UNIVERSITEIT VAN AMSTERDAM

College van Bestuur

Spui 21
1012 WX Amsterdam
Postbus 19268
1000 GG Amsterdam
www.uva.nl

Aan de voorzitter van de CSR
Nieuwe Achtergracht 170
1018 WV AMSTERDAM

Datum	Telefoon	Uw kenmerk
21 oktober 2016	020 525 2369	-
Contactpersoon	**Bijlage**	**Ons kenmerk**
dr. B.E.M. Widdershoven	1	2016cu1780

E-mail
B.E.M.Widdershoven@uva.nl

Onderwerp
Instemmingsverzoek privacybeleid en verwerking persoonsgegevens

Geachte voorzitter,

./. Bijgaand ontvangt u ter instemming de notitie inzake privacybeleid en verwerking persoonsgegevens. Het College van Bestuur hecht eraan dat persoonsgegevens niet alleen op juiste wijze en gronden worden verzameld, maar ook dat zij – vervolgens – op juiste wijze worden bewaard en beschermd. Voorkomen moet worden dat onbevoegden de beschikking krijgen over de persoonsgegevens.

Het College van Bestuur is graag bereid dit onderwerp met u bespreken. Ik hoop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
het College van Bestuur,

prof. dr. Geert T.M. ten Dam,
voorzitter

PRIVACYBELEID EN BELEID VERWERKING PERSOONSGEGEVENS

UNIVERSITEIT VAN AMSTERDAM

Oktober 2016

Inhoud

1. Inleiding

Het verwerken[1] van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van de Universiteit van Amsterdam (UvA) en de met haar verbonden rechtspersonen. 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[2]. 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 de bescherming van persoonsgegevens valt onder deze verantwoordelijkheid.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt UvA haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren 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.

Betrokkene: een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

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

Bewerker: een door de UvA ingeschakelde (derde) partij die ten behoeve van de UvA persoonsgegevens verwerkt.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

Verwerking: elk handeling of geheel van handelingen met betrekking tot persoonsgegevens.

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

---

[1] In de Wet bescherming persoonsgegevens (Wbp) wordt onder '**verwerking**': elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

[2] De verantwoordelijke in de zin van de Wbp is degene die formeel-juridisch de zeggenschap over de verwerking heeft. Het gaat om degene die bevoegd is doel en middelen 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 uitoefenen. Bij de UvA is het College van Bestuur de verantwoordelijke. Dit vloeit voort uit de Algemene wet bestuursrecht (Awb) en artikel 9.2 en 9.5 van de WHW.

Datalek: persoonsgegevens die in handen vallen van derden die geen toegang tot die gegevens (mogen) hebben.

Privacy by design: het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan alle omvattende waarborgen met betrekking tot nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van persoonsgegevens.

Privacy impact Assessment/ Privacyeffectbeoordeling: een tool dat helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

Minderjarige: een persoon die de leeftijd van 18 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, gasten, 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 die in een bestand zijn opgenomen. Eveneens is het beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij 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 persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en 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 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 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 vastgesteld 'best pratice' of norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.

- **Het stellen van normen**: de basis voor de beveiliging van persoonsgegevens is ISO 27001[3]. Maatregelen worden op basis van 'best practices' in het hoger onderwijs en op basis van ISO 27002[4] genomen.

- **Het Juridisch Normenkader Cloudservices Hoger Onderwijs**[5] wordt gehanteerd als 'best practice' voor Cloud services en andere outsource contracten.

- **Het nemen van de verantwoordelijkheid**: door het College van Bestuur door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor de UvA.

- **Compliant zijn/worden** 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 UvA geheel of gedeeltelijk is verbonden zijn zelf verantwoordelijk voor het beleid met betrekking tot de verwerking van persoonsgegevens. Dit betekent dat dit beleid niet onverkort op hen van toepassing is. De functionaris voor de gegevensbescherming (FG) houdt geen toezicht op de naleving van de privacywetgeving door voornoemde rechtspersonen en vennootschappen. De leiding van voornoemde rechtspersonen en vennootschappen kan er voor kiezen dit beleid geheel of gedeeltelijk over te nemen en zelf een FG te benoemen. In overleg met het College van Bestuur kan van het voorgaande worden afgeweken.

Het College van Bestuur behoudt zich het recht voor de leiding van de verbonden partijen adviezen en/of richtlijnen te geven indien het door een verbonden partij gevoerde beleid op het terrein van de bescherming van persoonsgegevens sterk afwijkt van dit beleid en schadelijk is voor de UvA.

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 eigen keuzes te maken met betrekking tot zijn/haar persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

---

[3] Voluit: NEN-ISO/IEC 27001: Eisen aan managementsystemen voor informatiebeveiliging.

[4] Voluit: NEN-ISO/IEC 27002: Code voor informatiebeveiliging.

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

- Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 8 van de wet bescherming persoonsgegevens (Wbp).
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- 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.
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- 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.
- 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.
- Iedere betrokkene heeft recht op inzage, respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem/haar betreffende persoonsgegevens, en heeft het recht van verzet zoals geformuleerd in hoofdstuk 8 van dit beleid.
- Bij alle registraties op vrijwillige basis zal aan betrokkene een eenduidige zogenaamde opt-out procedure worden aangeboden.

3. Wet- en regelgeving

Bij de UvA wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

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

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 (niet)wetenschappelijk onderzoek nageleefd en toegepast.

3.2 Wet bescherming persoonsgegevens (Wbp)

De UvA heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van persoonsgegevens en nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens) geïmplementeerd door middel van het beleid.

3.3 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.

4. Rollen en verantwoordelijkheden met betrekking tot verwerking van persoonsgegevens

Om verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken wordt bij de UvA een aantal rollen onderkend die aan functionarissen in de organisatie zijn toegewezen.

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 het beleid, de maatregelen en de procedures op het gebied van verwerking vast.

4.2 Portefeuillehouder beveiliging persoonsgegevens

De portefeuillehouder beveiliging persoonsgegevens is het bestuurslid dat privacy in portefeuille heeft. Hij/zij is eerstverantwoordelijke voor de beveiliging van persoonsgegevens binnen de UvA.

4.3 Functionaris gegevensbescherming (FG)

De FG houdt binnen de UvA toezicht op de toepassing en naleving van de Wbp. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij de UvA.

4.4 Systeemeigenaar

De systeemeigenaar[6] is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het beleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu, als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.

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;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

[6] Wie als 'systeemeigenaar' moet worden aangemerkt, is afhankelijk van de concrete omstandigheden van het geval. In veel gevallen zal dit een ICT-medewerker in een faculteit zijn maar voorstelbaar is ook dat dit de coördinator van een bepaald project is of een functionaris is die op centraal niveau opereert.

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 Wbp. 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 gouvernance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de UvA, zoals medewerkers, studenten, subsidieverstrekkers en partners, alsmede de samenleving als geheel. Een goed corporate gouvernance-beleid heeft aandacht voor de rechten van alle betrokkenen[7].

5.1 Verdeling van de verantwoordelijkheden

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 de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen.

Het zorgvuldig omgaan met persoonsgegevens is ieders verantwoordelijkheid. Er wordt van medewerkers en studenten verwacht dat zij zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies voor de UvA of van individuen. Het is om deze reden dat er gedragscodes kunnen zijn geformuleerd.

5.2 Inpassing in de instellingsgouvernance/ afstemming met aanpalende beleidsterreinen

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

Op **strategisch niveau** wordt richtinggevend gesproken over gouvernance 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.

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

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.

[7] Dit is een algemeen aanvaarde opvatting die onder meer tot uiting komt in artikel 2.1.2 van de Code goed bestuur universiteiten 2013.

5.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van verwerking van persoonsgegevens 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 Security Managers en de Security Officer.

5.4 Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de Information Security Officer en de interne auditor de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventueel externe controles worden uitgevoerd door onafhankelijke en erkende deskundigen op het terrein van gegevensbescherming en –beveiliging. Dit wordt zo veel mogelijk gecoördineerd met de normale Planning en Control cyclus en wordt – indien nodig -gekoppeld aan het jaarlijkse accountantsonderzoek. Peer-reviews kunnen onderdeel uitmaken van de externe controles.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekort schieten, dan kan de UvA de betrokken medewerker of student een sanctie opleggen, binnen de kaders van de cao en de wettelijke mogelijkheden.

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

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 8 Wbp. 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.

Bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren[8].

De UvA hanteert bij de implementatie het principe 'privacy by design'.

6.2 Melden en documenteren van verwerkingen

De FG beoordeelt de rechtmatigheid van de registratie en draagt zorg voor adequate documentatie. Verwerkingen die onder het bereik van het vrijstellingsbesluit Wbp vallen, worden eveneens door of namens de FG geregistreerd en gedocumenteerd.

Verwerkingen worden voldoende gedocumenteerd en geregistreerd. Deze registratie kan door een ieder kosteloos worden geraadpleegd.

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. Een ieder 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[9] buiten het bereik van de actieve administratie gebracht te worden. De UvA zal de persoonsgegevens na het verstrijken van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren.

---

[8] 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.

[9] Bewaartermijnen kunnen wettelijk zijn bepaald maar kunnen ook – voor zover dit wettelijk is toegestaan – door de UvA worden bepaald.

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.

6.7 Doorgifte persoonsgegevens aan derden

6.7.1 Uitbesteden van verwerking aan een bewerker

Indien UvA persoonsgegevens laat verwerken door een bewerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen de verantwoordelijke en de bewerker.

6.7.2 Uitgifte persoonsgegevens binnen de Europese Unie

UvA verstrekt persoonsgegevens alleen aan derden als doorgifte 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[10]. Daarbij hanteert UvA als uitgangspunt de lijst met landen met passend beschermingsniveau van de Europese Commissie[11].

UvA verstrekt persoonsgegevens alleen aan landen zonder een passend beschermingsniveau, waar zij een vergunning van de minister van Veiligheid en Justitie voor heeft verkregen, dan wel op basis van een modelcontract opgesteld door de Europese Commissie en met instemming van de Autoriteit Persoonsgegevens[12].

6.7.4 Lijst van derden aan wie UvA persoonsgegevens doorgeeft:

UvA verstrekt, met in achtneming van wet- en regelgeving, persoonsgegevens aan de derden op grond van wettelijke verplichtingen en voor zover dit verband houdt met haar onderwijs en onderzoek en haar overige activiteiten die hieruit voortvloeien, zoals aan:

DUO

Overheidsinstellingen

---

[10] Artikel 76 Wbp.

[11] Deze lijst is te vinden via de volgende link http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[12] Artikel 77 Wbp.

Belastingdienst

Controlerend accountant

Instellingen voor hoger onderwijs, ingeval van gemeenschappelijk onderwijs en/of onderzoek

Met UvA verbonden rechtspersonen in het kader van haar onderwijs, onderzoek en/of overige activiteiten die daarmee samenhangen of hieruit voortvloeien

Stagebedrijven/organisaties

Studenten woning coöperaties

7. Incidenten met betrekking tot persoonsgegevens

Iedere melding van over (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

Incidenten kunnen gemeld worden bij het CERT-UvA[13][14]. Een beveiligingsincident[15] kan tijdens kantooruren worden gemeld bij de ICTS Servicedesk via servicedesk-icts@uva.nl of telefonisch op 020-5252200. Buiten kantooruren of bij ernstige beveiligingsincidenten kan dit rechtstreeks bij CERT-UvA via cert@uva.nl of telefonisch op 020-5253322. Van elk incident en de afhandeling daarvan zal een registratie bijgehouden worden. Een incident kan gemeld worden door een betrokkene, een bewerker of een derde.

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 goede naam 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[16].

---

[13] CERT staat voor Computer Emergening ResponseTeam.

[14] CERT-UvA is gevestigd in Gebouw Leeuwenburg, Weesperzijde 190, 1097 DZ Amsterdam.

[15] Voorbeelden van een beveiligingsincident zijn een gehackte computer of e-mailbox, het verliezen van vertrouwelijke informatie op de laptop, telefoon of USB-stick, een phishing e-mail of een virusuitbraak (ransomware).

[16] Beleidsregels voor toepassing van artikel 34a van de Wbp. Staatscourant Nr. 46128, 16 december 2015.

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 maken 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 id-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

Algemene mededeling

UvA beoogt de verwerking van persoonsgegevens van studenten, medewerkers en andere betrokkenen door middel van een algemene bekendmaking van haar beleid verwerking persoonsgegevens mede te delen. Daarnaast beoogt UvA in overeenstemming met de wet, alle betrokkenen onder bepaalde omstandigheden rechten te verschaffen waarmee zij de aan hen toebehorende persoonsgegevens naar behoren kunnen beschermen.

UvA verstrekt de betrokkene tenminste het volgende:

De identiteit en de contactgegevens van de voor de verwerking verantwoordelijke functionaris en de FG.

De specifieke doeleinden van verwerking waarvoor de persoonsgegevens zijn bestemd alsook informatie betreffende beveiliging van de verwerking.

Mededeling van aanpassingen

Als het beleid in de loop der tijd ingrijpend wordt aangepast dan wel veranderd, deelt UvA dit mee om zorgvuldige en behoorlijke verwerking te waarborgen.

8.2 Recht op inzage

Verzoek tot inzage

Iedere betrokkene heeft recht op inzage in hem/haar betreffende persoonsgegevens. Een verzoek hiertoe kan schriftelijk worden ingediend bij het College van Bestuur. Deze leidt het verzoek door naar de afdeling Juridische Zaken die met de feitelijke afhandeling van het verzoek is belast.

Een verzoek om inzage van minderjarigen geschiedt door de wettelijk vertegenwoordiger. Verzoeken om inzage door ouders of voogden van meerderjarige studenten worden geweigerd. Verzoeken om inzage worden eveneens geweigerd indien zij afkomstig zijn van werkgevers.

Herhaalde en zeer frequentie verzoeken om inzage kunnen worden geweigerd[17].

Termijn

Op het verzoek wordt zo spoedig mogelijk, doch uiterlijk binnen vier weken na indiening schriftelijk gereageerd. De UvA draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker[18].

Mededeling

Indien gegevens worden verwerkt, bevat de mededeling van de UvA een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de categorieën van ontvangers, alsmede beschikbare informatie over herkomst van de gegevens en de termijn van bewaring van gegevens[19].

Kosten

De aanvraag kan kosteloos worden ingediend[20].

8.3 Recht op verbetering, aanvulling, verwijdering of afscherming

Verzoek tot verbetering, aanvulling, verwijdering of afscherming

Iedere betrokkene kan met betrekking tot de over hem/haar opgenomen persoonsgegevens bij de UvA van deze gegevens verzoeken die te wijzigen, te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek bevat de aan te brengen wijzigingen[21].

Verzoeken tot verbetering, aanvulling verwijdering of afscherming moeten schriftelijk worden ingediend bij het College van Bestuur. Deze leidt het verzoek door naar de afdeling of de functionaris die met de beoordeling van het verzoek is belast en daarover advies uitbrengt[22].

---

[17] Artikel 35 Wbp.

[18] Artikel 37 Wbp.

[19] Artikel 35 Wbp.

[20] Artikel 39 Wbp.

[21] Het verzoek moet concreet zijn. Duidelijk moet (gemotiveerd) worden aangegeven om welk gegeven of informatie het gaat en waarom om wijziging, aanvulling etc. wordt verzocht.

Termijn

UvA deelt binnen vier weken na ontvangst van het verzoek schriftelijk aan betrokkene mede of aan zijn/haar verzoek wordt voldaan in een voor bezwaar en beroep vatbaar besluit[23].

Kennisgeving

Indien opgenomen persoonsgegevens van de betrokkene feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd zijn met een wettelijk voorschrift zijn verwerkt[24], wordt dit verbeterd[25].

Bovendien worden ook derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld. De verzoeker mag opgave verzoeken van degene aan wie UvA deze mededeling heeft gedaan.

Termijn voor uitvoering

UvA zorgt er voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

8.4 Recht van verzet

Gronden voor verzet[26]

In verband met zijn of haar persoonlijke omstandigheden, mag iedere betrokkene verzet aantekenen tegen verwerking van persoonsgegevens bij UvA, als deze verwerking plaatsvond in het kader van de vervulling van een publiekrechtelijke taak van de UvA als bedoeld in artikel 8 letter e en f Wbp. Daarbij wordt slechts rekening gehouden met omstandigheden die UvA kent. Er is derhalve sprake van een gerechtvaardigde verwerking. Het is echter mogelijk dat er bijzondere persoonlijke omstandigheden zijn die maken dat in het kader van de belangenafweging er een ander besluit moet worden genomen. Het recht van verzet ziet op die (uitzonderlijke) situatie.

Is het verzet gerechtvaardigd, dan geeft dit geen recht op schadevergoeding als bedoeld in artikel 49 Wbp omdat de oorspronkelijke verwerking – gelet op de kennis die UvA toen had – gerechtvaardigd was.

---

[22] Afhankelijk van de aard van het verzoek kan niet op voorhand worden aangegeven wie met de beoordeling van het verzoek is belast. Zo zal een verzoek om wijziging in het studentedossier veelal door een opleiding worden beoordeeld terwijl een verzoek om wijziging in een personeelsdossier veelal verloopt via het administratief centrum of de decentrale personeelsfunctionaris. De afdeling of de functionaris die het verzoek beoordeelt, is niet bevoegd dit zelfstandig af te doen. Volstaan wordt met het uitbrengen van advies. Het verzoek wordt afgedaan door of namens het College van Bestuur in een voor bezwaar en beroep vatbaar besluit. Van het voorgaande wordt afgeweken indien het gaat om kleine of evidente fouten. In die gevallen wordt geen advies uitgebracht maar wordt de fout hersteld door de betreffende afdeling of functionaris.

[23] Artikel 45 Wbp.

[24] Artikel 36 Wbp.

[25] Zie ook voetnoot 18.

[26] Artikel 40 Wbp.

Termijn

UvA deelt binnen vier weken na ontvangst van het verzoek schriftelijk aan betrokkene mede of het verzet gerechtvaardigd is in een voor bezwaar en beroep vatbaar besluit[27].

8.5 Rechtsbescherming

Indien de betrokkene van mening is dat de wettelijke bepalingen inzake privacybescherming jegens hem/haar niet correct worden gehandhaafd, kan hij/zij verzoeken de gegevens aan te passen. Dit verzoek moet schriftelijk worden ingediend bij het College van Bestuur. Met betrekking tot de beoordeling van het verzoek wordt hierover door het College van Bestuur advies ingewonnen bij de FG. Vervolgens wordt de beoordeling van het verzoek vervat in een voor bezwaar en beroep vatbaar besluit in de zin van de Algemene wet bestuursrecht[28].

Termijn indienen bezwaar

Indien betrokkene het niet eens is met de beoordeling van zijn/haar verzoek, kan hij/zij uiterlijk binnen zes weken na dat besluit schriftelijk bezwaar maken bij het College van Bestuur.

9. Tot slot

Dit beleid is vastgesteld door het College van Bestuur op....., na een positief advies van de gezamenlijke vergadering van de centrale ondernemingsraad (COR) en de centrale studentenraad (CSR). Het beleid vervangt eerder vastgesteld beleid met betrekking tot de bescherming van de verwerking van persoonsgegevens en treedt in werking de dag na de vaststelling.

Voor vragen of opmerkingen over dit beleid kan men terecht bij de functionaris voor de gegevensbescherming.

[27] Artikel 45 Wbp.

[28] Artikel 45 Wbp.