UNIVERSITEIT VAN AMSTERDAM

PRIVACYBELEID EN BELEID VERWERKING PERSOONSGEGEVENS UNIVERSITEIT VAN AMSTERDAM

Inhoud

1. Inleiding

Het verwerken van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van de Universiteit Van Amsterdam (UvA). Dit dient met de grootste zorgvuldigheid te gebeuren, omdat misbruik van persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere betrokkenen bij de UvA (waaronder alumni), maar ook bij de UvA zelf. De UvA hecht dan ook veel waarde aan het beschermen van persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop de persoonsgegevens worden verwerkt. Het op de juiste manier verwerken van persoonsgegevens is de verantwoordelijkheid van het College van Bestuur[1]. Aan die verantwoordelijkheid wordt (mede) inhoud gegeven door middel van voorlichting, scholing en het geven van richtlijnen over het verwerken van persoonsgegevens. Ook het bieden van een deugdelijke rechtsbescherming met betrekking tot de bescherming van persoonsgegevens valt onder deze verantwoordelijkheid.
Met het beschrijven van de maatregelen in dit beleidsdocument beoogt - en neemt de UvA haar verantwoordelijkheid - om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te borgen en daarmee te voldoen aan relevante wet- en regelgeving.

1.1 Definities

Beleid: dit beleid met betrekking tot de verwerking van persoonsgegevens van de UvA.

Persoonsgegeven: een gegeven dat betrekking heeft op een geïdentificeerde of identificeerbaar natuurlijke persoon. Een persoon is identificeerbaar indien zijn identiteit nog niet is vastgesteld, maar dit redelijkerwijs, zonder onevenredige inspanning, wel kan gebeuren.

Betrokkene: een natuurlijk persoon op wie de gegevens betrekking hebben wordt de betrokkene genoemd.

Verantwoordelijke: het College van Bestuur van de UvA die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: de partij die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. Dit kan een door de UvA ingeschakelde (derde) partij zijn, maar er zijn ook situaties denkbaar waarin de UvA als verwerker optreedt ten behoeve van een (derde) verantwoordelijke.
Verwerking: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés. Veel voorkomende verwerkingshandelingen zijn: verzamelen, vastleggen, opvragen, raadplegen, opslaan, gebruiken, verstrekken, wissen en vernietigen.

Derde(n): ieder ander, niet zijnde de betrokkene, noch verantwoordelijke, noch verwerker, noch ieder ander die onder rechtstreeks gezag valt van de verantwoordelijke of de verwerker en gemachtigd is om persoonsgegevens te verwerken.

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

[1] De verantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming (AVG) is degene die formeel-juridisch de zeggenschap over de verwerking heeft. Het gaat om degene die bevoegd is het doel en de middelen voor de verwerking vast te stellen. Dat laat onverlet dat het feitelijk beheer over de gegevensverwerking aan een ander kan worden gemandateerd. De ratio hiervan is dat een betrokkene kan weten bij wie hij zijn rechten desgewenst kan uit oefenen. Bij de UvA is het College van Bestuur de verantwoordelijke. Dit vloeit voort uit de Algemene wet bestuursrecht (Awb) en de artikelen 9.2 en 9.5 van de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW).

Privacy by design: het meenemen van privacy en gegevensbescherming als voorwaarden voor de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt.

Privacy Impact Assessment (PIA) / Privacyeffectbeoordeling: een gestandaardiseerde procedure die helpt om bij een voorgenomen verwerking van persoonsgegevens de privacyrisico's te identificeren en handvatten aan te dragen om de privacyrisico' s te verkleinen tot een acceptabel niveau.

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

1.2 Reikwijdte en doelstelling van het Beleid

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

In het Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de UvA alsmede op de daaraan ten grondslag liggende documenten. Eveneens is het Beleid van toepassing op niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Het Beleid ziet niet op het verwerken van persoons-gegevens voor persoonlijk gebruik, zoals persoonlijke werkaantekeningen.
Bij de UvA wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoons-gegevens. Er wordt aandacht geschonken aan deze raakvlakken en er wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het Beleid bij de UvA heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te borgen 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 de persoonsgegevens veilig zijn bij de UvA.

Doelstelling van het Beleid voor de UvA is concreet het volgende:

- **Het bieden van een kader:** het Beleid biedt een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde norm of 'best practice'; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie eenduidig vorm te geven.
- **Het stellen van normen:** de basis voor de beveiliging van persoonsgegevens is ISO 27001[2] Maatregelen worden genomen op basis van 'best practices' in het hoger onderwijs en op basis van ISO 27002[3]. De laatste versie van het Juridisch Normenkader Cloudservices Hoger Onderwijs[4] wordt gehanteerd als 'best practice' voor Cloud services en andere outsource contracten.

2 Voluit: NEN-1SO/IEC 27001: Eisen aan managementsystemen voor informatiebeveiliging.

3 Voluit: NEN-1SO/IEC 27002: Code voor informatiebeveiliging.

4 SURF taskforce Cloud, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014 en geactualiseerd in oktober 2016, te vinden via https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger- onderwijs.html.

- **Het nemen van de verantwoordelijkheid:** het College van Bestuur neemt haar verantwoordelijkheid door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor alle betrokkenen binnen de UvA.
- **Compliant worden/blijven** 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 vermijding van risico's als gevolg van het niet compliant zijn met relevante wet- en regelgeving.

1.3 Beleid in relatie tot verbonden partijen

Rechtspersonen en vennootschappen waarmee de UvA geheel of gedeeltelijk is verbonden zijn zelf verantwoordelijk voor het beleid met betrekking tot hun verwerking van persoonsgegevens. Dit betekent dat dit Beleid niet onverkort op hen van toepassing is. De Functionaris Gegevensbescherming (FG) van de UvA houdt geen toezicht op naleving van de privacywetgeving door deze rechtspersonen en vennootschappen.

2. Beleidsprincipes verwerking persoonsgegevens

2.1 Beleidsuitgangspunt en -principes

Algemeen uitgangspunt is dat persoonsgegevens in overeenstemming met relevante wet- en regelgeving op een behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van de UvA om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving keuzes te maken met betrekking tot zijn of haar persoonsgegevens.
Om aan bovenstaand beleidsuitgangspunt te voldoen, gelden de volgende principes:

- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijke, welbepaalde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd en houden direct of indirect altijd verband met het verzorgen van onderwijs of het uitvoeren van onderzoek.
- Ieder verwerkingsdoel is gebaseerd op een van de zes wettelijke grondslagen, zoals genoemd in artikel 6 lid 1 Algemene Verordening Gegevensbescherming (AVG): toestemming van betrokkene[5]; noodzakelijk voor het uitvoeren van een overeenkomst; een wettelijke verplichting; het beschermen van een vitaal belang; het vervullen van een taak van algemeen belang of openbaar gezag; of een gerechtvaardigd belang[6].
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigingstermijnen in acht genomen.
- Bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (dataminimalisatie).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (zie pagina 6, 'het stellen van normen').

5 Indien wetenschappelijk onderzoek erkende ethische normen in acht neemt, is een generiekere vorm van toestemming mogelijk (artikel 4 lid 11 AVG en overweging 33)

6 Hoewel dat vaak wordt gedacht, is er voor een verwerking dus niet altijd toestemming vereist.

- Iedere betrokkene heeft recht op informatie over de verwerkingen; inzage in zijn/haar gegevens; correctie van zijn/haar gegevens als deze niet kloppen; verwijdering van de gegevens en het 'recht om vergeten te worden'; beperking van de gegevensverwerking; verzet tegen de gegevensverwerking; en overdracht van zijn/haar gegevens (dataportabiliteit) (zie hoofdstuk 8, 'rechten van betrokkenen').
- Bij alle verwerkingen die zijn gebaseerd op toestemming van de betrokkene, wordt het recht geboden om deze toestemming in te trekken. Het intrekken van toestemming dient in alle gevallen net zo eenvoudig te zijn als het geven daarvan.

3. Wet- en regelgeving

In dit hoofdstuk komt de voor de UvA relevante wet- en regelgeving aan bod, waar zij bij de verwerking van persoonsgegevens mee te maken heeft (niet limitatief).

3.1 Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW)

De UvA is een publiekrechtelijke rechtspersoon op grond van artikel 1.8, tweede lid, juncto bijlage 1 onder a, van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). De bestuurlijke structuur is vastgelegd in de WHW en in het daarop gebaseerde Universiteitsreglement, en is in overeenstemming met de Code goed bestuur universiteiten van de VSNU (versie 2017)[7]. De UvA heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (wetenschappelijk) onderzoek[8] nageleefd en toegepast.

3.2 Wet bescherming persoonsgegevens (Wbp)

De Wet bescherming persoonsgegevens (Wbp) is op 25 mei 2018 vervangen door de Algemene Verordening Gegevensbescherming. Onderliggend Beleid is daarom vormgegeven op basis van de bepalingen uit de AVG (zie volgende paragraaf).

3.3 Algemene Verordening Gegevensbescherming (AVG)

25 mei 2018 is de AVG rechtstreeks van toepassing in alle lidstaten van de Europese Unie. De AVG is de opvolger van de Wbp in Nederland en kent onder andere striktere eisen voor documentatie van verwerkingen en verantwoording naar betrokkenen. De UvA heeft deze striktere eisen uit de AVG verwerkt in dit Beleid.

3.4 Archiefwet

De UvA houdt zich aan de voorschriften van de Archiefwet over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en dergelijke. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

Vanzelfsprekend worden er - met het oog op de archivering - krachtens de AVG passende waarborgen getroffen voor de bescherming van de rechten en vrijheden van betrokkenen.

7 Code goed bestuur, versie 2017. Te vinden via: www.vsnu.nl > domeinen > Governance & Accountability > Code goed bestuur.
Direct link: https://www.vsnu.nl/files/documenten/Domeinen/Governance/Code%20Goed%20Bestuur%202017.pdf

8 Dit betreft onder andere De Nederlandse Gedragscode Wetenschapsbeoefening, 2014. Te vinden via: > domeinen > Governance & Accountability > Nederlandse gedragscode Wetenschapsbeoefening. Direct link: http://www.vsnu.nl/files/documenten/Domeinen/Onderzoek/Code_wetenschapsbeoefening_2004_(2014).pdf

4. Rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens

Om verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken is bij de UvA een aantal rollen onderkend die aan verschillende functionarissen binnen de organisatie zijn toegewezen. De toegang tot (de verwerking van) persoonsgegevens wordt door middel van autorisatietabellen afgebakend. In de autorisatietabel wordt de volgende informatie opgenomen: naam of namen van de geautoriseerde(n) functionaris, functie, duur en omvang van de toegestane handelingen. In dit hoofdstuk worden de rollen in algemene zin toegelicht.

De betrokken (externe) partij(en) en de eigenschappen van de verwerking(en) worden per verwerking vastgelegd in een verwerkingsregister. Het verwerkingsregister betreft een feitelijk en actueel overzicht van de verwerkingsactiviteiten waarvoor het College van Bestuur Verantwoordelijke is (zie paragraaf 2 van hoofdstuk 6).

4.1 Het College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen de UvA en stelt naast het Beleid, de uitwerking van het Beleid vast door middel van maatregelen en procedures op het gebied van verwerkingsactiviteiten.

4.2 Portefeuillehouder beveiliging persoonsgegevens

De portefeuillehouder financiën en bedrijfsvoering is het lid van het College van Bestuur dat privacy in portefeuille heeft. Hij/zij is eerstverantwoordelijke voor de beveiliging van persoonsgegevens binnen de UvA.

4.3 Functionaris gegevensbescherming (FG)

De FG heeft allereerst een informerende en adviserende rol binnen de UvA. De FG bevordert het privacy bewustzijn van betrokkenen, bijvoorbeeld door informatie via de UvA-website te verstrekken over privacy en de daaruit voortvloeiende rechten.
De FG dient tevens als aanspreekpunt voor degenen die vragen hebben over de bescherming van persoonsgegevens (contact: fg@uva.nl).
De FG beheert het register van meldingen van verwerkingen van persoonsgegevens en houdt toezicht op de toepassing en naleving van de AVG en het interne gegevensbeschermingsbeleid van de UvA.
De FG is niet verantwoordelijk voor het uitvoeren van PIA'S, maar met het oog op het informeren, adviseren over en toezien op de naleving van de AVG, wordt de FG wel tijdig betrokken bij het uitvoeren van PIA's.
In verband met voornoemde taken, brengt de FG jaarlijks een verslag uit aan het College van Bestuur. Het College van Bestuur deelt de bevindingen uit de verslaglegging van de FG met de Centrale Ondernemingsraad (COR) en de Centrale Studentenraad (CSR).
De FG vervult een onafhankelijke positie binnen de UvA. Dit houdt onder andere in dat er geen instructies aan de FG mogen worden gegeven.

4.4 Systeemeigenaar

De systeemeigenaar[9] is ervoor verantwoordelijk dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces en voldoet aan het Beleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu, als in de toekomst de applicatie en bijbehorende ICT-faciliteiten beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.

9 De systeemeigenaar is verantwoordelijk voor de beschikbaarheid en kwaliteit van de informatiediensten die door het systeem geleverd worden. Het systeemeigenaarschap wordt belegd op het niveau van afdelingshoofd; divisiemanager of directeur.

4.5 Leidinggevende

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

4.6. Chief Information Security Officer (CISO)

De CISO is verantwoordelijk voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid binnen de UvA. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan de organisatorische en technische beveiligingsmaatregelen.

5. Implementatie van beleid

Het College van Bestuur van de UvA is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. Zij wordt aangemerkt als verantwoordelijke in de zin van de AVG. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van de UvA uitgevoerd. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de UvA, zoals medewerkers, studenten, subsidieverstrekkers en partners, alsmede de samenleving als geheel. De UvA streeft een goed corporate governance-beleid na en heeft in dit verband aandacht voor de rechten van alle betrokkenen, zoals geformuleerd in de Code goed bestuur universiteiten van de VSNU.[10]

5.1 Verdeling van de verantwoordelijkheden

Iedere medewerker heeft overeenkomstig zijn rol een eigen verantwoordelijkheid. Het zorgvuldig verwerken van persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid: dit betekent dat de lijnmanagers (afdelingshoofden/centrale diensten) de primaire verantwoordelijkheid dragen voor zorgvuldige verwerking van persoonsgegevens op hun afdeling/eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder 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 verwacht dat zij zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk door een doen of nalaten[11] onveilige situaties ontstaan die leiden tot schade en/of imagoverlies voor de UvA of van individuen. De UvA informeert haar studenten en medewerkers over de verwerking van persoonsgegevens en bijbehorende verantwoordelijkheden, via de privacy- en cookiestatement en door middel van informatie op intranet (o.a. in de zo-genoemde ‘A-Z lijst’ onder ‘AVG’ en ‘Privacy’)

5.2 Inpassing in de instellingsgovernance/ afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

10 Artikel 2.1.2 van de Code goed bestuur universiteiten van de VSNU.

11 Het nalaten kan bestaan uit het niet melden van een verwerking van persoonsgegevens die gemeld had moeten worden of het niet melden van een datalek.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, bereik en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt ingevuld in het overleg tussen het College van Bestuur en de decanen (CBO).

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen en evaluatie-methoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld in het overleg tussen het College van Bestuur, de directeuren van de centrale stafdiensten en de directeuren van de centrale diensten (BVO).

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering en uitvoering aangaan. Het operationeel niveau wordt ingevuld door de directeuren van de centrale diensten en de directeuren bedrijfsvoering, alsmede door (groepen van) medewerkers waar de directeuren leiding aan geven.

5.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van verwerking van persoons-gegevens uit te sluiten. Noodzakelijk is het om bij de UvA het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Deze campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met andere beveiligingscampagnes. Verhoging van het bewustzijn is de verantwoordelijkheid van de FG, de CISO en de leidinggevende.

5.4 Controle en naleving

De FG houdt toezicht op de naleving van de privacywetgeving en het Beleid, inclusief de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van personeel en stemt dit af met de Chief Information Security Officer (CISO). Aanvullend hierop maken audits het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit.

Externe controles worden uitgevoerd door onafhankelijke en erkende deskundigen op het terrein van gegevensbescherming en -beveiliging. Dit wordt zo veel mogelijk geïntegreerd met de normale Planning en Control cyclus en wordt - indien nodig - gekoppeld aan het jaarlijkse accountants-onderzoek.

Indien de UvA persoonsgegevens laat verwerken door een externe verwerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen de verantwoordelijke en de verwerker (verwerkersovereenkomst). De door de UvA ingeschakelde verwerkers worden door middel van de verwerkersovereenkomst gebonden aan het Beleid en - eveneens krachtens deze verwerkersovereenkomst - verplicht om mee te werken aan de externe controles.

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

5.5 Privacy by Design & Privacy Impact Assessment (PIA)

Bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy en gegevensbescherming. Dit houdt onder andere in dat de UvA handelt conform haar beleidsuitgangspunten en -principes (paragraaf 2.1), betrokkenen informeert over de functies en de verwerking van persoonsgegevens (paragraaf 8.1), haar systemen beveiligt en zij haar betrokkenen in staat stelt om hun rechten uit te oefenen (hoofdstuk 8).

Bij nieuwe systemen die een hoog risico voor de privacy rechten en - vrijheden van betrokkenen opleveren, wordt er standaard een PIA uitgevoerd.[12] Bij het vaststellen van het risico houdt de UvA - krachtens de AVG - rekening met onder andere: het aantal betrokkenen, de categorieën van persoonsgegevens en of het een verwerking betreft waarin gegevens met derden worden verwerkt.

In een PIA worden de effecten van een voorgenomen verwerkingsactiviteiten beoordeeld en worden deze gestandaardiseerd in kaart gebracht. Op basis hiervan worden maatregelen getroffen om de geconstateerde effecten te voorkomen of te verkleinen. Het is de taak van de FG om risico's te signaleren.

De PIA wordt uitgevoerd door of namens het College van Bestuur als verwerkingsverantwoordelijke. De FG wordt, met het oog op zijn/haar taak, tijdig betrokken bij het uitvoeren van de PIA.

6. Rechtmatige en zorgvuldige verwerking van persoonsgegevens

6.1 Grondslag, doelbinding en belangenafweging

Het verwerken van persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 6 lid 1 AVG. Hoewel dat vaak wordt gedacht, is er voor een verwerking dus niet altijd toestemming vereist.
De verantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen.

De UvA treft de nodige maatregelen om te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij zijn verzameld en vervolgens worden verwerkt, juist en nauwkeurig zijn.
De UvA hanteert bij de implementatie het principe 'privacy by design' (zie paragraaf 5.5).

6.2 Documenteren van verwerkingen

Gegevensverwerkingen worden gemeld bij de FG.
De FG draagt zorg voor de registratie van deze meldingen. In het register worden niet de daadwerkelijke persoonsgegevens opgenomen, maar wordt er door beschrijvingen inzicht gegeven in de verwerkingsactiviteiten. Dit wordt vorm gegeven, door middel van de volgende informatie[13]:

(a) de naam en de contactgegevens van: de FG van de UvA, de verwerkingsverantwoordelijke en van eventuele gezamenlijke verwerkingsverantwoordelijken;
(b) de verwerkingsdoeleinden;
(c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
(d) een lijst van organisaties aan wie de persoonsgegevens worden verstrekt[14];
(e) een lijst van derde landen naar wie de persoonsgegevens worden doorgegeven;
(f) de beoogde bewaartermijnen; en
(g) een beschrijving van de genomen beveiligingsmaatregelen.

12 In veel gevallen zal het uitvoeren van een PIA een onderdeel zijn van het inkoopproces. Afhankelijk van de concrete omstandigheden van het geval kunnen ook andere afdelingen of functionarissen hier mee te maken krijgen.
13 Conform artikel 30 lid 1 AVG.
14 Dit geldt zowel voor de ontvangers in derde landen als ontvanger binnen de EU, zie art. 30 lid 1 sub d

Voor de gevallen dat de UvA als verwerker optreedt houdt zij ook een register aan. Voor die gevallen wordt de volgende informatie in het register opgenomen[15]:
(a) de naam en de contactgegevens van: de FG van de UvA, de verwerker(s) en de verwerkingsverantwoordelijke voor rekening waarvan de UvA handelt;
(b) de categorieën van verwerkingen;
(c) een lijst van derde landen naar wie de persoonsgegevens worden doorgegeven en documenten inzake passende waarborgen; en
(d) een beschrijving van de genomen beveiligingsmaatregelen.

Het register is voor de FG een middel om zijn taken rondom het toezicht op de naleving van de AVG te vervullen en de organisatie te informeren en adviseren over de gegevensverwerking die plaatsvindt.

6.3 Organisatie van de beveiliging
De UvA 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 privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van de UvA.

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

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

6.5 Bewaartermijnen/vernietigingstermijnen per soort gegeven
Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie gebracht te worden. De UvA zal de persoonsgegevens na het verstrijken van de bewaartermijn vernietigen of - indien noodzakelijk voor historische, statistische of wetenschappelijke doeleinden of in het algemeen belang - in een archief bewaren. Uiteraard worden de gearchiveerde persoonsgegevens onderworpen aan passende waarborgen zoals omschreven in artikel 24 AVG.

6.6 Bijzondere persoonsgegevens
Het verwerken van bijzondere persoonsgegevens is verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar basisbescherming niet voldoende is, moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

15 Conform artikel 30 lid 2 AVG.

6.7 Doorgifte persoonsgegevens aan derden

6.7.1 Uitbesteden van verwerking aan een verwerker
Indien de UvA persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen de verantwoordelijke en de verwerker.

6.7.2 Uitgifte persoonsgegevens binnen de Europese Unie
De AVG heeft rechtstreekse werking binnen de gehele Europese Unie en harmoniseert daarmee de regels voor de bescherming van persoonsgegevens. Bij het verstrekken van persoonsgegevens binnen de EU hanteert de UvA daarom geen extra controle met betrekking tot het beschermingsniveau van het desbetreffende EU-land. Uiteraard verstrekt de UvA persoonsgegevens alleen aan derden als doorgifte van de persoonsgegevens is gebaseerd op een wettelijke grondslag.

6.7.3 Uitgifte persoonsgegevens buiten de Europese Unie
UvA verstrekt persoonsgegevens alleen aan derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of dat bedrijf of die instelling specifiek een passend beschermingsniveau waarborgt.[16] Daarbij hanteert UvA als uitgangspunt de lijst met landen met passend beschermingsniveau van de Europese Commissie (de zogenoemde *adequaatheids-besluiten*).[17] De Europese Commissie heeft voor de Verenigde Staten bepaald dat er een passend beschermingsniveau aanwezig is, voor zover de ontvangende partij zichzelf heeft verplicht zich te houden aan de principes zoals vastgelegd in het adequaatheidsbesluit, genaamd het 'Privacy Shield'. [18]
UvA verstrekt persoonsgegevens enkel aan landen zonder een passend beschermingsniveau, indien zij hier een vergunning van de minister van Veiligheid en Justitie voor heeft verkregen, dan wel op basis van standaard contractbepalingen die zijn vastgesteld door de Europese Commissie of de Autoriteit Persoonsgegevens.[19]

7. Incidenten met betrekking tot persoonsgegevens

Iedere melding over een (vermeend) onjuiste verwerking van persoonsgegevens is een incident. De bekendste vorm van een incident is een datalek. Dit hoofdstuk beschrijft het Beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1 Melding en registratie
Een datalek[20] kan tijdens kantooruren worden gemeld bij de ICTS Servicedesk via servicedesk-icts@uva.nl of telefonisch op 020-5252200. Buiten kantooruren of bij ernstige beveiligings-incidenten kan dit rechtstreeks bij CERT- UvA[21] via cert@uva.nl of telefonisch op 020-5253322. Van elk incident en de afhandeling daarvan wordt een registratie bijgehouden. Een incident kan gemeld worden door een betrokkene, een verwerker of een derde.

16 Artikel 44 AVG
17 Deze lijst is te vinden via de volgende link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
18 Zie voor meer informatie: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en
19 Artikel 46 en 49 AVG
20 Voorbeelden van een 'datalek' zijn een gehackte computer of e-mailbox, het verliezen van vertrouwelijke informatie op een laptop, fysiek dossier, telefoon of USB-stick, gevolg geven aan instructies uit een phishing e-mail of een virusuitbraak (ransomware).
21 CERT staat voor Computer Emerging Response Team en is gevestigd in Gebouw Leeuwenburg, Weesperzijde 190, 1097 DZ Amsterdam.

7.2 Afhandeling

Incidenten worden zo veel mogelijk ter afhandeling doorgezet naar de verantwoordelijke afdeling of persoon.
Als de persoonsgegevens van betrokkene of de bedrijfsprocessen, de financiën of de reputatie van de UvA ernstig in gevaar zijn, worden in ieder geval het College van Bestuur en de FG op de hoogte gesteld. Van een situatie als bedoeld in de vorige volzin is in ieder geval sprake ingeval van een (een ernstig vermoeden van) een datalek.

Indien sprake is van ernstige datalekken worden deze conform de in de relevante wet- en regelgeving opgenomen specifieke bepalingen over datalekken afgehandeld.

7.3 Evaluatie

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage over incidenten maakt daarom een vast onderdeel uit van de jaarrapportages van het College van Bestuur aan de Raad van Toezicht en van de FG aan het College van Bestuur.

7.4 Bijzondere omstandigheden

Indien een incident niet via de standaardprocedure als bedoeld onder 7.2 kan worden opgelost en er sprake is van een zo spoedeisend belang waarbij (enig) uitstel niet mogelijk is, is CERT-UvA bevoegd tijdelijk de maatregelen te nemen waar de situatie op dat moment om vraagt. Dit kan onder meer betekenen dat een UvA-netID-account van een betrokkene wordt geblokkeerd en/of een verbinding met een derde wordt verbroken of geblokkeerd. Van een situatie als bedoeld in de eerste volzin kan sprake zijn als het incident plaats vindt buiten de reguliere openingstijden van de UvA in een periode waarin de reguliere bedrijfsprocessen verstoord zijn of omdat de aard van het incident vraagt om noodmaatregelen. CERT-UvA informeert het College van Bestuur en de FG over de genomen maatregelen en legt daarover verantwoording af aan de leidinggevende. Voor de uitoefening van de in deze alinea beschreven bevoegdheid wordt door het College van Bestuur aan CERT-UvA een bijzonder mandaat verstrekt.

8. Rechten van betrokkenen

8.1 Informatieplicht

De UvA informeert haar studenten, medewerkers en andere betrokkenen over de gegevens-verwerkingen die zij uitvoert, de doeleinden van deze verwerkingen en de informatie betreffende beveiliging van de verwerking.

Het uitgangspunt geldt dat de betrokkene over een gegevensverwerking wordt geïnformeerd op het moment dat de UvA persoonsgegevens van een betrokkene verzamelt of ontvangt. Dit geldt niet wanneer de UvA ervan uit kan gaan dat de betrokkene op de hoogte is van de gegevensverwerking of wanneer de verkrijging van de persoonsgegevens bij wet is voorgeschreven en in die wet de gerechtvaardigde belangen van de betrokkene zijn gewaarborgd.

Betrokkenen worden actief geïnformeerd via de privacy- en cookiestatement en door middel van informatie op intranet (o.a. in de zogenoemde ‘A-Z lijst’ onder ‘AVG’ en ‘Privacy’). Daarnaast is het voor betrokkenen mogelijk om op verzoek informatie te ontvangen over de verwerkingen die worden uitgevoerd door de UvA (verzoeken kunnen worden ingediend bij de FG: fg@uva.nl).

8.2 Recht op inzage

Iedere betrokkene heeft recht op inzage in zijn of haar persoonsgegevens die door of namens de UvA zijn verzameld en, wanneer dat het geval is, inzage in de verwerkingsdoelen, categorieën van

persoonsgegevens, de categorieën van ontvangers, de (verwachte) bewaartermijn, beschikbare informatie over de herkomst van de gegevens en informatie over de rechten die toekomen aan de betrokkenen. Het inzagerecht strekt zich niet uit tot bedrijfsgevoelige informatie, werkdocumenten of interne notities. Deze persoonsgegevens zullen niet worden overhandigd of onleesbaar worden gemaakt.

Verzoek
Op de website van de UvA wordt een actueel overzicht van systemen bij gehouden die de UvA gebruikt voor het verwerken van persoonsgegevens. Studenten kunnen het recht op inzage voor een belangrijk deel direct zelf uitoefen via Studielink en via het Studenten Informatie Systeem (SIS). Medewerkers kunnen het recht op inzage voor een belangrijk deel zelf uitoefenen door hun personeelsdossier te raadplegen. Het personeelsdossier is toegankelijk via Zelfbediening, onder het tabblad 'Mijn gegevens'.

Voor overige vragen of voor andere betrokkenen is het nog altijd mogelijk om een schriftelijk verzoek in te dienen bij Juridische Zaken (avg@uva.nl). Een verzoek om inzage van minderjarigen dient door de wettelijk vertegenwoordiger te geschieden. Vóórdat aan het verzoek tot inzage gehoor wordt gegeven, dient de betrokkene of de wettelijke vertegenwoordiger zichzelf te identificeren.

Termijn
De betrokkene wordt zo spoedig mogelijk, uiterlijk binnen vier weken, voorzien van een antwoord. Complexe verzoeken worden met maximaal twee maanden verlengd. Over een eventuele verlenging wordt de betrokkene binnen vier weken geïnformeerd.

Kosten
Het verstrekken van de informatie in verband met het verzoek op inzage gebeurt kosteloos. Slechts voor aanvullende kopieën op verzoek van betrokkene wordt de kostprijs gerekend.

8.3 Recht op rectificatie, beperken, verwijderen of vergetelheid

Iedere betrokkene kan met betrekking tot de over hem/haar opgenomen persoonsgegevens bij de UvA van deze gegevens verzoeken die te rectificeren, beperken, verwijderen of te vergeten.

8.3.1. Recht op rectificatie
Het rectificeren betreft het aanpassen of aanvullen van gegevens die niet (meer) kloppen, incompleet zijn of niet ter zake dienend. De UvA streeft naar een juiste (verwerking van) persoonsgegevens. De UvA rectificeert persoonsgegevens dan ook graag -mits conform wet- en regelgeving- op verzoek maar ook op eigen initiatief.

8.3.2. Recht op beperking
Het recht op beperking houdt in dat de verwerking van persoonsgegevens, met uitzondering van opslag ervan, tijdelijk wordt stil gezet. Dit recht kan bijvoorbeeld worden ingeroepen, wanneer betrokkene de juistheid van de gegevens betwist die de UvA over hem of haar verwerkt. Bij een 'verzoek tot beperking' maakt de UvA de beperkte gegevens voor gebruikers tijdelijk niet beschikbaar. De UvA verwijdert de persoonsgegevens niet. Het moet immers mogelijk blijven om de door betrokkene verzochte beperking op enig moment weer ongedaan te maken.

Afwijzing
Wanneer de UvA de persoonsgegevens vanwege gewichtige redenen nodig heeft, mag en zal de UvA de persoonsgegevens voor dit doel blijven verwerken en wordt het verzoek op beperking afgewezen. Hiervan zal betrokkene gemotiveerd op de hoogte worden gesteld.

8.3.3. Recht op verwijderen en het recht om vergeten te worden

Onder bepaalde omstandigheden hebben betrokkenen het recht om hun gegevens door de verwerkingsverantwoordelijke te laten *verwijderen*, bijvoorbeeld omdat de verwerking niet meer strekt tot het doel waarvoor de gegevens zijn verzameld. Het *recht om vergeten* te worden ligt in het verlengde van het recht op verwijdering. Dit houdt in dat na het verwijderen van de gegevens, daar bovenop – iedere koppeling naar de persoonsgegevens verwijderd.

Afwijzing

Ook het verzoek om persoonsgegevens te verwijderen en het verzoek om vergeten te worden kan worden afgewezen. Denk hierbij aan een wettelijke verwerkingsverplichting, een taak van algemeen belang of archivering (zie meer over archivering in paragraaf 3.4)

Verzoek

Een verzoek tot rectificatie, beperking, verwijdering of vergetelheid kan schriftelijk worden ingediend bij Juridische Zaken (avg@uva.nl). Een verzoek van een minderjarige dient door de wettelijk vertegenwoordiger te geschieden. Vóórdat aan het verzoek een verzoek gehoor wordt gegeven, dient de betrokkene of de wettelijke vertegenwoordig zichzelf te identificeren.

Termijn

De betrokkene wordt zo spoedig mogelijk, uiterlijk binnen vier weken, voorzien van een antwoord. Complexe verzoeken worden met maximaal twee maanden verlengd. Over een eventuele verlenging wordt de betrokkene binnen vier weken geïnformeerd.

Kennisgeving

Derden aan wie de gegevens, voorafgaand aan de rectificatie, beperking, verwijdering of vergetelheid, zijn verstrekt worden hiervan in kennis gesteld. De verzoeker mag opgave verzoeken van degene aan wie UvA deze mededeling heeft gedaan.

8.4 Recht van bezwaar

Voor de grondslagen ‘taak van algemeen belang’ (artikel 6 lid 1 punt e AVG) en ‘gerechtvaardigd eigen belang’ (punt f) voert de UvA een algemene en abstracte belangenafweging uit, ten aanzien van de privacy van betrokkenen. Een betrokkene kan echter in specifieke situatie anders tegen deze afwegingen aankijken. Het recht van bezwaar geeft de betrokkene de mogelijkheid om van de UvA te verlangen dat de belangen die ten grondslag liggen aan een verwerking, opnieuw af te wegen.

Verzoek

Een verzoek hiertoe kan schriftelijk worden ingediend bij Juridische Zaken (avg@uva.nl). Een verzoek van een minderjarige dient door de wettelijk vertegenwoordiger te geschieden. Vóórdat aan een verzoek gehoor wordt gegeven, dient de betrokkene of de wettelijke vertegenwoordig zichzelf te identificeren.

Termijn

De betrokkene wordt zo spoedig mogelijk, uiterlijk binnen vier weken, voorzien van een antwoord. Complexe verzoeken worden met maximaal twee maanden verlengd. Over een eventuele verlenging wordt de betrokkene binnen vier weken geïnformeerd.

Toestemming

Wanneer een verwerking is gebaseerd op de grondslag toestemming (artikel 6 lid 1 punt a) is het niet mogelijk om bezwaar te maken. In dat geval kan de betrokkene wel zijn toestemming intrekken (artikel 7 lid 3).

8.5 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Op verzoek kan iedere betrokkene een kopie ontvangen van de persoonsgegevens die hij of zij zelf aan de UvA heeft verstrekt en welke geautomatiseerd van hem of haar door de UvA worden verwerkt.

Afwijzing

Het recht op dataportabiliteit kan alleen worden uitgeoefend wanneer de persoonsgegevens krachtens toestemming of krachtens de uitvoering van een overeenkomst worden verwerkt en betreffen alleen die gegevens die rechtstreeks door betrokkene aan de UvA zijn verstrekt. Het recht op data-portabiliteit geldt dus niet voor het geval dat de UvA persoonsgegevens verwerkt krachtens een gerechtvaardigd belang. Betrokkene kan in dat geval wel een verzoek tot inzage doen (paragraaf 8.2).

Verzoek

Medewerkers kunnen voor een verzoek tot dataportabiliteit hun personeelsdossier raad plegen, via Zelfbediening, onder het tabblad 'Mijn gegevens'. Studenten kunnen deze gegevens opvragen via Studielink. Voor overige vragen of voor andere betrokkenen is het nog altijd mogelijk om een schriftelijk verzoek in te dienen bij Juridische Zaken (avg@uva.nl).
Een verzoek van minderjarigen dient door de wettelijk vertegenwoordiger te geschieden. Vóórdat aan het verzoek gehoor wordt gegeven, dient de betrokkene of de wettelijke vertegenwoordig zichzelf te identificeren.

Termijn

De betrokkene wordt zo spoedig mogelijk, uiterlijk binnen vier weken, voorzien van een antwoord. Complexe verzoeken worden met maximaal twee maanden verlengd. Over een eventuele verlenging wordt de betrokkene binnen vier weken geïnformeerd.

9. Tot slot

Dit Beleid is vastgesteld door het College van Bestuur op 17 december 2018, na instemming van de Centrale Ondernemingsraad (COR) en de Centrale Studentenraad (CSR).
Het College van Bestuur stelt nadere uitwerking van dit Beleid vast in separate documenten en regelingen, met inachtneming van de rechten van de Centrale Ondernemingsraad (COR) en de Centrale Studentenraad (CSR). Een overzicht van op dit moment geplande uitwerkingen is als bijlage bij dit Beleid gevoegd.

Voor vragen of opmerkingen over dit Beleid kan men terecht bij de Functionaris voor Gegevensbescherming (mail: fg@uva.nl).

I Overzicht documenten en regelingen die voortvloeien uit Privacybeleid

- Reglement Cameratoezicht
- Privacystatement (betreft vervanging van huidige tekst n.a.v. AVG)
- Cookiestatement (betreft vervanging van huidige tekst n.a.v. AVG)
- Model verwerkersovereenkomst en checklist
- Informatiebeveiligingsbeleid

II Aan het informatiebeveiligingsbeleid gerelateerde documenten

Het Informatiebeveiligingsbeleid schetst het kader en de uitgangspunten van het beleid. De nadere uitwerking van dit beleid vindt plaats in separate documenten. Hieronder een overzicht van de documenten op het gebied van informatiebeveiliging. Alle beleidsdocumenten worden na vaststelling gepubliceerd op de website van de UvA.

1) Security principes.

Het hoogste niveau van idealen en waarden die de organisatie leiden in haar gedrag. Voorbeelden zijn:

- Openheid - Security oplossingen zijn gebouwd op open protocollen en systemen, zijn onderhoudbaar, worden ondersteund door een breed aantal platformen, ondersteunen een breed aantal grote industrie standaarden. Geen security by obscurity.
- Security by Design - Security moet worden ontworpen als een integraal onderdeel van de systeem architectuur

De security principes worden vastgesteld door het CvB en wordt ter instemming aangeboden aan de COR/CSR.

2) Security organisatie.

Dit document beschrijft de taken, verantwoordelijkheden en bevoegdheden van de verschillende rollen in de security organisatie en de organisatorische positionering. Tevens wordt de functionele en hiërarchische relatie van de rollen beschreven. Voor de rol van Security Officer bij faculteiten en diensten wordt een advies geformuleerd voor het type functie(s) dat deze rol kan invullen. De security organisatie worden vastgesteld door het CvB en wordt ter instemming aangeboden aan de COR/CSR.

3) Acceptable Use Policy voor medewerkers van de Universiteit van Amsterdam.

Met deze gedragslijn stelt de UvA regels omtrent het gewenst gebruik van haar ICT-faciliteiten door medewerkers. Het streven daarbij is een goede balans aan te brengen tussen het inzetten van ICT-faciliteiten ten behoeve van onderwijs, onderzoek en bedrijfsvoering aan de ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de medewerker aan de andere kant. De Acceptable Use Policy wordt vastgesteld door het CvB en wordt instemming aangeboden aan de COR.

4) Acceptable Use Policy voor studenten van de Universiteit van Amsterdam.

Met deze gedragslijn stelt de UvA regels omtrent het gewenst gebruik van haar ICT-faciliteiten door studenten. Het streven daarbij is een goede balans aan te brengen tussen het inzetten van ICT-faciliteiten ten behoeve van onderwijs, onderzoek en bedrijfsvoering aan de ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de student aan de andere kant. De Acceptable Use Policy wordt vastgesteld door het CvB en wordt ter instemming aangeboden aan de CSR.

5) Classificatierichtlijn Informatie en Informatiesystemen UvA.
Dit document beschrijft de classificatiemethodiek die wordt toegepast om informatiesystemen te classificeren op de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid. Op basis van deze classificatie kan het niveau van beveiligingsmaatregelen worden bepaald. De richtlijn wordt samen met de HvA opgesteld. De classificatierichtlijn wordt vastgesteld door het CvB en wordt ter informatie aangeboden aan de COR en CSR.

6) Autorisatiebeleid.
Het Autorisatiebeleid geeft algemene richtlijnen hoe bij informatiesystemen om te gaan met autorisaties. Het toekennen van rechten wie wat mag, noemen we autorisatie. De UvA gebruikt informatiesystemen om relevante gegevens te raadplegen en vast te leggen. Bij alle systemen is de integriteit van belang, we willen immers niet dat iedereen zomaar gegevens kan veranderen. Bij veel systemen speelt de vertrouwelijkheid een rol, niet iedereen mag zomaar persoonsgegevens of anderszins vertrouwelijke informatie raadplegen. Voor het naleven van de AVG is het noodzakelijk dat het autorisatiebeleid van de systemen welke de gegevens over personen bevatten goed is geregeld. Het autorisatiebeleid wordt vastgesteld door het CvB en wordt ter instemming aangeboden aan de COR en CSR.

7) UvA-leidraad voor Responsible Disclosure.
Responsible disclosure binnen de ICT-wereld is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure. De leidraad beschrijft verantwoordelijkheden van de organisatie en de melder en de bouwstenen voor responsible disclosure bij de UvA. De leidraad wordt opgesteld gebruik makend van voorbeelden zoals die van het Ministerie van Veiligheid en Justitie. De UvA-leidraad voor Responsible Disclose wordt vastgesteld door het CvB en wordt ter informatie aangeboden aan de COR en CSR.

8) Wachtwoordregeling.
Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging van de instelling. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie die onder beheer van de instelling valt (instellingsinformatie). Wachtwoorden beschermen de gebruiker tegen misbruik van zijn account en tegen onbedoelde verspreiding van zijn persoonlijke gegevens. Het doel van deze wachtwoordregeling is tweeledig:
- het vaststellen van regels waar wachtwoorden en wachtwoord procedures aan moeten voldoen;
- het vaststellen van de bescherming van de wachtwoorden.

De wachtwoordregeling is vastgesteld door het CvB en wordt ter informatie aangeboden aan de COR en CSR.

9) Inrichting-CERT-UvA.
Het document Inrichting CERT-UvA beschrijft het doel, taken, verantwoordelijkheden en bevoegdheden, organisatie en middelen van CERT-UvA . De Inrichting CERT-UvA is vastgesteld door het CvB.

10) Hulpmiddelen voor verantwoorde gegevensopslag.
Er wordt een handreiking opgesteld waarmee medewerkers, aan de hand van de aard van de gegevens, kunnen bepalen op welke plaats de gegevens het beste kunnen worden opgeslagen. De handreiking wordt opgesteld door ICTS en wordt ter informatie aangeboden aan de COR.