Privacybeleid
Avans Hogeschool

Herziening 2024

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	30-10-17	Cees Bal, Thom van den Brule, Paul Logtens	Opzet Avans beleid ten behoeve van bespreking kader.
0.2	Feb 2018	Paul Logtens, Thom van den Brule, Mark van den Hove, Irene Willems	Eerste uitgewerkte versie van het nieuwe privacy beleid.
0.3	Mrt 2018	Cees Bal, Paul Logtens, Thom van den Brule, Mark van den Hove, Irene Willems	Redigeerslag door Beleidsverantwoordelijke, Functionaris Gegevensbescherming, Juridisch Team, projectleider privacy-project.
1.0	Apr 2018	Cees Bal, Paul Logtens, Thom van den Brule, Mark van den Hove, Irene Willems	Oplevering aan afvaarding netwerkbijeenkomst.
1.1	Okt 2018	Irene Willems	Kleine aanpassing doorgevoerd in bijlage I, te weten bij de subcategorieën van de categorie ‘Overig’.
1.5	Jan 2023	Bas van der Heijden	Eerste opzet herziene versie.
1.9	Feb 2023	Bas van der Heijden	Feedback op eerste opzet herziene versie verwerkt.
2.0	Maa 2023	Bas van der Heijden	Definitief

Inhoudsopgave

1 Inleiding

Het verwerken van Persoonsgegevens[1] is noodzakelijk voor de bedrijfsprocessen van iedere onderwijs- en onderzoeksinstelling en dient met de grootste zorgvuldigheid te gebeuren. Misbruik van Persoonsgegevens kan immers grote schade berokkenen aan studenten, medewerkers en andere Betrokkenen van Avans Hogeschool (hierna: Avans). Ook voor Avans zelf is het van groot belang dat zorgvuldig met Persoonsgegevens wordt omgegaan. Op die manier kunnen financiële schade en reputatieschade zoveel mogelijk worden beperkt.

Avans hecht dan ook veel waarde aan het beschermen van de Persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop Persoonsgegevens onder haar verantwoordelijkheid worden verwerkt. Het op een juiste manier verwerken van Persoonsgegevens is de verantwoordelijkheid van het College van Bestuur van Avans.

Met het beschrijven van de maatregelen in dit beleidsdocument neemt Avans haar verantwoordelijkheid om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren en beoogt zij te voldoen aan relevante privacywet- en regelgeving, voortvloeiende uit onder meer de Algemene Verordening Gegevensbescherming, de Uitvoeringswet AVG, de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek, de Archiefwet, arbeidsregelgeving, en gedragscodes zoals de Nederlandse Gedragscode Wetenschappelijke Integriteit en het Referentiekader privacy en ethiek voor studiedata.

1.1 Reikwijdte en doelstellingen van het Beleid

1.1.1 Reikwijdte van het Beleid

Dit Beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen Avans, waaronder alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing) vallen, alsmede alle andere Betrokkenen waarvan Avans Persoonsgegevens verwerkt.

In dit Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische Verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Avans. Dit Beleid is echter eveneens van toepassing op de Verwerking van Persoonsgegevens die in een (elektronisch of fysiek) bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

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.[2] Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht. Het informatiebeveiligingsbeleid van Avans is opgenomen in een separaat document, genaamd Informatiebeveiligingsbeleid Avans Hogeschool.

Het Beleid heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens bij Avans 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 fundamenteel 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 Avans.

---

[1] Een lijst van definities is opgenomen in Bijlage A Definities.
[2] Een nadere beschrijving van de samenhang tussen privacy en informatiebeveiliging is opgenomen in Bijlage B Samenhang Informatiebeveiliging en Privacy.

1.1.2 Doelstellingen van het Beleid

Met dit Beleid beoogt Avans concreet de volgende doelstellingen te behalen:

- 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: vaststellen hoe de organisatie om wil gaan met Persoonsgegevens.
- Het nemen van verantwoordelijkheid: door de uitgangspunten en de organisatie van het verwerken van Persoonsgegevens vast te leggen voor de hele organisatie van Avans.
- Daadkrachtige implementatie van het Beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- Compliant zijn met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter beperking van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

1.1.3 Ambities van Avans

Om inzichtelijk te maken waar de organisatie staat en wat de effecten zijn van de maatregelen die door de organisatie worden getroffen, maakt Avans gebruik van het SURFaudit Toetsingskader Privacy. Het maakt benchmarking met andere instellingen mogelijk, omdat afgesproken is dat dit model ook gebruikt wordt door de andere instellingen.

Avans heeft de ambitie om de privacy organisatie met behulp van dit Beleid naar volwassenheidsniveau 3 te brengen en daar te houden.

2 Beleidsprincipes Verwerking Persoonsgegevens

2.1 Uitgangspunt en -principes

Uitgangspunt 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 Avans om Persoonsgegevens te verwerken en het belang van Betrokkene ter eerbiediging van zijn persoonlijke levenssfeer en om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.

Om aan bovenstaand uitgangspunt te voldoen, gelden de volgende principes, welke principes verder zijn uitgewerkt in hoofdstuk 4 van dit Beleid:

Verantwoordelijkheid	Voor iedere gegevensverwerking is (intern) een verantwoordelijke benoemd. De verantwoordelijke maakt afspraken met Verwerkers en eventuele Derden over de veilige en zorgvuldige Verwerking van Persoonsgegevens.
Legitiem doel en grondslag	Het doel van de Verwerking moet voorafgaand aan de Verwerking voldoende specifiek en helder omschreven zijn. Een Verwerking van Persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG.
Ethisch verantwoord	Bij het beoordelen van Verwerkingen van Persoonsgegevens wordt ook rekening gehouden met ethische aspecten (het mag misschien, maar willen we dit ook).
Dataminimalisatie	Er worden niet meer gegevens verzameld dan noodzakelijk is voor het doel dat men wil bereiken. Gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel).
Doelbinding	Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
Bewaren en vernietigen	Persoonsgegevens zijn voorzien van een bewaartermijn. Persoonsgegevens worden vernietigd of geanonimiseerd wanneer deze niet langer nodig zijn voor de vastgestelde verwerkingsdoelen.
Juistheid	Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
Transparantie en informatie	Voor Betrokkenen is het inzichtelijk in hoeverre en op welke manier er Persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn.
Delen van gegevens	Persoonsgegevens worden alleen gedeeld met anderen als daar een rechtmatige grondslag voor is.

	Waar Persoonsgegevens gedeeld worden met andere partijen dienen daar goede afspraken over gemaakt te worden.
Informatiebeveiliging	Persoonsgegevens worden beveiligd door het nemen van technische en organisatorische maatregelen (risk-based). Toegang tot Persoonsgegevens wordt gegeven op basis van need-to-know. Systemen worden ontworpen en ingericht volgens de principes Privacy by design en Privacy by default.
Rechten van Betrokkenen	Iedere Betrokkene heeft, in overeenstemming met hetgeen daarover is bepaald in de AVG, recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van zijn/haar Persoonsgegevens, en heeft het recht van bezwaar. Bij alle Verwerkingen die gebaseerd zijn op de grondslag “toestemming” wordt voorafgaande aan de Verwerking om toestemming gevraagd. Toestemming is voor Betrokkenen net zo eenvoudig in te trekken als deze te geven is.
Verantwoordingsplicht	Avans kan aantonen dat zij voldoet aan de AVG.

3 Governance

3.1 Rollen en verantwoordelijkheden

Om de Verwerkingen van Persoonsgegevens gestructureerd en gecoördineerd op te pakken, wordt bij Avans een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

3.1.1 College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen Avans en stelt dit Beleid vast.

3.1.2 Portefeuillehouder privacy

De portefeuillehouder privacy is het lid van het College van Bestuur, dat bescherming van Persoonsgegevens in zijn portefeuille heeft. De portefeuillehouder privacy is het eerste aanspreekpunt op bestuurlijk niveau voor privacyzaken en betrekt de Functionaris Gegevensbescherming tijdig bij aangelegenheden die verband houden met de bescherming van Persoonsgegevens. Tevens is de portefeuillehouder privacy verantwoordelijk voor de regie op beleidsimplementatie. De portefeuillehouder privacy mandateert taken en bevoegdheden naar de beleidsverantwoordelijke eenheid.

3.1.3 Directeuren

Het bestuurs- en beheersreglement van Avans is leidend. Hierin staan de bevoegdheden en verantwoordelijkheden van een directeur beschreven. Een directeur is daardoor integraal verantwoordelijk voor compliance in zijn bedrijfsonderdeel. Dit betekent dat hij proceseigenaar en verantwoordelijke is voor de aan hem gestelde mandaten en/of volmachten. Een directeur is verantwoordelijk voor de uitvoering en de implementatie van het Beleid voor zijn bedrijfsonderdeel.

In relatie tot het Beleid is een directeur verantwoordelijk voor:

- de rechtmatige Verwerking van Persoonsgegevens;
- het vaststellen van processen en procedures voor de zorgvuldige Verwerking van Persoonsgegevens;
- het afhandelen van verzoeken in het kader van de rechten van Betrokkenen;
- het vullen en actualiseren van het verwerkingsregister;
- het sluiten van verwerkersovereenkomsten;
- het uitvoeren van Data Protection Impact Assessments;
- het treffen van beveiligingsmaatregelen, onder andere door ervoor te zorgen dat de ondersteunende applicatie(s) en bijbehorende ICT-faciliteiten een goede en veilige ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het Beleid;
- bewustwording van de medewerkers;
- het naar behoren en tijdig betrekken van de Functionaris Gegevensbescherming bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens.

3.1.4 Functionaris Gegevensbescherming

Het College van Bestuur benoemt een Functionaris Gegevensbescherming en draagt zorg voor registratie van deze functionaris bij de Autoriteit Persoonsgegevens. De Functionaris Gegevensbescherming is de interne toezichthouder op toepassing en naleving van de privacywetgeving én dit Beleid, en adviseert de Verwerkingsverantwoordelijke. De Functionaris Gegevensbescherming rapporteert rechtstreeks aan de portefeuillehouder privacy van het College van Bestuur.

De Functionaris Gegevensbescherming heeft de volgende taken:

- de Functionaris Gegevensbescherming informeert en adviseert alle betrokken partijen over hun verplichtingen onder de privacywetgeving;
- de Functionaris Gegevensbescherming ziet toe op de naleving van de privacywetgeving en dit Beleid;

- de Functionaris Gegevensbescherming adviseert over de manier waarop Verwerkingen rechtmatig, behoorlijk en transparant kunnen plaatsvinden, bijvoorbeeld op basis van het verwerkingsregister en aan de hand van Data Protection Impact Assessments;
- de Functionaris Gegevensbescherming is verplicht samen te werken met en op te treden als eerste aanspreekpunt van de Autoriteit Persoonsgegevens;
- de Functionaris Gegevensbescherming neemt de ruimte om het College van Bestuur te informeren over zijn bevindingen inzake de naleving van de privacywet- en regelgeving.

Het College van Bestuur kent daarvoor de volgende bevoegdheden toe aan de Functionaris Gegevensbescherming:

- de Functionaris Gegevensbescherming heeft toegang tot alle informatie die nodig is om bovengenoemde activiteiten te kunnen vervullen;
- de Functionaris Gegevensbescherming krijgt de benodigde middelen om zijn deskundigheid in stand te houden;
- de Functionaris Gegevensbescherming mag andere taken en functies vervullen, mits die niet tot een belangenconflict kunnen leiden.

De Functionaris Gegevensbescherming is werkzaam binnen de stafafdeling Beleidsevaluatie en Control (BE&C).

3.1.5 Beleidsverantwoordelijke eenheid

De Diensteenheid ICT en Facilitaire Dienst (DIF) is de beleidsverantwoordelijke eenheid voor dit Beleid en is daarmee verantwoordelijk voor:

- de doorlopende ontwikkeling en actualisatie van het Beleid;
- het monitoren van de implementatie en uitvoering van het Beleid;
- het faciliteren van de organisatie door het beschikbaar stellen van handreikingen waarin praktische vertaalslagen van dit Beleid zijn opgenomen;
- de opzet en inrichting van het verwerkingsregister.

3.1.6 Privacy Officer

De privacy officer helpt privacyrisico's naar een acceptabel niveau te reduceren en heeft de volgende taken:

- de privacy officer informeert en adviseert over privacy aangelegenheden;
- de privacy officer bewaakt de kwaliteit van het verwerkingsregister;
- de privacy officer signaleert privacyrisico's;
- de privacy officer adviseert bij het opstellen van Data Protection Impact Assessements en Privacy Risk Assessments;
- de privacy officer coördineert de afhandeling van verzoeken met betrekking tot rechten van Betrokkenen.

3.1.7 Privacy Contactpersoon

Alle academies van Avans benoemen een privacy contactpersoon. De rol is gekoppeld aan de rol van ICT-contactpersoon, tenzij de directeur van een bedrijfsonderdeel hier iemand anders (of anderen) voor aanwijst. De privacy contactpersoon is kennishouder van dit Beleid en van interne privacygerelateerde regelgeving. Hij weet wat zich in de haarvaten van de academie afspeelt en is eerste aanspreekpunt voor de academie op het gebied van privacy. De privacy contactpersoon heeft korte lijnen met collega's zodat privacy risico's tijdig gesignaleerd kunnen worden. In voorkomende gevallen kan de privacy contactpersoon de privacy officer of de Functionaris Gegevensbescherming raadplegen. Tevens zijn de privacy contactpersonen aanspreekpunten voor Functionaris Gegevensbescherming en privacy officer.

De taken van de privacy contactpersoon zijn:

- Het signaleren van vraagstukken op het gebied van privacy in de academie;
- Aanspreekpunt voor privacy vragen binnen de academie;
- Het leveren van een bijdrage aan het bewustwordingsproces rondom privacy binnen de academie.

3.1.8 Juridische Zaken

Juridische Zaken verleent tweedelijns ondersteuning aan team Privacy (zoals is beschreven in het Protocol Juridische Advisering van Avans). Dat betekent dat privacy-gerelateerde vragen enkel bij Juridische Zaken terecht komen via team Privacy.

3.1.9 CISO

De CISO is verantwoordelijk voor de professionalisering en borging van de informatiebeveiliging van Avans. Hieronder wordt verstaan de beveiliging van de informatievoorziening (waaronder IT-infrastructuur), het inzichtelijk maken van risico's Avans-breed, het opstellen van kaders, het monitoren van de naleving daarvan en het doen van verbetervoorstellen om het beveiligingsniveau continu te verbeteren. De CISO rapporteert integraal over informatiebeveiliging bij Avans aan het College van Bestuur.

3.1.10 CPO

De CPO is verantwoordelijk voor de professionalisering van de organisatie op het gebied van privacy en bevordert de toepassing en naleving van de privacywetgeving. Hieronder wordt verstaan de borging van de privacy van Betrokkenen, het inzichtelijk maken van risico's Avans-breed, het opstellen van kaders, het monitoren van de naleving daarvan en het doen van verbetervoorstellen om het volwassenheidsniveau van de organisatie op het gebied van privacy continu te verbeteren. De CPO rapporteert integraal over privacy aan het College van Bestuur.

3.2 Three Lines of Defence

De Governance bij Avans is ingericht volgens het zogenaamde Three Lines of Defence model[3] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

3.2.1 Eerste lijn

Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. De directeuren zorgen ervoor dat privacy afspraken ook werkelijk worden geïmplementeerd, dat awareness programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. Dit is de eerste lijn.

3.2.2 Tweede lijn

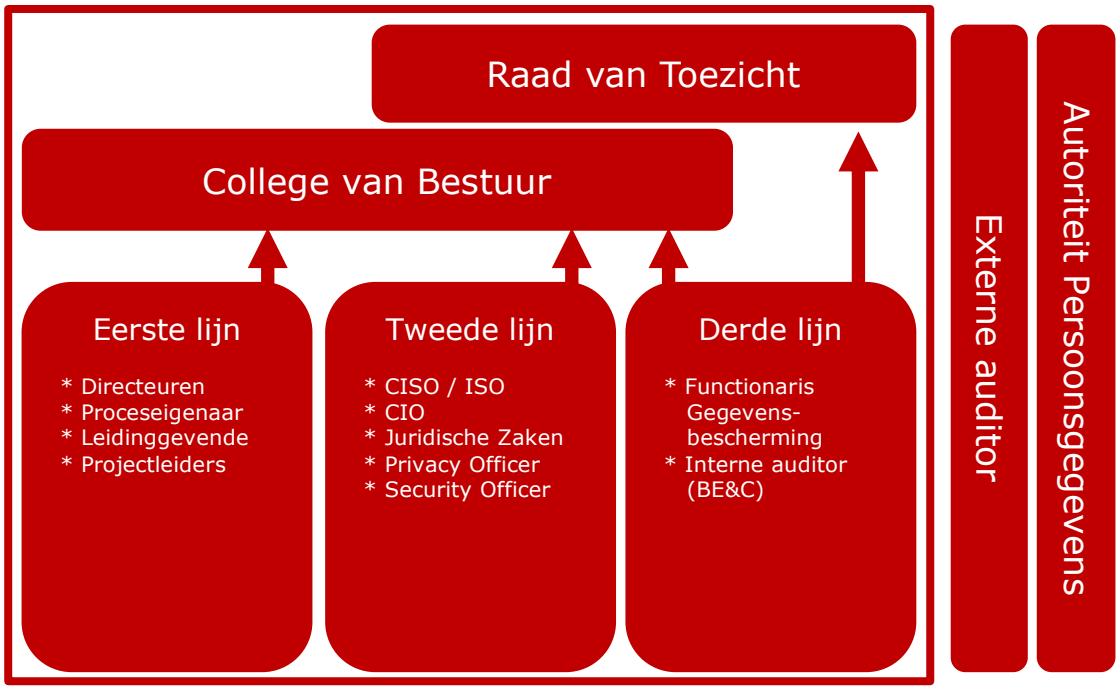
Daarnaast moet er een functie zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn. De privacy officer bevindt zich in de tweede lijn.

3.2.3 De derde lijn

Het is wenselijk dat er binnen de organisatie een functie bestaat die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. Daarbij kijkt de derde lijn ook of er geen overlapping is en of er blinde vlekken bestaan. Deze functie is de derde lijn.

De Functionaris Gegevensbescherming en de afdeling BE&C behoren tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan College van Bestuur, maar ook aan de Raad van Toezicht.

[3] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained



3.3 Verdeling van verantwoordelijkheden

Avans (Stichting Avans) wordt aangemerkt als Verwerkingsverantwoordelijke in de zin van de AVG. De feitelijke Verwerking van Persoonsgegevens vindt echter op allerlei lagen van Avans plaats. Stichting Avans, vertegenwoordigd door het College van Bestuur, is eindverantwoordelijk voor de Verwerkingen van Persoonsgegevens, waarvoor zij het doel en de middelen vaststelt.

Het zorgvuldig verwerken van Persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid. Dat betekent dat de directeuren de primaire verantwoordelijkheid dragen voor een zorgvuldige Verwerking van Persoonsgegevens op hun eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het Beleid te communiceren de medewerkers van de eenheid.

Het zorgvuldig omgaan met Persoonsgegevens is ieders verantwoordelijkheid. In dit verband wordt van medewerkers en studenten verwacht dat zij zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van Avans of van individuen.

3.4 Bewustwording en kennis

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van Persoonsgegevens uit te sluiten. Het is noodzakelijk om bij zowel medewerkers als studenten van Avans het privacy-bewustzijn en de kennis over zorgvuldige omgang met Persoonsgegevens voortdurend aan te scherpen, zodat het bewustzijn van de risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

3.4.1 Bewustwording

Avans zet zich in om het privacy-bewustzijn te verhogen en daarna periodiek op te frissen en aan te scherpen, zodat (externe) medewerkers:

- de noodzaak inzien van privacyregels en -beleid;
- proactief en conform Beleid en instructies handelen;
- elkaar aanspreken op mogelijke risico's en gedrag;

- weten hoe (beveiligings)incidenten moeten worden gemeld;
- bereid zijn om de dialoog aan te gaan met betrokkenen van Avans;
- voorbeeldgedrag tonen en zich bewust zijn van hun eigen gedrag;
- weten hoe en waar de informatie is te vinden om te kunnen werken conform dit Beleid.

Avans onderneemt geregeld activiteiten om het privacy-bewustzijn bij (externe) medewerkers te verhogen en hoog te houden. Daarvoor worden bewustwordingscampagnes georganiseerd, zo mogelijk in combinatie met interne campagnes (bijvoorbeeld campagnes vanuit informatiebeveiliging). Voor de bewustwording van nieuwe medewerkers wordt zoveel mogelijk aangesloten bij reeds bestaande communicatiemomenten.

De beleidsverantwoordelijke eenheid (DIF) is eindverantwoordelijk voor het organiseren van Avans-brede bewustwordingscampagnes.

3.4.2 Kennis

Behalve privacy-bewustzijn is het van belang dat (externe) medewerkers en studenten kennis hebben van of informatie kunnen vinden over het werken met Persoonsgegevens. Over wat bij Avans veilig en verantwoord gedrag is en wat niet.

Daarvoor stelt Avans een privacy & security website beschikbaar voor iedereen die onder de verantwoordelijkheid van Avans Persoonsgegevens verwerkt of zijn kennis over privacy wil aanscherpen. De beleidsverantwoordelijke eenheid (DIF) is eindverantwoordelijk voor de totstandkoming, de verdere ontwikkeling en het onderhoud van de privacy & security website.

3.5 Controle en naleving

3.5.1 PDCA-cyclus

De ambitie van Avans is dat dit Beleid in opzet en bestaan aantoonbaar geïntegreerd is binnen haar bedrijfsvoering. Om dat mogelijk te maken, is inbedding in de PDCA-cyclus van belang. Onderdeel van een volledige PDCA-cyclus is het meten van de kwaliteit en het opstarten van verbeteracties. Met een PDCA-cyclus wordt ook inzichtelijk waar de organisatie staat met het voldoen aan wet- en regelgeving. Daarvoor wordt gebruik gemaakt van het SURFaudit Toetsingskader Privacy, welke Avans – evenals de PDCA-cyclus – heeft opgenomen in haar Het zorgvuldig verwerken van Persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid. Dat betekent dat de directeuren de primaire verantwoordelijkheid dragen voor een zorgvuldige Verwerking van Persoonsgegevens op hun eenheid..

Privacy management is opgenomen binnen de planning en control-cyclus van Avans. De Functionaris Gegevensbescherming doet jaarlijks verslag aan het College van Bestuur en geeft aanbevelingen voor een verdere optimalisering van de privacy beleidsvoering. Het College van Bestuur besluit over bijsturing van dit Beleid in overeenstemming met de aanbevelingen van de Functionaris Gegevensbescherming.

3.5.2 Naleving

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. Team Beleidsevaluatie & Control (BE&C) initieert de interne controle op het rechtmatig en zorgvuldig verwerken van Persoonsgegevens.

Als blijkt dat de naleving van maatregelen ter bescherming van Persoonsgegevens ernstig tekortschiet, dan kan Avans de betrokken medewerkers een disciplinaire sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van bijvoorbeeld arbeidsovereenkomsten/CAO, gedragscodes, het protocol sancties en ordemaatregelen studenten en/of andere wettelijke mogelijkheden in bijvoorbeeld de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Primair is dit een verantwoordelijkheid van het College van Bestuur, maar dit is conform het Bestuurs- en beheersreglement in sommige gevallen gemandateerd aan directeuren.

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

4 Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

Avans verwerkt Persoonsgegevens in overeenstemming met de principes zoals benoemd in paragraaf 2.1 van dit Beleid. Ter uitwerking van deze principes treft Avans de in dit hoofdstuk genoemde maatregelen.

4.1 Verantwoordelijkheid

Voor iedere gegevensverwerking is een verantwoordelijke benoemd. In veel gevallen kan dit intern belegd worden bij een proces- of systeemeigenaar. De verantwoordelijke ziet erop toe dat de Verwerking voldoet aan de principes uit dit Beleid, voert een Privacy Risk Assessment uit en laat zo nodig een Data Protection Impact Assessment (DPIA) uitvoeren.

De verantwoordelijke maakt afspraken met Verwerkers en eventuele Derden over de veilige en zorgvuldige Verwerking van Persoonsgegevens. Voor het maken van afspraken met Verwerkers en Derden wordt gebruik gemaakt van de hiervoor door Avans gehanteerde modellen (zoals de modellen voor een verwerkersovereenkomst en het model voor een ‘Overeenkomst voor gezamenlijke verwerkingsverantwoordelijken’) en wordt gehandeld in overeenstemming met de daarbij behorende procesbeschrijvingen en beslisbomen. Voor meer informatie over de verwerkersovereenkomst, zie paragraaf 4.9.1.

4.2 Legitiem doel en grondslag

Avans verwerkt alleen Persoonsgegevens als daar een gerechtvaardigd doel voor is. Het doel van een Verwerking wordt voorafgaand aan de Verwerking voldoende specifiek en helder omschreven en vastgelegd in het verwerkingsregister. Bovendien worden Persoonsgegevens alleen verwerkt als daar een legitieme grondslag voor is, zoals beschreven in artikel 6 van de AVG. Meer informatie hierover kan worden gevonden in het privacystatement van Avans, onder de kop ‘Gebruik van persoonsgegevens bij Avans’ en ‘Grondslag voor de verwerking van jouw persoonsgegevens’.

4.3 Ethisch verantwoord

Bij het beoordelen van Verwerkingen van Persoonsgegevens wordt ook rekening gehouden met ethische aspecten (verwerking mag dan misschien wel, maar willen we dit ook/moeten we dit willen?). Deze aspecten worden meer in het bijzonder meegenomen bij Verwerkingen die bedoeld zijn om te profileren of daar naar hun aard om vragen, bijvoorbeeld omdat nieuwe technologieën worden gebruikt.

4.4 Dataminimalisatie

Er worden niet meer Persoonsgegevens verzameld dan noodzakelijk voor het doel dat Avans wil bereiken met het verwerken van die gegevens. Persoonsgegevens dienen toereikend en ter zake dienend te zijn.

Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel). Als het doel van de Verwerking ook bereikt kan worden op een manier die minder inbreuk maakt op de privacy van de Betrokkene, dan wordt voor deze manier gekozen.

Avans geeft invulling aan deze beginselen door het toepassen van “Privacy by default” en “Privacy by design” bij ingebruikname van nieuwe systemen of processen.

4.5 Doelbinding

Persoonsgegevens die voor een bepaald doel verzameld zijn, mogen alleen verder worden verwerkt voor andere doeleinden als deze doeleinden verenigbaar zijn met het oorspronkelijke doel.

Indien Avans verdere Verwerking wenselijk acht, dan dient aan een aantal elementen te worden getoetst of de verdere Verwerking verenigbaar is:

- Het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter de twee doelen bij elkaar liggen, hoe eerder de verdere Verwerking van Persoonsgegevens verenigbaar is met het oorspronkelijke doel.
- De context waarin de Persoonsgegevens zijn verzameld. Hierbij wordt in belangrijke mate rekening gehouden met de redelijke verwachting die de Betrokkene mag hebben betreffende de verdere Verwerking van zijn Persoonsgegevens voor dit nieuwe doel.
- De aard van de Persoonsgegevens. Wanneer het bijvoorbeeld gevoelige Persoonsgegevens betreft, geldt dat deze een hoger beschermingsniveau verdienen en dat deze minder snel voor andere doelen mogen worden gebruikt.
- De mogelijke gevolgen van de verdere Verwerking voor Betrokkenen.
- Het bestaan van passende waarborgen, zoals versleuteling of het gebruik van gepseudonimiseerde Persoonsgegevens.

De verdere Verwerking van Persoonsgegevens voor wetenschappelijk en historisch onderzoek, voor statistische doeleinden en voor archiveringsdoeleinden in het algemeen belang, worden door de AVG als verenigbaar aangemerkt, mits voldoende passende technische en organisatorische maatregelen zijn toegepast, zoals bijvoorbeeld het Pseudonimiseren van Persoonsgegevens.

Indien Avans Persoonsgegevens wenst te verwerken voor een doel dat onverenigbaar is met het oorspronkelijke doel, kan dat alleen als de Betrokkene hiervoor toestemming heeft gegeven of in geval van een specifieke wettelijke verplichting om bepaalde Persoonsgegevens te verstrekken aan een overheidsorgaan.

In zo'n geval is er sprake van een nieuwe Verwerking van Persoonsgegevens en moeten opnieuw de rechtmatigheid, zorgvuldigheid en noodzakelijkheid hiervan worden beoordeeld.

4.6 Bewaren en vernietigen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doeleinden te realiseren waarvoor de Persoonsgegevens zijn verzameld, of zo lang als specifieke wetten of regelingen voorschrijven. Avans zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen, Anonimiseren of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren en passende technische en organisatorische maatregelen nemen, zoals Pseudonimisering.

Bij het archiveren hanteert Avans de Selectielijst Avans Hogeschool als uitgangspunt voor de bewaartermijnen. De bewaartermijnen in deze selectielijst vinden hun oorsprong in diverse wetgeving zoals de WHW, AVG en Archiefwet.

Meer informatie hierover kan worden gevonden in het privacystatement van Avans, onder de kop 'Zo bewaart Avans jouw persoonsgegevens'.

4.7 Juistheid

Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn. Persoonsgegevens die onjuist of achterhaald zijn, worden gecorrigeerd of gewist.

Processen en systemen zijn zo ontworpen en ingericht dat juistheid van Persoonsgegevens zoveel mogelijk afgedwongen en controleerbaar is.

4.8 Transparantie en informatie

Avans verwerkt Persoonsgegevens op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat Avans aan de Betrokkene op een toegankelijke wijze en in begrijpelijke taal inzichtelijk maakt in hoeverre en op welke manier diens Persoonsgegevens worden verwerkt. Bij het verzamelen van de Persoonsgegevens zal Avans de Betrokkene informeren middels haar privacystatement of

een aanvullend informatiedocument. Inlichting zal plaatsvinden voorafgaand aan de Verwerking, tenzij dit redelijkerwijs niet mogelijk is.

4.8.1 Recht op informatie

Avans informeert de Betrokkene 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. Avans kan aantonen dat de informatie verstrekt is.

Verkrijging direct van Betrokkene

Avans verstrekt de Betrokkene voorafgaand aan de verzameling van de Persoonsgegevens 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.
- De gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of Derde als de Verwerking is gebaseerd op de rechtsgrond ‘gerechtvaardigd belang’.
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land, welk land dit is en op grond van welk wettelijk doorgiftemechanisme de Persoonsgegevens daarnaartoe worden verstuurd, en in bepaalde gevallen welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.
- De periode gedurende welke de Persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijn te bepalen.
- Het bestaan van het recht om de Verwerkingsverantwoordelijke te verzoeken om inzage, rectificatie of verwijdering van de Persoonsgegevens, beperking van de hem betreffende Verwerking, alsmede het recht tegen de Verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid.
- Indien de Verwerking is gebaseerd op de grondslag ‘toestemming’, het recht van de Betrokkene om die toestemming te allen tijde in te trekken en wat de gevolgen hiervan zijn ten aanzien van de Verwerking voorafgaand aan de intrekking.
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
- Of de Persoonsgegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting, en of de Betrokkene verplicht is de Persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer de Persoonsgegevens niet worden verstrekt.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming, met inbegrip van Profilering. Tevens moet de onderliggende logica, alsmede het belang en de te verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.

Verkrijging niet direct van Betrokkene

Als de Persoonsgegevens niet direct bij de Betrokkene zelf zijn verzameld maar langs een andere route (bijvoorbeeld wanneer de Persoonsgegevens van een derde partij zijn verkregen), 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.

Deze informatie zal zo snel mogelijk, maar niet later dan één maand na verkrijging van de gegevens, dan wel bij het eerste contact met de Betrokkene, worden verstrekt.

4.9 Delen van gegevens

4.9.1 Verwerking door een Verwerker

Indien Avans Persoonsgegevens laat verwerken door een Verwerker, wordt de uitvoering van de Verwerkingen vastgelegd in een verwerkersovereenkomst tussen Avans (de Verwerkingsverantwoordelijke) en deze Verwerker. Een verwerkersovereenkomst wordt overeengekomen voor aanvang van de betreffende

Verwerking, conform de door Avans opgestelde procesbeschrijving voor het aangaan van verwerkersovereenkomsten, en op basis van de daarvoor door Avans opgestelde modelovereenkomst. Afwijkingen van procesmatige bepalingen in de door Avans opgestelde modelovereenkomst (zoals de bepalingen met betrekking tot het verrichten van audits en het tijdsbestek waarbinnen de Verwerker verplicht is om contact op te nemen met Avans als een Datalek heeft plaatsgevonden) mogen altijd door de privacy officer zelf overeengekomen worden. Indien de Verwerker niet-procesmatige bepalingen in de door Avans opgestelde modelovereenkomst wenst te wijzigen, of indien de Verwerker een ander model wenst te gebruiken (bijvoorbeeld omdat de Verwerker goed kan beargumenteren waarom zij enkel haar eigen model kan hanteren), wordt onderscheid gemaakt tussen inkoopgerelateerde en niet-inkoopgerelateerde verwerkersovereenkomsten.[4] Bij niet-inkoopgerelateerde verwerkersovereenkomsten zijn afwijkingen alleen toegestaan na verplichte consultatie van Juridische Zaken door een privacy officer. Bij inkoopgerelateerde verwerkersovereenkomsten zullen de privacy officer en een vertegenwoordiger van team Inkoop en Contractmanagement de afwijking beoordelen aan de hand van de risicomatrix, alvorens een eventuele wijziging wordt toegestaan.

4.9.2 Verwerking door of gezamenlijk met een andere Verwerkingsverantwoordelijke

Indien Avans samen met één of meerdere partijen de doelen en middelen voor de Verwerking van Persoonsgegevens bepaalt, is er sprake van een gezamenlijke verwerkingsverantwoordelijkheid en worden afspraken omtrent de zorgvuldige en veilige Verwerking van Persoonsgegevens vastgelegd in de ‘Overeenkomst voor gezamenlijke verwerkingsverantwoordelijken’.

Indien Avans Persoonsgegevens moet aanleveren om gebruik te kunnen maken van diensten van een andere partij, waarbij die partij een zelfstandige verantwoordelijkheid heeft met betrekking tot de Verwerking van die Persoonsgegevens, dan worden de afspraken vastgelegd in de ‘Overeenkomst tussen twee of meer zelfstandig verwerkingsverantwoordelijken’.

Avans hanteert voor beide situaties haar eigen modelovereenkomst. Aanpassingen op het model of het gebruik van een ander model (bijvoorbeeld omdat de Verwerker goed kan beargumenteren waarom zij enkel haar eigen model kan hanteren) is alleen mogelijk na verplichte consultatie via de privacy officiers van Juridische Zaken.

4.9.3 Doorgifte binnen de Europese Economische Ruimte (hierna ‘EER’)

Avans verstrekt Persoonsgegevens alleen aan een ontvanger (zijnde Verwerker, Verwerkingsverantwoordelijke of Derde) gevestigd binnen de EER, als de Verwerking:
- is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 AVG; en
- voldoet aan artikel 9 AVG; en
- als de ontvanger voldoet aan de wettelijke vereisten uit de AVG.

De EER omvat alle landen van de Europese Unie plus Noorwegen, IJsland en Liechtenstein.

Meer informatie over het delen van gegevens kan worden gevonden in het privacystatement van Avans, onder de kop ‘Zo gaat Avans om met het verstrekken van gegevens aan derden’.

4.9.4 Doorgifte Persoonsgegevens buiten de EER

Avans kan Persoonsgegevens ook buiten de EER doorgeven. Dat kan alleen als:
- is voldaan aan de voorwaarden die gelden voor de doorgifte van Persoonsgegevens binnen de EER (zie paragraaf 4.9.3); en
- het betreffende land een passend beschermingsniveau heeft in overeenstemming met de Europese wetgeving; en
- aanvullende en passende afspraken zijn gemaakt, conform de criteria in de landenlijst Europese Commissie.

[4] Inkoopgerelateerde verwerkersovereenkomsten zijn verwerkersovereenkomsten die verband houden met een Verwerking waarvoor Avans een financiële tegenprestatie verricht.

Meer informatie over het delen van gegevens kan worden gevonden in het privacystatement van Avans, onder de kop 'Zo gaat Avans om met het verstrekken van gegevens aan derden'.

4.10 Informatiebeveiliging

Avans 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. Avans heeft een intern informatiebeveiligingsbeleid geïmplementeerd waarin maatregelen zijn uitgewerkt die de werknemers van Avans hanteren. Het betreffende informatiebeveiligingsbeleid is opgenomen in een separaat document, genaamd Informatiebeveiligingsbeleid Avans Hogeschool.

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

Bij Avans worden alle Persoonsgegevens (minimaal) als vertrouwelijk geclassificeerd. Eenieder 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.

4.11 Rechten van betrokkenen

De AVG geeft Betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. Een verzoek kan worden ingediend door te mailen naar privacy@avans.nl of door een formulier in te vullen waar in het privacystatement van Avans naar wordt verwezen.

Conform artikel 44 van de UAVG geldt voor de Verwerking van Persoonsgegevens in het kader van wetenschappelijk onderzoek dat het recht op inzage, het recht op rectificatie en het recht op beperking van de Verwerking niet geldt, mits er voorzieningen zijn getroffen om te garanderen dat de Persoonsgegevens alleen voor wetenschappelijke doeleinden kunnen worden gebruikt.

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

Mededeling aan Betrokkene
Avans 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 de Betrokkene. De taal zal worden afgestemd op de doelgroep.

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

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

4.11.1 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 de hem betreffende Persoonsgegevens. Als Avans veel gegevens van de Betrokkene verwerkt, mag Avans de Betrokkene voorafgaand aan de informatieverstrekking verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.

Mededeling
Indien Persoonsgegevens worden verwerkt, bevat de mededeling van Avans een volledig overzicht van de gevraagde Persoonsgegevens, inclusief, indien van toepassing:

- De Persoonsgegevens zelf.
- Een omschrijving van de doeleinden van de Verwerking.
- De categorieën van Persoonsgegevens waarop de Verwerking betrekking heeft.
- De ontvangers of categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties.
- De bewaartermijn van de Persoonsgegevens of, indien dat niet mogelijk is, de criteria om die termijn te bepalen.
- Alle beschikbare informatie over de bron van de Persoonsgegevens, als de Persoonsgegevens niet bij de Betrokkene zijn verzameld.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.
- De passende waarborgen die zijn getroffen, indien de Persoonsgegevens worden doorgegeven aan een derde land.
- Het recht van de Betrokkene om de Verwerkingsverantwoordelijke te verzoeken om rectificatie of verwijdering van zijn Persoonsgegevens, beperking of bezwaar van de Verwerking alsmede het recht op gegevensoverdraagbaarheid.
- Het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.

Kopie
De Betrokkene kan om een kopie van zijn Persoonsgegevens verzoeken, maar heeft niet zonder meer het recht op een kopie van alle documenten met zijn Persoonsgegevens. Wanneer de Betrokkene zijn verzoek elektronisch heeft ingediend, en niet om een andere regeling heeft verzocht, wordt de informatie in een gangbare elektronische vorm verstrekt.

Rechten en vrijheden van anderen
Avans zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen. Dit kan er bijvoorbeeld toe leiden dat bij het verstrekken van inzage in de Persoonsgegevens van Betrokkene, de gegevens die herleidbaar zijn tot anderen worden afgeschermd of weggelakt.

4.11.2 Recht op gegevensoverdraagbaarheid

Gronden voor verzoek
Iedere Betrokkene kan een verzoek indienen bij Avans om zijn Persoonsgegevens te verkrijgen in een gestructureerde, gangbare en machine leesbare vorm dan wel deze rechtstreeks aan een andere Verwerkingsverantwoordelijke over te laten dragen, zonder daarbij te worden gehinderd door Avans, indien is voldaan aan beide volgende voorwaarden:

1. De Verwerking door Avans 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
Avans zal bij verstrekking van de Persoonsgegevens rekening houden met de rechten en vrijheden van anderen.

Verwijderen van Persoonsgegevens
Indien een Betrokkene zijn recht van gegevensoverdraagbaarheid heeft uitgeoefend in het kader van een Verwerking ter uitvoering van een overeenkomst, mag Avans niet besluiten de gegevens te wissen. Na het verstrijken van de bewaartermijn, dient Avans de gegevens echter alsnog te wissen.

4.11.3 Recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking

Verzoek tot rectificatie, aanvulling, verwijdering of beperking

Iedere Betrokkene kan met betrekking tot de over hem opgenomen Persoonsgegevens verzoeken deze te corrigeren, aan te vullen, te verwijderen of de Verwerking te beperken. Bij het recht op beperking van de Verwerking worden de Persoonsgegevens tijdelijk afgeschermd en niet meer verwerkt door Avans. De beperking wordt duidelijk in het bestand aangegeven. Studenten of medewerkers van Avans kunnen bepaalde gegevens ook zelf wijzigen in Osiris of in het medewerkersportaal HR-selfservice.

Meer informatie over het recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking kan worden gevonden in het privacy statement van Avans, onder de kop 'Jouw rechten met betrekking tot jouw persoonsgegevens'.

Kennisgeving
Indien blijkt dat de verwerkte 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 Verwerkingsverantwoordelijke als de Verwerker zijn) deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken.

Bovendien worden Derden aan wie de Persoonsgegevens, 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 Avans deze mededeling heeft gedaan.

4.11.4 Recht van bezwaar

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

1. Iedere Betrokkene mag, in verband met zijn of haar persoonlijke omstandigheden, bezwaar maken tegen een Verwerking bij Avans, als deze Verwerking plaatsvindt op grond van
    a. de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag van de Verwerkingsverantwoordelijke, of
    b. de behartiging van het gerechtvaardigd belang van Avans of van een Derde aan wie de Persoonsgegevens worden verstrekt.

    Indien de Betrokkene bezwaar maakt, zal Avans de verdere Verwerking in beginsel staken. Indien Avans kan aantonen dat haar 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 Avans (kosteloos) de 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. Avans zal bij bezwaar de Verwerking voor direct marketing doeleinden direct staken en gestaakt houden.

4.11.5 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.

Slechts in de volgende drie situaties mag Avans besluiten nemen op grond van geautomatiseerde Verwerking:

1. Indien het besluit noodzakelijk is bij de sluiting of uitvoering van een overeenkomst met de Betrokkene.
2. Indien het besluit is toegestaan bij een Europese of nationale wet, mits deze wet voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene.
3. Indien het besluit berust op uitdrukkelijke toestemming van de Betrokkene. Deze toestemming kan te allen tijde worden ingetrokken.

In alle hierboven beschreven situaties, zal Avans passende maatregelen nemen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene. Hieronder zullen tenminste vallen het

recht op menselijke tussenkomst door Avans, het recht van de Betrokkene om zijn standpunt kenbaar te maken, alsmede het recht om het besluit aan te vechten. Minderjarigen zullen nimmer worden onderworpen aan geautomatiseerde besluitvorming.

4.11.6 Rechtsbescherming

Algemene klachten

Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de bescherming van zijn privacy, dan wel de bepalingen van dit Beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen door te mailen naar privacy@avans.nl. Uiteraard kan hij (daarna) ook contact opnemen met de Functionaris Gegevensbescherming van Avans. De Functionaris Gegevensbescherming is bereikbaar via privacy@avans.nl.

Overige bezwaarmogelijkheden

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

A. Verzoekschriftprocedure bij de rechtbank

Indien Avans afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 4.11 van dit Beleid, of Avans heeft het verzoek van de Betrokkene afgewezen, dan wel naar de opvatting van de Betrokkene onvoldoende beantwoord, dan heeft de Betrokkene op grond van artikel 35 lid 2 Uitvoeringswet Algemene Verordening Gegevensbescherming de mogelijkheid een verzoekschriftprocedure te starten bij de rechtbank.

Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van Avans ingediend te worden bij de rechtbank. Indien Avans 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. Verzoek tot handhaving bij toezichthoudende autoriteit

De Betrokkene heeft de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens, dan wel om een belangenorganisatie namens hem op te laten treden.

4.12 Verantwoordingsplicht

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

4.12.1 Register van verwerkingsactiviteiten

De proceseigenaar en de privacy officer van Avans zorgen er samen voor dat iedere (geheel of gedeeltelijk geautomatiseerde) Verwerking van Persoonsgegevens wordt opgenomen in het verwerkingsregister. Zij handelen daarbij conform de ‘Procesbeschrijving verwerkingsregister’ van Avans. De Functionaris Gegevensbescherming toetst of de inrichting van het verwerkingsregister voldoet aan de vereisten van artikel 30 AVG en draagt zorg voor de controle en monitoring van de documentatie/bewijsvoering van de geregistreerde Verwerkingen.

4.12.2 *Beoordeling gerechtvaardigd belang (Legitimate Interest Assessment)*

Indien de verwerking van persoonsgegevens wordt gebaseerd op het gerechtvaardigd belang van Avans, dient een zorgvuldige belangenafweging te worden gemaakt en gedocumenteerd. Bij deze belangenafweging wordt bepaald of de privacy risico’s voor betrokkenen niet hoger zijn dat het belang dat Avans heeft bij de verwerking van persoonsgegevens.
De verantwoordelijkheid daarvoor ligt altijd bij het (waarde- en service)team dat (of de proceseigenaar die) verantwoordelijk is voor de verwerking. Daarbij kan gebruik worden gemaakt van het ‘*Model beoordeling gerechtvaardigd belang*’.

4.12.3 Privacy Risk Assessment & Data Protection Impact Assessments

Bij (onderzoeks-)projecten, infrastructurele wijzigingen of nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen, voert Avans een DPIA uit conform het daarvoor opgestelde model.

Verwerkingen houden in ieder geval een hoog risico in voor betrokkenen, indien:

- er systematisch en uitgebreid persoonlijke aspecten worden geëvalueerd, gebaseerd op geautomatiseerde Verwerking, waaronder Profiling, en daarop besluiten worden gebaseerd die gevolgen hebben voor de Betrokkenen;
- op grote schaal Bijzondere of strafrechtelijke Persoonsgegevens worden verwerkt;
- op grote schaal en stelselmatige wijze mensen worden gevolgd in een publiek toegankelijk gebied;
- de Verwerking is opgenomen in de door de AP gepubliceerde lijst van Verwerkingen waarvoor het uitvoeren van een DPIA verplicht is;[5]
- de Verwerking voldoet aan twee of meer van de negen criteria die door de Europese privacy-toezichthouders zijn geformuleerd om te beoordelen of het uitvoeren van een DPIA verplicht is.[6]

Een DPIA wordt uitgevoerd voordat de nieuwe of gewijzigde Verwerking daadwerkelijk plaatsvindt.

Om te bepalen of een DPIA verplicht is, wordt allereerst een Privacy Risk Assessment (PRA) uitgevoerd. Het PRA is de eerste inventarisatie van de kenmerken van de Verwerking en de daaraan verbonden privacyrisico's, en is zo opgebouwd dat snel duidelijk wordt of de AVG van toepassing is en of een DPIA moet worden verricht.

Elke DPIA wordt ter advies voorgelegd aan de Functionaris Gegevensbescherming. De Functionaris Gegevensbescherming brengt zijn advies uit aan de Verwerkingsverantwoordelijke.

Indien de Verwerking een hoog risico zou betekenen als Avans geen maatregelen neemt om het risico te beperken, raadpleegt Avans voorafgaand aan de Verwerking de toezichthoudende autoriteit.

4.12.4 Datalekregister

Van een Datalek is sprake in geval van toegang tot of vernietiging, wijziging of het vrijkomen van Persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie. Het kan hierbij bijvoorbeeld gaan om de diefstal van een laptop, een verloren usb-stick, een verkeerd uitgegeven autorisatie, een e-mail die naar de verkeerde persoon is verstuurd of om een geslaagde ransomware-aanval waardoor Persoonsgegevens niet beschikbaar zijn. Ieder Datalek wordt opgenomen in het datalekregister. Sommige Datalekken moeten daarnaast worden gemeld bij de Betrokkene en/of de toezichthoudende autoriteit. Daarover beslist de privacy officer die het Datalek in behandeling heeft genomen, zo nodig in overleg met de Functionaris Gegevensbescherming. Melding bij de toezichthoudende autoriteit dient binnen 72 na ontdekking plaats te vinden.

Avans heeft een procedure voor het afhandelen van Datalekken opgenomen in een separaat document, genaamd ‘Protocol Datalekken’.

[5] Welke lijst kan worden teruggevonden op de website van de AP: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667
[6] Welke criteria kunnen worden teruggevonden op de website van de AP: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668

5 Tot slot

5.1 Vaststelling

Dit Beleid is vastgesteld door het College van Bestuur van Avans, d.d. 09-04-2024.

5.1.1 Ingangsdatum

Dit Beleid treedt in werking per 09-04-2024.

5.1.2 Einddatum

Voor dit Beleid geldt geen specifieke einddatum. Het Beleid geldt totdat het wordt herzien dan wel ingetrokken. Herziening dan wel intrekking gebeurt onder verantwoordelijkheid van de beleidsverantwoordelijke eenheid Diensteenheid ICT en Facilitaire Dienst (hierna: DIF) en bij besluit van het College van Bestuur van Avans.

5.1.3 Uiterste evaluatiedatum

In het kader van de PDCA-cyclus van Avans, wordt minimaal eens in de twee jaar, of eerder indien daar aanleiding toe is, beoordeeld of dit Beleid herzien moet worden.

5.2 Publicatie

Persoonsgegevens moeten verwerkt worden op een manier die transparant is voor de Betrokkene. Transparantie houdt in dat het voor de Betrokkene duidelijk moet zijn dat zijn Persoonsgegevens verzameld, gebruikt, geraadpleegd of op een andere manier verwerkt worden, waarom en door wie.

In het kader van de transparantie stelt Avans dit Beleid beschikbaar: in voorliggende vorm alsook in de vorm van een privacystatement.

5.2.1 Privacystatement

Afgeleid van dit beleidsdocument, stelt Avans een privacystatement op. Het privacystatement wordt gepubliceerd de website van Avans.

Het privacystatement is openbaar en daarmee beschikbaar voor alle Betrokkenen van Avans. Avans beoogt hiermee Betrokkenen op een toegankelijke wijze te informeren over de wijze waarop zij omgaat met Persoonsgegevens van studenten, medewerkers en overige Betrokkenen.

5.2.2 Privacybeleid

Voorliggend beleidsdocument is openbaar en wordt gepubliceerd op het intranet van Avans.

Bijlage A Definities

Anonimiseren: is een methode waarbij Persoonsgegevens zodanig worden bewerkt dat deze niet meer gebruikt kunnen worden om een persoon te identificeren. Ook niet als deze gegevens gecombineerd worden met andere gegevens. Deze bewerking is onomkeerbaar. Na volledige anonimisering van gegevens is de privacywet- en regelgeving niet meer van toepassing op die gegevens.

AVG: Algemene Verordening Gegevensbescherming.

Beleid: Dit beleid met betrekking tot het verwerken van Persoonsgegevens onder de verantwoordelijkheid van Avans.

Betrokkene: Een geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft.

Bijzondere persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling): Een beoordeling van een Verwerking die helpt bij het beoordelen van de rechtmatigheid van de Verwerking, het identificeren van privacy risico's en die maatregelen voorstelt om deze risico's te verkleinen tot een acceptabel niveau.

Datalek: Een inbreuk op de beveiliging van Persoonsgegevens, die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Derde: Een partij, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker, die gemachtigd is om Persoonsgegevens te verwerken.

Encryptie: Het versleutelen van gegevens op basis van een bepaald algoritme. Het belangrijkste doel van encryptie is dat de veiligheid van gegevens gewaarborgd blijft, óók als derden toegang zouden verkrijgen tot het opslagmedium of het communicatiekanaal. De versleuteling zorgt er dan voor dat deze derden de gegevens niet kunnen lezen.

Functionaris Gegevensbescherming (FG): De persoon die door Avans is aangewezen om intern toe te zien op naleving van privacywetgeving en te adviseren op nader in de AVG genoemde specifieke onderwerpen. De Functionaris Gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens en heeft een FG-nummer toegekend gekregen. De wettelijke taken en bevoegdheden van de Functionaris Gegevensbescherming geven deze functionaris een onafhankelijke positie bij Avans.

Minderjarige: Iedereen die de leeftijd van 16 jaar nog niet heeft bereikt is in het kader van de privacywetgeving minderjarig.

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

Privacy by default: Het toepassen van standaardinstellingen ('default settings') op een zodanige wijze dat de privacy van Betrokkenen zo optimaal mogelijk wordt gewaarborgd in het proces (de Verwerking). Dit betekent onder meer dat er zo min mogelijk Persoonsgegevens worden gevraagd en verwerkt, en bijvoorbeeld dat check boxes aan de hand waarvan iemand wordt gevraagd om toestemming te geven voor een bepaalde Verwerking, niet vooraf mogen zijn aangevinkt.

Privacy by design: Houdt in dat er al tijdens het ontwerpen van producten en diensten (zoals informatiesystemen) voor wordt gezorgd dat Persoonsgegevens goed worden beschermd, bijvoorbeeld door gegevens niet langer te bewaren dan nodig (recordmanagement) en door enkel de gegevens te verzamelen die noodzakelijk zijn om het doel van de beoogde Verwerking te bereiken (dataminimalisatie).

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.

Pseudonimiseren: Met pseudonimiseren worden persoonsgegevens getransformeerd in een dataset die niet meer direct herleidbaar is tot een persoon. Om dit te doen worden de direct identificeerbare elementen van een set Persoonsgegevens, zoals een naam, weggehaald, of wordt de dataset omgecodeerd tot een nummer. Vervolgens worden de gepseudonimiseerde dataset en de (sleutel tot de) brondata apart bewaard en zijn er waarborgen aanwezig die re-identificatie voorkomen (bijv. beleid of contracten). Belangrijk is dat de originele identificerende elementen, of de brondata, nog aanwezig zijn. Wanneer deze data vernietigd zijn, of re-identificatie anderszins onmogelijk is, is sprake van anonieme gegevens.

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming.

Verwerkingsverantwoordelijke: De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt.

Verwerker: Een partij die ten behoeve van en op instructie van Avans Persoonsgegevens verwerkt, zonder dat deze partij onder rechtstreeks gezag van Avans staat.

Verwerking: Elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige ander vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Bijlage B Samenhang Informatiebeveiliging en Privacy

Binnen Avans gelden de termen privacy en informatiebeveiliging als synergetische, overlappende onderwerpen. Heb je het over privacy, dan bedoel je vaak informatiebeveiliging, en vice versa. Privacy gaat echter over het correct, voor een bepaald doel, gebruiken van verzamelde Persoonsgegevens. Informatiebeveiliging daarentegen, draait om de inspanningen die we verrichten om te zorgen dat deze gegevens vertrouwelijk, integer en beschikbaar blijven.

Informatiebeveiliging	**Privacy**
Informatiebeveiliging omvat alle gegevens van een organisatie.	Privacy gaat alleen over Persoonsgegevens.
Informatiebeveiliging beschermt de organisatie.	Privacy beschermt de mensen.
Informatiebeveiliging is gericht op de belangen van de organisatie zelf. Het doel van het informatiebeveiligingsbeleid is om de continuïteit van de organisatie te waarborgen, en te voorkomen dat gevoelige informatie op straat komt te liggen.	Privacy is erop gericht de rechten en vrijheden van natuurlijke personen te beschermen en beschermt mensen binnen en buiten de organisatie tegen misbruik van hun gegevens. Ook tegen overmatig gebruik van de gegevens door de organisatie zelf.
Informatiebeveiliging zorgt ervoor dat beveiligingsincidenten, zoals Datalekken, adequaat worden opgelost.	Vanuit privacy is het belangrijk om Datalekken op te lossen. Hiervoor bestaat de afhankelijkheid van informatiebeveiliging waar beveiligingsincidenten (inclusief Datalekken) worden opgelost.
Informatiebeveiliging leunt op drie kernbegrippen: vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Samen bepalen zij de betrouwbaarheid van informatiesystemen binnen de organisatie.	Privacy is erop gericht dat iedere Verwerking van Persoonsgegevens binnen de organisatie rechtmatig, behoorlijk en transparant plaatsvindt. De kernbegrippen vertrouwelijkheid, integriteit en beschikbaarheid spelen wel een rol binnen privacy, maar vormen niet de kern. Voor privacy zijn vooral de begrippen doelbinding, dataminimalisatie, juistheid en opslagbeperking van belang.
De organisatie van informatiebeveiliging is een cyclisch proces op basis van de Plan-Do-Check Act-cyclus. De organisatie krijgt hierdoor steeds beter grip op informatiebeveiliging en verbetert continu. Hiervoor bestaat een internationale richtlijn ISO 27001 voor een Information Security Management System (ISMS). Binnen Avans wordt momenteel gewerkt in de geest van ISO 27001. De ambitie bestaat wel om de organisatie voor ISO 27001 binnen afzienbare tijd te certificeren.	Ook voor privacy wordt de PDCA-aanpak steeds belangrijker. Sinds enkele jaren bestaat internationaal de ISO 27701 als privacy-uitbreiding van de ISO 27001. ISO 27701 beschrijft een Privacy Information Management System (PIMS). Binnen Avans vindt integratie van privacy management plaats in het ISMS. Avans beraadt zich momenteel nog of zij zich op termijn ook voor ISO 27701 wil certificeren.
Informatiebeveiliging is binnen Avans strategisch georganiseerd op basis van het Three Lines of Defense principe. De CISO heeft hierbinnen een centrale rol vanuit de tweede lijn voor advies, ondersteuning en controle. De CISO wordt ondersteund door een team van Cyber Security Managers en security specialisten in de IT-operatie. De uitvoerende verantwoordelijkheid ligt bij de diensten en academies. De eindverantwoordelijkheid ligt bij het College van Bestuur.	Privacy is eveneens georganiseerd op basis van het Three Lines of Defense principe (zie paragraaf 3.3). De privacy officer heeft een vergelijkbare rol als de CISO voor informatiebeveiliging. En die wordt ondersteund door een team van privacy officers. Een verschil met de organisatie voor informatiebeveiliging is de rol van de Functionaris Gegevensbescherming. De Functionaris Gegevensbescherming heeft een onafhankelijke beschermde rol om Avans als organisatie als geheel te kunnen ondersteunen, adviseren en beoordelen op het vlak van privacybeleid en -beheer.