



---

Beleidsdocument verwerking  
persoonsgegevens  
Wageningen University & Research

---

Beleidsdocument verwerking  
persoonsgegevens

Wageningen University & Research



---

# Inhoud

<b>1</b>	<b>Inleiding</b>	<b>5</b>
	1.1 Definities	5
	1.2 Reikwijdte en doelstelling van het Beleid	6
<b>2</b>	<b>Beleidsprincipes Verwerking Persoonsgegevens</b>	<b>8</b>
	2.1 Beleidsuitgangspunt en -principes	8
<b>3</b>	<b>Wet- en Regelgeving</b>	<b>9</b>
	3.1 Wet op het Hoger onderwijs en Wetenschappelijk onderzoek	9
	3.2 Algemene Verordening Gegevensbescherming	9
	3.3 Archiefwet	9
<b>4</b>	<b>Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens</b>	<b>10</b>
	4.1 College van Bestuur	10
	4.2 Portefeuillehouder beveiliging persoonsgegevens	10
	4.3 Functionaris gegevensbescherming	10
	4.4 Systeemeigenaar	10
	4.5 Leidinggevende	10
<b>5</b>	<b>Implementatie Beleid</b>	<b>11</b>
	5.1 Verdeling van de verantwoordelijkheden	11
	5.2 Inpassing in de instellingsgovernance / Afstemming met aanpalende beleidsterreinen	11
	5.3 Bewustwording en training	12
	5.4 Controle en naleving	12
<b>6</b>	<b>Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens</b>	<b>13</b>
	6.1 Grondslag, doelbinding en belangenafweging	13
	6.2 Melden en documenteren van Verwerkingen	13
	6.3 De organisatie van de beveiliging	13
	6.4 Geheimhouding	14
	6.5 Bewaartermijnen / vernietigingstermijnen per soort gegeven	14
	6.6 Bijzondere Persoonsgegevens	14
	6.7 Doorgifte Persoonsgegevens aan Derden	14
	6.7.1 Uitbesteden van Verwerking aan een Verwerker	14
	6.7.2 Doorgifte Persoonsgegevens binnen de Europese Unie (inclusief de EER)	14
	6.7.3 Doorgifte Persoonsgegevens buiten de Europese Unie	15
	6.7.4 Lijst van (niet limitatieve) Derden aan wie Wageningen University & Research Persoonsgegevens doorgeeft	15
<b>7</b>	<b>Incidenten met betrekking tot Persoonsgegevens</b>	<b>16</b>
	7.1 Melding en registratie	16
	7.2 Afhandeling	16
	7.3 Evaluatie	16
	7.4 Bijzondere omstandigheden	16

---

<b>8</b>	<b>Rechten van Betrokkenen</b>	<b>18</b>
	8.1 Informatieplicht	18
	8.2 Recht op inzage	18
	8.3 Recht op verbetering, aanvulling, verwijdering, afscherming of dataportabiliteit	19
	8.4 Recht van bezwaar/verzet	19
	8.5 Rechtsbescherming	20
<b>9</b>	<b>Tot slot</b>	<b>21</b>

---

# 1 Inleiding

Opslag en Verwerking van Persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van instellingen van onderwijs en onderzoek. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere Betrokkenen bij Wageningen University & Research<sup>1</sup>. Ook kan Wageningen University & Research als organisatie forse boetes opgelegd krijgen wanneer de verantwoordelijkheid hiervoor niet goed wordt uitgevoerd. Wageningen University & Research hecht als kennisinstelling veel waarde aan het beschermen van de Persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop deze Persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van Persoonsgegevens is de verantwoordelijkheid van het college van bestuur<sup>2</sup> van Wageningen University & Research. Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt Wageningen University & Research haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van Persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacy wet- en regelgeving.

Op 25 mei 2016 is de Europese algemene verordening gegevensbescherming (AVG)<sup>3</sup> in werking getreden. De AVG heeft rechtstreekse werking en hoeft dus niet eerst te worden omgezet in nationale regelgeving. De algehele toepasselijkheid van de verordening is bepaald op 25 mei 2018. Op deze wijze wordt in een overgangstermijn van 2 jaar voorzien om organisaties die met Persoonsgegevens werken de gelegenheid te geven zich op de nieuwe regelgeving voor te bereiden. Echter maatregelen die sneller kunnen worden ingevoerd om compliant te zijn aan de AVG dienen binnen de overgangstermijn te worden ingevoerd.

De AVG legt regels vast met betrekking tot de bescherming van natuurlijke personen op het gebied van persoonsgegevens en het vrij verkeer hiervan. De verordening ziet op het geheel of gedeeltelijk automatisch verwerken van persoonsgegevens en voorts op het verwerken op andere manieren dan geautomatiseerd, als deze persoonsgegevens deel uit maken van een bestand of hiervoor bedoeld zijn.

Op basis van de AVG (artikel 24) dient Wageningen University & Research het gegevensbeschermingsbeleid te hebben zoals in dit beleidsdocument is vastgelegd.

## 1.1 Definities

In de AVG (artikel 4) worden definities gegeven van veel gebruikte begrippen. Voor een volledig overzicht en een uitgebreidere definitie, raadpleeg de verordening. In dit beleidsplan is voor de leesbaarheid slechts een korte uitleg van de meest voorkomende begrippen opgenomen.

“Beleid”: onderhavig beleid met betrekking tot het verwerken van Persoonsgegevens aan Wageningen University & Research.

“Betrokkene”: een individueel en natuurlijk persoon op wie een Persoonsgegeven betrekking heeft.

“Verwerkingsverantwoordelijke”: college van bestuur van Wageningen University & Research die het doel van en middelen voor de Verwerking van Persoonsgegevens vaststelt.

---

<sup>1</sup> Wageningen University & Research is een samenwerkingsverband tussen de publiekrechtelijke rechtspersoon Wageningen University en de privaatrechtelijke stichting Wageningen Research

<sup>2</sup> Met het college van bestuur van Wageningen University & Research wordt bedoeld: college van bestuur van Wageningen University en/of het college van bestuur van stichting Wageningen Research

<sup>3</sup> <http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&qid=1468410766389&from=NL>

---

“Verwerker”: een door Wageningen University & Research ingeschakelde (derde) partij die ten behoeve van Wageningen University & Research Persoonsgegevens verwerkt.

“Persoonsgegevens”: elk gegeven/alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

“Verwerking van persoonsgegevens”: elke (geautomatiseerde) 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 andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

“Derde”: Ieder ander, niet zijnde de Betrokkene, de Verwerkingsverantwoordelijke of de Verwerker, of enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker en gemachtigd is om Persoonsgegevens te verwerken.

“Datalek/Inbreuk”: een inbreuk op de beveiliging met de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, tot gevolg.

“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 allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

“Privacy by default”: Aanvullend op privacy by design, alle bedrijfsprocessen worden aldus ingericht dat risico’s op schending van privacy zoveel mogelijk worden uitgesloten. Data-minimalisatie is voor de organisatie het uitgangspunt bij de omschrijving van de doeleinden en de inrichting van de bedrijfsprocessen. Persoonsgegevens worden niet breder gecommuniceerd dan strikt noodzakelijk is.

“Privacy Impact Assessment /gegevensbeschermingseffectbeoordeling (PIA)”: een tool die helpt bij het identificeren van privacy risico’s en de handvaten levert om deze risico’s te verkleinen tot een acceptabel niveau.

## 1.2 Reikwijdte en doelstelling van het Beleid

Het Beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen Wageningen University & Research, waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), alsmede op andere Betrokkenen waarvan Wageningen University & Research Persoonsgegevens verwerkt.

In het Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van het college van bestuur 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 Wageningen University & Research wordt het beschermen van Persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein Informatiebeveiliging<sup>4</sup>, 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.

---

<sup>4</sup> <https://www.wageningenur.nl/nl/Expertises-Dienstverlening/Faciliteiten/Informatiebeveiliging.htm>

---

Het Beleid bij Wageningen University & Research 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.

Er wordt naar gestreefd 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 dienen te zijn bij Wageningen University & Research.

Doelstelling van het Beleid voor Wageningen University & Research is concreet het volgende:

- Het bieden van een kader: het Beleid biedt een kader om (toekomstige) Verwerkingen van Persoonsgegevens te toetsen aan een vastgestelde 'best practice' of norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- Het stellen van normen: de basis voor de beveiliging van Persoonsgegevens is ISO 27001.<sup>5</sup> Maatregelen worden op basis van 'best practices' in het hoger onderwijs en o.b.v. ISO 27002 genomen.<sup>6</sup>
- Het Juridisch Normenkader Cloudservices Hoger Onderwijs<sup>7</sup> 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 gehele organisatie. 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 vermijding van risico's als gevolg van het nog niet volledig compliant zijn met de relevante wet- en regelgeving.

---

<sup>5</sup> Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging

<sup>6</sup> Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging

<sup>7</sup> SURF taskforce Cloud, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014, te vinden via: <https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html>



---

## 2 Beleidsprincipes Verwerking Persoonsgegevens

### 2.1 Beleidsuitgangspunt en -principes

Algemeen beleidsuitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van Wageningen University & Research om Persoonsgegevens te verwerken en het belang van Betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een Verwerking van Persoonsgegevens is toegestaan indien aan ten minste een van de in artikel 6 lid 1 van de AVG genoemde voorwaarden is voldaan.
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de Verwerking geformuleerd.
- Bij een Verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
- 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 ze zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke Verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van verzet, zoals geformuleerd in hoofdstuk 8 van dit Beleid.
- Bij alle registraties op vrijwillige basis zal aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

---

## 3 Wet- en Regelgeving

Bij Wageningen University & Research wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

### 3.1 Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

Wageningen University & Research heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden de gedrags- en integriteitscodes voor (niet-)wetenschappelijk personeel nageleefd en toegepast<sup>8</sup> en worden persoonsgegevens in onderzoeksdata beveiligd.

### 3.2 Algemene Verordening Gegevensbescherming

Wageningen University & Research heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig Verwerken van Persoonsgegevens en het nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige Verwerking van data c.q. Persoonsgegevens) geïmplementeerd door middel van het Beleid.

### 3.3 Archiefwet

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

---

<sup>8</sup> <http://www.wageningenur.nl/nl/Over-Wageningen-UR/Corporate-Governance.htm>

---

## 4 Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens

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

### 4.1 College van Bestuur

Het college van bestuur is eindverantwoordelijk voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen Wageningen University & Research 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 de Verwerking van Persoonsgegevens in portefeuille heeft.

### 4.3 Functionaris gegevensbescherming

Wageningen University & Research is verplicht om een interne toezichthouder op de Verwerking van Persoonsgegevens aan te stellen. Deze toezichthouder wordt functionaris voor de gegevensbescherming (FG) genoemd. De FG houdt binnen Wageningen University & Research toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij Wageningen University & Research.

### 4.4 Systeemeigenaar

De systeemeigenaar 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 Verwerking Persoonsgegevens is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het Beleid;
- toe te zien op de naleving van het Beleid door zijn medewerkers;
- periodiek het onderwerp bescherming Persoonsgegevens onder de aandacht te brengen in Werkoverleggen.

---

## 5 Implementatie Beleid

Het college van bestuur van Wageningen University & Research is verantwoordelijk voor Verwerkingen van de Persoonsgegevens waarvan zij het doel en de middelen voor de Verwerking vaststelt. Zij wordt aangemerkt als de Verwerkingsverantwoordelijke in de zin van de AVG. De feitelijke Verwerking van Persoonsgegevens wordt echter op allerlei lagen van Wageningen University & Research uitgevoerd. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat onder andere de relatie met de belangrijkste stakeholders van Wageningen University & Research, zoals de: medewerkers, studenten, derden en de samenleving als geheel. Een goed corporate governancebeleid draagt zorg voor de rechten van alle Betrokkenen.

### 5.1 Verdeling van de verantwoordelijkheden

- Het zorgvuldig verwerken van Persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid: dat betekent dat de lijnmanagers (afdelingshoofden/centrale stafdiensten) de primaire verantwoordelijk dragen voor een 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 imagooverlies van Wageningen University & Research of van individuen. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.<sup>9</sup>

### 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 dit onderwerp op verschillende niveaus.

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

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 door de architectuur board.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Het operationeel niveau wordt ingevuld door het directeuren bedrijfsvoeringsoverleg.

---

<sup>9</sup> <https://www.wur.nl/nl/Over-Wageningen/Integriteit.htm>

---

## 5.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het Verwerken van Persoonsgegevens uit te sluiten. Noodzakelijk is het om bij Wageningen University & Research 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 gezamenlijke verantwoordelijkheid van alle stakeholders van Wageningen University & Research waaronder in het bijzonder het college van bestuur als de Verwerkingsverantwoordelijke, het lijnmanagement, de Functionaris voor de Gegevensbescherming, de (centrale) Information Security Officer en de (decentrale) Security Managers en privacy officers.

## 5.4 Controle en naleving

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. De Functionaris voor de Gegevensbescherming initieert gezamenlijk met de (centrale) Information Security Officer en de interne auditor de controle op het rechtmatig en zorgvuldig Verwerken van Persoonsgegevens.

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

In geval de naleving op de bescherming van data- en privacygegevens ernstig tekort schiet kan Wageningen University & Research de betrokken medewerkers eventueel een sanctie opleggen binnen de kaders van de CAO of andere wettelijke mogelijkheden.

Het Verwerken van Persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten Wageningen University & Research maken het noodzakelijk om periodiek te bezien of het Beleid voldoende op koers ligt.

---

# 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 de AVG artikel 6. De Verwerkingsverantwoordelijke 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 ze zijn verkregen.

Wageningen University & Research treft de nodige maatregelen om te zorgen dat Persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden Verwerkt, juist en nauwkeurig zijn.

Bij (onderzoek)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met privacy by design dan wel het uitvoeren van een Gegevensbeschermingseffectbeoordeling/ Privacy Impact Assessment (PIA). Bij onderzoeksprojecten worden met betrekking tot het wetenschappelijk onderzoek en privacy de best practices gevolgd op de website van het Landelijk Coördinatiepunt Research Data Management (LCRDM) <https://www.lcrdm.nl/>.

Wageningen University & Research hanteert bij de aanschaf en implementatie van nieuwe systemen de principes: "Privacy by Design" en meer algemeen: "Privacy by Default".

## 6.2 Melden en documenteren van Verwerkingen

Een geheel of gedeeltelijk geautomatiseerde Verwerking van Persoonsgegevens dient gemeld te worden bij de FG. De FG beoordeelt de rechtsgeldigheid van de registratie en laat zorg dragen voor adequate documentatie.

De Verwerkingen worden voldoende gedocumenteerd en gepubliceerd op voor de Betrokkene toegankelijke media met vermelding van het doel van de registraties en de Verwerkingsverantwoordelijken.

## 6.3 De organisatie van de beveiliging

Wageningen University & Research 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 om 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 Wageningen University & Research.

Vanwege de aanzienlijke materiële risico's is de risicoanalyse op privacybescherming en informatiebeveiliging opgenomen in de Governance Code van Wageningen University & Research en daarmee ondergebracht in het aandachtgebied van de raad van toezicht.

---

## 6.4 Geheimhouding

Bij Wageningen University & Research 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 ambt, 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<sup>10</sup> buiten het bereik van de actieve administratie gebracht te worden. Wageningen University & Research zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, adequaat archiveren.

## 6.6 Bijzondere Persoonsgegevens

Het verwerken van bijzondere Persoonsgegevens is verboden, tenzij er sprake is van een wettelijke grondslag (b.v. arbeids- en sociaal zekerheidsrecht), uitdrukkelijke toestemming van de Betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze Persoonsgegevens. Daar waar de 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. Bijzondere Persoonsgegevens kunnen mogelijk uit een bepaalde context (een aantal niet bijzondere gegevens) gedistilleerd worden waardoor ook deze gegevens onder de kwalificatie bijzondere Persoonsgegevens kunnen komen te vallen.

## 6.7 Doorgifte Persoonsgegevens aan Derden

### 6.7.1 Uitbesteden van Verwerking aan een Verwerker

Indien Wageningen University & Research Persoonsgegevens laat verwerken door een derde partij als Verwerker, wordt de uitvoering van Verwerkingen geregeld in een separate schriftelijke overeenkomst tussen Wageningen University & Research, de Verwerkingsverantwoordelijke en deze derde partij in de hoedanigheid van Verwerker.

### 6.7.2 Doorgifte Persoonsgegevens binnen de Europese Unie (inclusief de EER)

Wageningen University & Research verstrekt Persoonsgegevens alleen aan Derden als deze doorgifte voldoet aan de criteria gesteld in hoofdstuk V van de AVG (artikelen 44 t/m 50). Bijzondere

---

<sup>10</sup> Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of bij formele studieresultaten, maar ze kunnen ook zijn vastgelegd door Wageningen University & Research, b.v. in een overeenkomst tussen Wageningen University & Research en de Betrokkenen

---

persoonsgegevens worden niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

### 6.7.3 Doorgifte Persoonsgegevens buiten de Europese Unie

Wageningen University & Research verstrekt Persoonsgegevens alleen aan Derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of dat bedrijf/die instelling specifiek een passend beschermingsniveau waarborgt.

Wageningen University & Research verstrekt Persoonsgegevens alleen aan landen zonder passend beschermingsniveau, waar zij een vergunning van de Minister van Veiligheid & Justitie heeft verkregen, dan wel o.b.v. een modelcontract (als opgesteld door de Europese Commissie) een contract is aangegaan. In beide gevallen voorziet Wageningen University & Research de Autoriteit Persoonsgegevens (AP) van een melding van doorgifte naar een land buiten de EU.

### 6.7.4 Lijst van (niet limitatieve) Derden aan wie Wageningen University & Research Persoonsgegevens doorgeeft

- DUO
- Overheidsinstellingen
- Gemeenten
- Belastingdienst
- Stage bedrijven/organisaties
- Studenten woning corporaties
- Studieverenigingen
- Studentenverenigingen
- Sportverenigingen



---

# 7 Incidenten met betrekking tot Persoonsgegevens

Iedere klacht of melding met betrekking tot de Verwerking van Persoonsgegevens binnen Wageningen University & Research is een incident. De bekendste vorm van zo'n incident is diefstal of het hacken van gegevensdragers (laptop/telefoon/usb-stick e.d.) of de servers van Wageningen University & Research. Wanneer Persoonsgegevens betrokken zijn bij diefstal of een hack spreken we van 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 dienen te worden gemeld bij de servicedesk IT of in uitzonderlijke gevallen bij de vertrouwenspersoon of studentbegeleiding van Wageningen University & Research. Van elk incident, de afhandeling en eventueel te nemen maatregelen zal een verplichte nauwgezette registratie bijgehouden worden. De meldingsformulieren worden door de Servicedesk IT verstrekt die ook op de website van Wageningen University & Research te downloaden zijn.

Een incident kan gemeld worden door een Betrokkene, een Verwerker of een Derde.

## 7.2 Afhandeling

Incidenten worden zo veel mogelijk doorgezet naar de afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures afgehandeld.

Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van Wageningen University & Research in geding zijn, worden in ieder geval het college van bestuur, de (centrale) Information Security Officer en de FG op de hoogte gesteld.

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 met betrekking tot Persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van het college van bestuur en van de FG.

## 7.4 Bijzondere omstandigheden

Om voorbereid te zijn op (de dreiging tot) incidenten op het gebied van Persoonsgegevens in bijzondere omstandigheden heeft Wageningen University & Research een speciaal operationeel team, Calamiteiten Management Team (CMT), ingesteld.

---

Dit team heeft als voornaamste taak om te acteren bij incidenten met Persoonsgegevens in die gevallen waarbij de staande organisatie een incident niet via de standaard procedures kan oplossen. Dit kan zijn omdat het incident plaatsvindt buiten de reguliere openingstijden van Wageningen University & Research, in een periode waarbij de reguliere bedrijfsprocessen verstoord zijn of omdat de aard van het incident vraagt om noodmaatregelen en/of specifieke mandaten om deze maatregelen uit te voeren.

Het CMT werkt volgens een door het college van bestuur vastgesteld Operationeel Model en heeft bijzondere mandaten die overeenkomen met de mandaten van de FG waarbij het team altijd achteraf verantwoording moet afleggen waarom en op welke wijze het team van deze mandaten gebruik heeft gemaakt.

Het team heeft een directe link naar het college van bestuur als Verwerkingsverantwoordelijke in kader van de relevante wet- en regelgeving.

---

# 8 Rechten van Betrokkenen

## 8.1 Informatieplicht

### **Algemene mededeling**

Wageningen University & Research beoogt het Beleid Verwerking Persoonsgegevens aan studenten, medewerkers en andere Betrokkenen door middel van algemene kennisgeving mede te delen. Daarnaast beoogt Wageningen University & Research, in overeenstemming met de wet, Betrokkene onder bepaalde omstandigheden rechten te verschaffen waarmee de aan Betrokkene toebehorende Persoonsgegevens naar behoren kunnen beschermen.

Wageningen University & Research verstrekt de Betrokkene tenminste het volgende:

- De identiteit en contactgegevens van de Verwerker en indien van toepassing die van de Functionaris Gegevensbescherming;
- De specifieke doeleinden van Verwerking waarvoor de Persoonsgegevens zijn bestemd, alsook informatie betreffende de beveiliging van Verwerking;
- De periode gedurende welke de Persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen;
- Het bestaan van het recht om van de Verwerker toegang tot en rectificatie of wissen van Persoonsgegevens betreffende de Betrokkene te verlangen;
- Het recht om een klacht in te dienen bij het college van bestuur;
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.

### **Mededeling van aanpassingen**

Als het Beleid mettertijd ingrijpend wordt aangepast dan wel verandert, deelt Wageningen University & Research deze wijzigingen in algemene zin mede via de website, om zodoende zorgvuldige en behoorlijke Verwerking te waarborgen (zie ook Hoofdstuk 8).

## 8.2 Recht op inzage

### **Verzoek tot inzage**

Iedere Betrokkene heeft recht op inzage in hem betreffende verwerkte Persoonsgegevens. Een verzoek hiertoe kan schriftelijk worden ingediend bij het functionele E-mailadres van het privacy team van Wageningen University & Research.

Een verzoek tot inzage van minderjarigen die de leeftijd van 16 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger.

### **Termijn**

Op het verzoek wordt zo spoedig mogelijk, doch uiterlijk binnen vier weken na indiening, schriftelijk gereageerd. Wageningen University & Research draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.

### **Mededeling**

Indien gegevens worden verwerkt, bevat de inhoudelijke reactie van Wageningen University & Research 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.

---

## **Kosten**

Iedere eerste aanvraag kan kosteloos worden ingediend. Per additionele aanvraag zal Wageningen University & Research een vergoeding van administratieve kosten a € 25,- in rekening brengen bij de Betrokkene.

## **8.3 Recht op verbetering, aanvulling, verwijdering, afscherming of dataportabiliteit**

### **Verzoek tot verbetering, aanvulling verwijdering, afscherming of dataportabiliteit**

Iedere Betrokkene kan met betrekking tot over hem opgenomen Persoonsgegevens bij Wageningen University & Research van deze gegevens verzoeken die te wijzigen, verbeteren, aan te vullen, te verwijderen, af te schermen, of over te laten dragen.

Een verzoek tot verbetering, aanvulling, verwijdering, afscherming van minderjarigen die de leeftijd van 16 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger. Bij alle registraties op vrijwillige basis zal aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

### **Termijn**

Wageningen University & Research deelt binnen vier weken na ontvangst van het verzoek schriftelijk aan de Betrokkene mede of zijn verzoek gegrond is.

### **Kennisgeving**

Indien opgenomen Persoonsgegevens van de Betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de Verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, verbetert de gegevensbeheerder (functioneel beheerder dan wel de Verwerker) deze gegevens.

Bovendien worden Derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld. De verzoeker mag opgave verzoeken van degene aan wie Wageningen University & Research deze mededeling heeft gedaan.

### **Termijn voor uitvoering**

De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

## **8.4 Recht van bezwaar/verzet**

### **Gronden voor bezwaar/verzet:**

In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar aantekenen tegen Verwerking bij Wageningen University & Research, als deze Verwerking plaatsvond op grond van:

- a. de vervulling van een publiekrechtelijke taak van de gegevensbeheerder; of,
- b. de behartiging van het gerechtvaardigd belang van Wageningen University & Research of van een Derde aan wie de gegevens worden verstrekt;
- c. Persoonsgegevens die de worden gebruikt voor wetenschappelijke of statistische doeleinden tenzij het onderzoeken betreft van algemeen belang.

Elke Betrokkene heeft het recht zich te verzetten tegen het gebruik van zijn Persoonsgegevens voor direct marketing-doeleinden en profilering. De verantwoordelijke Verwerker mag de Persoonsgegevens dan niet meer voor deze doeleinden gebruiken.

---

### **Termijn**

Wageningen University & Research beoordeelt binnen vier weken na ontvangst van het bezwaar of verzet of deze gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, treft Wageningen University & Research maatregelen die nodig zijn om de Verwerking te beëindigen.

### **Kosten**

De kosten die Wageningen University & Research hiervoor berekent, bedragen niet meer dan het door de Verwerkingsverantwoordelijke vastgestelde bedrag. De vergoeding wordt teruggegeven in geval het bezwaar of verzet gegrond wordt bevonden.

## **8.5 Rechtsbescherming**

### **Algemene klachten**

Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van het Beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij Wageningen University & Research.

### **Bezwaarmogelijkheden na indienen algemene klacht**

Indien het antwoord van Wageningen University & Research voor de Betrokkene niet leidt tot een voor hem acceptabel resultaat, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de rechtbank.

### **Bezwaarmogelijkheden na afwijzing van een verzoekschrift tot inzage**

Indien Wageningen University & Research afwijzend heeft beslist op een verzoek tot inzage in of verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens, of Wageningen University & Research heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de rechtbank.

### **Termijn indienen bezwaar**

Het schriftelijk verzoek wordt binnen zes weken na ontvangst van het antwoord van Wageningen University & Research ingediend bij de rechtbank. Indien Wageningen University & Research niet binnen de gestelde termijn heeft geantwoord, moet het verzoekschrift binnen zes weken na afloop van de gestelde termijn worden ingediend.

---

## 9 Tot slot

Dit beleid is vastgesteld door de colleges van bestuur van Wageningen University en Wageningen Research op 27 maart 2017. Aanpassingen van dit beleid worden aangekondigd via de website en de meest recente versie is gepubliceerd op de internetpagina van Wageningen University & Research.

Voor vragen of opmerkingen met betrekking tot het Beleid kunt u terecht bij de FG:  
<mailto:functionarisgegevensbescherming@wur.nl>.

To explore  
the potential  
of nature to  
improve the  
quality of life



---

Wageningen University & Research  
Postbus 9101  
6700 HB Wageningen  
[www.wur.nl/nl/Over-Wageningen/Integriteit](http://www.wur.nl/nl/Over-Wageningen/Integriteit)

De missie van Wageningen University & Research is 'To explore the potential of nature to improve the quality of life'. Binnen Wageningen University & Research bundelen Wageningen University en gespecialiseerde onderzoeksinstituten van Stichting Wageningen Research hun krachten om bij te dragen aan de oplossing van belangrijke vragen in het domein van gezonde voeding en leefomgeving. Met ongeveer 30 vestigingen, 5.000 medewerkers en 10.000 studenten behoort Wageningen University & Research wereldwijd tot de aansprekende kennisinstellingen binnen haar domein. De integrale benadering van de vraagstukken en de samenwerking tussen verschillende disciplines vormen het hart van de unieke Wageningen aanpak.

---