechten heeft of dient te hebben, wordt door middel van autorisaties op gedeelde media en binnen systemen afgeschermd. In voorkomende gevallen zal op basis van functies en taken van personen nader worden bekeken of de standaard autorisaties afdoende zijn of dat aanvulling noodzakelijk is. Deze geheimhoudingsplicht wordt eenieder bij het begin van een dienstverband duidelijk gemaakt en is een onderdeel van de arbeidsovereenkomst.

Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens vindt uitsluitend plaats indien sprake is van de wettelijke uitzonderingen in de AVG en de UAVG. Aan de beveiliging van bijzondere persoonsgegevens worden strengere eisen gesteld. Daar waar de basisbescherming niet afdoende is, moeten voor elk informatiesysteem afzonderlijk extra maatregelen worden genomen.

5.6 Privacybeleid en -reglement

Privacyverklaring

HvHL maakt aan de betrokkene inzichtelijk in hoeverre en op welke manier diens persoonsgegevens verwerkt worden. Bij het verzamelen van de persoonsgegevens zal HvHL middels een privacyverklaring de betrokkene inlichten.

Uitbesteden van verwerking aan een verwerker

Indien HvHL persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van verwerkingen geregeld in een verwerkersovereenkomst. Is er sprake van meerdere



verwerkingsverantwoordelijken, zoals het geval is bij een samenwerkingsverband met een andere instelling waarbij over en weer persoonsgegevens worden gewisseld, dan wordt een gegevensuitwisselingsovereenkomst gesloten. HvHL gebruikt daarbij de modellen die door SURF worden aangeboden. Bij significante afwijking van die modellen wordt de DPO om advies gevraagd.

Doorgifte persoonsgegevens binnen de Europese Economische Ruimte (EER)

HvHL 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 AVG of artikel 9 AVG en als de Verwerker voldoet aan de wettelijke vereisten uit de AVG. Het verwerkingenregister vermeldt expliciet de grondslag van de verwerkingen.

Doorgifte persoonsgegevens buiten de EER

HvHL verstrekt Persoonsgegevens alleen aan Verwerkers die zich bevinden in een land buiten de EER indien aan een van de volgende voorwaarden is voldaan:

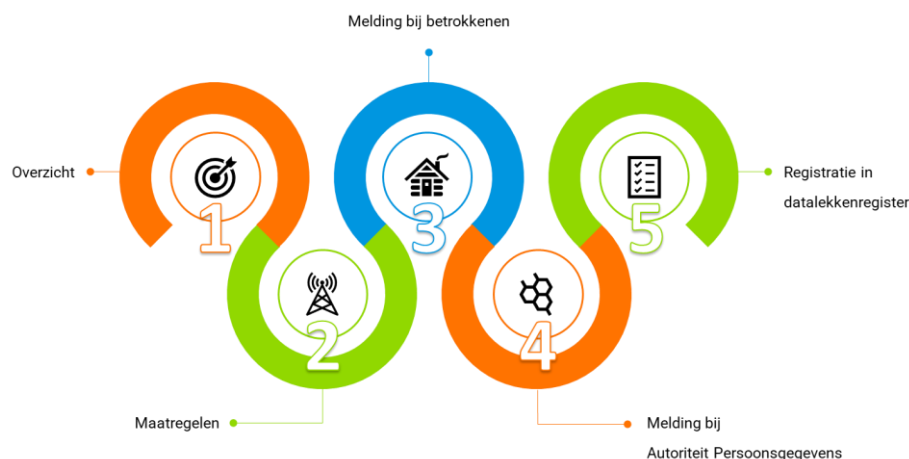
- Het derde land, gebied welbepaalde sector in een derde land of een internationale organisatie in kwestie biedt volgens de Europese Commissie een passend beschermingsniveau. Als passend beschermingsniveau hanteert HvHL de algemene lijst van landen met passend beveiligingsniveau gepubliceerd door de Europese Commissie;
- Doorgifte vindt plaats op basis van passende waarborgen uit de AVG, artikel 46 en 47;
- Doorgifte vindt plaats op basis van een van de wettelijke uitzonderingen uit artikel 49 van de AVG.



6. Datalekken

Van een datalek is sprake als er een inbreuk op de beveiliging van persoonsgegevens plaatsvindt die leidt tot enige ongeoorloofde verwerking daarvan. Dat is het geval indien sprake is van een inbreuk op de vertrouwelijkheid, de integriteit of de beschikbaarheid. Datalekken die op grond van de AVG moeten worden gemeld bij de Autoriteit Persoonsgegevens, worden binnen 72 uur na ontdekking ervan gemeld.

Een datalek kan bij HvHL binnen de eigen organisatie ontstaan, maar ook bij een door haar ingeschakelde verwerker. In de door HvHL gehanteerde modellen voor verwerkersovereenkomsten en gegevensuitwisselingsovereenkomsten zijn effectieve procedures opgenomen om bij een datalek tijdig en adequaat te kunnen handelen. Voor het melden van een datalek houdt HvHL een speciaal mailadres (datalekken@hvhl.nl) beschikbaar dat aan de hogeschoolgemeenschap is bekend gemaakt en in verwerkersovereenkomsten en gegevensuitwisselingsovereenkomsten is opgenomen.



Figuur 7: Stappenplan datalekken

Bij een datalek is het belangrijk om overzicht van de situatie te creëren. Gaat het om gelekte, vernietigde of gewijzigde gegevens? Wat is de omvang? Om welke persoonsgegevens gaat het? Wie heeft (mogelijk) toegang tot deze persoonsgegevens? Deze informatie heeft HvHL nodig bij de volgende stappen.

Het is van belang om te leren van datalekken, om risico's op herhaling of nieuwe datalekken en de nadelige gevolgen ervan te verkleinen. De DPO doet actief onderzoek naar aanleiding van een datalekmelding, attendeert het management waar mogelijk op verbeterpunten.

De procedure met betrekking tot de melding, registratie en afhandeling van datalekken is beschreven in het protocol Datalekken en beschikbaar op MyHVHL.nl.

7. Rechten van Betrokkenen

De AVG geeft betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. HvHL heeft in de “Procedure Rechten van Betrokkenen” de procedurele regels voor het indienen en afhandelen van verzoeken beschreven.



Figuur 8: Rechten van betrokkenen

De AVG stelt specifieke eisen aan de uitoefening van deze rechten. Sommige rechten zijn niet absoluut. Een verzoek om gegevens te wissen bijvoorbeeld moet worden afgewezen als de wet opdracht geeft tot het bewaren van die gegevens.

7.1 Melding aan Betrokkene

HvHL draagt er zorg voor dat de informatie en communicatie op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan betrokkene. De taal zal worden afgestemd op de doelgroep.

7.2 Termijn

Op een verzoek van een betrokkene wordt zo spoedig mogelijk, doch uiterlijk binnen een maand 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 redelijkerwijs niet haalbaar is, zal betrokkene daarvan binnen deze termijn op de hoogte worden gesteld.

7.3 Identiteit Betrokkene

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

7.4 Minderjarigen

Een verzoek tot uitoefening van een van de rechten zoals uitgewerkt in dit hoofdstuk door een betrokkene die minderjarig is, onder curatele gesteld of ten behoeve van wie een bewind of mentorschap is ingesteld, geschiedt door diens wettelijk vertegenwoordiger.



8. Implementatie beleid

Het CvB van HvHL is eindverantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van HvHL uitgevoerd.

8.1 Verdeling van de verantwoordelijkheden

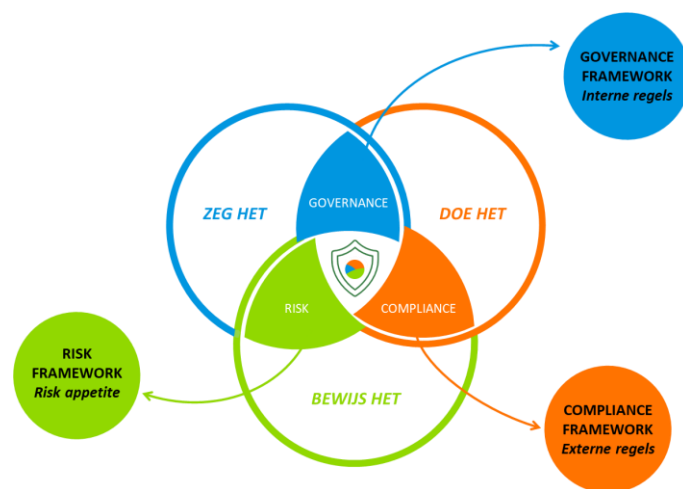
Het zorgvuldig verwerken van persoonsgegevens is de verantwoordelijkheid van alle leden van de hogeschoolgemeenschap. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen.

Er wordt van medewerkers en studenten verlangd dat zij zich integer gedragen, ook wat betreft een zorgvuldige omgang met persoonsgegevens. Niet aanvaardbaar is dat door (al dan niet opzettelijk) gedrag onveilige situaties ontstaan die leiden tot schade/reputatieverlies of risico's op identiteitsfraude bij individuen en/of imagooverlies van HvHL. In de Gedragscode voor de digitale werkomgeving en de Gedragscode voor gegevensbescherming zijn voor de leden van de hogeschoolgemeenschap de belangrijkste (gedrags)regels opgenomen over de bescherming van persoonsgegevens.

8.2 Gegevensbescherming in de organisatie

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 gegevensbescherming op verschillende niveaus.

Hiervoor hanteert HVHL onderstaand framework, dat gebaseerd is op 3 pijlers, die er gezamenlijk voor zorgen dat duidelijk is welke (persoons)gegevens verwerkt worden.



Figuur 9: Gegevensbescherming Governance Framework HVHL

Effectieve gegevensbescherming governance is bij HvHL een continue proces, uitgevoerd door mensen, mogelijk gemaakt door processen, visie en beleid en ondersteund door technologie.

8.3 Data Protection Office (DPO)

De DPO heeft als taak om toe te zien en ondersteuning te bieden bij de uitvoering van dit privacybeleid en de gedragscodes. De opzet en werking van de DPO is uitgewerkt in het document "Inrichting Data Protection Office".

8.4 Privacy/Security overleg

Op het snijvlak van privacy en informatieveiligheid wordt periodiek overleg gevoerd om ontwikkelingen op het beleidsterrein van gegevensbescherming te bespreken, beleidsvoornemens te formuleren, problemen te analyseren en bij te dragen aan de uitvoering van het jaarplan van de DPO. Indien nodig zal een vertegenwoordiger vanuit de organisatie en/of de manager IVT uitgenodigd worden.

8.5 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 HvHL 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 bezoekers.

8.6 Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De DPO initieert de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens. Het verwerkingenregister is daarbij een belangrijk instrument. Processen die zich naar hun aard (zoals verwerking van gevoelige gegevens en/of bij grootschalige verwerkingen) daartoe lenen, worden periodiek onderworpen aan een Data Protection Impact Assessment (DPIA). De uitvoering ervan vindt plaats onder regie van de DPO.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus. Peer-reviews van SURFaudit maken onderdeel uit van de externe controles van HvHL.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekort schieten, dan kan HvHL de betrokken verantwoordelijke medewerkers en studenten een sanctie op leggen, binnen de kaders van de CAO, WHW en wettelijke mogelijkheden.



9. Uitvoering van beleid

Dit privacybeleid is vastgesteld door het CvB van HvHL op 27-05-2025.

Versie	Datum	Wie	Aanpassing
1.0 Definitief	12-05-2021	A.van der Sluijs	
2.0 Ter goedkeuring CvB	31-12-2024	Linda Dijkstra	Geheel vernieuwde versie
2.1 Definitief	27-05-2025	Linda Dijkstra	Opmerkingen CvB verwerkt

Dit privacybeleid wordt eens in de drie jaar geëvalueerd en zo nodig herzien.

Dit privacybeleid wordt gepubliceerd op MyHVHL.nl

Voor vragen of opmerkingen met betrekking tot dit Beleid kunt u terecht op privacy@hvhl.nl.