

Proces Uitwisselen van persoonsgegevens

Voorbeelddocument

Versie: juni 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je bij het maken van een eigen proces voor het verantwoord uitwisselen van persoonsgegevens. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan, zodat het past bij jouw situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het beleid definitief maakt.
* Dit beleid gaat ervan uit dat taken, rollen en functies die nodig zijn om het beleid uit te voeren bij de juiste personen zijn belegd. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///C%3A/Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een e-mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Geef* *hier aan wie het document vaststelt. Dit kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld. |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties>. |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 5](#_Toc202170418)

[2 Processtappen 5](#_Toc202170419)

[2.1 Bepalen van de AVG-rollen van betrokken partijen 5](#_Toc202170420)

[2.2 Toetsen van gegevensverstrekkingen aan externe partijen 6](#_Toc202170421)

[2.3 Opstellen van een overeenkomst, indien vereist of wenselijk 6](#_Toc202170422)

[2.4 In kaart brengen en toetsen van gegevensuitwisselingen buiten de EER 7](#_Toc202170423)

[2.5 Controle en naleving 8](#_Toc202170424)

[3 Rollen en verantwoordelijkheden 10](#_Toc202170425)

# Inleiding

In een digitale leeromgeving wordt het delen van persoonsgegevens steeds gebruikelijker én noodzakelijker. Tegelijkertijd brengt dit verantwoordelijkheden met zich mee.Met dit proces tonen we als *<Naam schoolbestuur of naam school>* aan dat we persoonsgegevens zorgvuldig, veilig en in overeenstemming met de wet uitwisselen. We beschrijven hiervoor een stapsgewijze aanpak, met aandacht voor onder andere de voorbereiding, de rolbepaling volgens de AVG, het opstellen van verwerkersovereenkomsten en het veilig delen van gegevens, zowel binnen als buiten de Europese Economische Ruimte (EER).

# Processtappen

Het proces voor het uitwisselen van persoonsgegevens bestaat uit vier stappen:

1. Bepalen van de AVG-rollen van betrokken partijen
2. Toetsen van gegevensverstrekkingen aan externe partijen
3. Opstellen van een overeenkomst, indien vereist of wenselijk
4. In kaart brengen en toetsen van gegevensuitwisselingen buiten de EER

Hieronder lichten we elke stap toe.

## Bepalen van de AVG-rollen van betrokken partijen

***Toelichting***

* *In deze stap bepaal je de AVG-rollen van de partij met wie je gegevens uitwisselt. Je gaat ook na of je alle samenwerkingen en gegevensuitwisselingen in kaart hebt gebracht. Je kunt hiervoor gebruikmaken van de deelprojecten* [*1.5 Informatiearchitectuur in kaart brengen*](https://normenkaderibp.kennisnet.nl/groeipad/fase-1/deelproject-1-5-informatiearchitectuur-in-kaart-brengen/) *en* [*2.1 Opstellen verwerkingsregister*](https://normenkaderibp.kennisnet.nl/groeipad/fase-2/deelproject-2-1-opstellen-verwerkingsregister/) *helpen je daarbij. Tip: in het verwerkingsregister is een opgenomen van categorieën ontvangers.*
* *Er zijn verschillende handreikingen en artikelen beschikbaar die concrete richtsnoeren bevatten voor het uitwisselen van persoonsgegevens in specifieke situaties. Deze vind je terug op de deelprojectpagina.*
* *Voor het bepalen van de AVG-rol kun je gebruikmaken van de beslisboom van Kennisnet die je terugvindt op de deelprojectpagina. Gebruik je deze beslisboom niet? Pas dat dan aan in de beschrijving hieronder en geef aan hoe je het op jouw school doet. De school is bijna altijd verwerkersverantwoordelijke.*
1. Bepaal de AVG-rol van alle betrokken partijen. <Naam schoolbestuur of naam school> gebruikt hiervoor de beslisboom van Kennisnet.
2. Ga na of alle verwerkingen van persoonsgegevens binnen de school zorgvuldig in kaart zijn gebracht en of is vastgesteld welke externe partijen daarbij betrokken zijn. Daarbij wordt per partij bepaald of deze optreedt als verwerker, zelfstandig verwerkingsverantwoordelijke of gezamenlijk verwerkingsverantwoordelijke.
3. Train medewerkers in het herkennen van verschillende rollen en het belang hiervan.

## Toetsen van gegevensverstrekkingen aan externe partijen

***Toelichting***

* *In deze stap beschrijf je hoe je elke gegevensverstrekking aan externe partijen zorgvuldig toetst aan de AVG. Je kunt hiervoor de Template Verstrekken van persoonsgegevens aan een andere partij van Kennisnet gebruiken. Maak je gebruik van een andere methode? Pas de beschrijving van de stap hieronder dan aan.*
* *Bij de beoordeling wordt onder andere gekeken naar het doel van de gegevensverwerking, de juridische grondslag, de betrokken personen, de categorieën persoonsgegevens die worden verwerkt (zoals gevoelige of bijzondere gegevens) en de wijze waarop de uitwisseling veilig plaatsvindt. Je kunt hiervoor gebruikmaken van het Formulier Verstrekken van persoonsgegevens aan een andere partij van Kennisnet.*
* *Je kunt bij de toetsing gebruikmaken van de uitkomsten van andere deelprojecten. Zo biedt het* [*IBP-beleid in deelproject 1.3*](https://normenkaderibp.kennisnet.nl/groeipad/fase-1/deelproject-1-3-beleid-en-strategie-voor-ibp-bepalen/) *houvast voor de juiste juridische grondslag en naleving van privacyregels. Het* [*Model verwerkingsregister in deelproject 2.1*](https://normenkaderibp.kennisnet.nl/groeipad/fase-2/deelproject-2-1-opstellen-verwerkingsregister/) *helpt bij het bepalen van het doel van de gegevensverwerking. Voor het inschatten van privacyrisico’s en het uitvoeren van een (pre-)DPIA, geeft* [*deelproject 2.6*](https://normenkaderibp.kennisnet.nl/groeipad/fase-2/deelproject-2-6-privacyrisicos-inschatten-met-pre-dpias/) *praktische handvatten en deelproject 3.3 biedt* [*richtlijnen voor bewaartermijnen*](https://normenkaderibp.kennisnet.nl/groeipad/fase-3/deelproject-3-3-bewaren-en-vernietigen-van-gegevens/)*. In deelproject 4.2 staat hoe je* [*betrokkenen (ouders en leerlingen) goed informeert*](https://normenkaderibp.kennisnet.nl/groeipad/fase-4/deelproject-4-2-betrokkenen-informeren-over-privacyrechten/) *over de gegevensdeling en hun rechten, en in deelproject 5.8 hoe je* [*persoonsgegevens op de juiste manier beveiligt*](https://normenkaderibp.kennisnet.nl/groeipad/fase-4/deelproject-4-2-betrokkenen-informeren-over-privacyrechten/)*.*
* *Bewaar loggegevens voor eventuele audits en verdere onderzoeken. Denk hierbij aan een bewaartermijn van 12 maanden.*
1. Toets vooraf of de gegevensverstrekking aan een externe partij in overeenstemming is met de AVG en andere wet- of regelgeving. We gebruiken hiervoor de Template Verstrekken persoonsgegevens aan een andere partij die Kennisnet aanbiedt.
2. Medewerkers van <naam schoolbestuur of naam school> kunnen bij <geef aan bij wie of waar medewerkers terecht kunnen> met vragen over gegevensuitwisseling.
3. Betrek medewerkers actief bij het naleven van deze toetsingsstappen door <geef aan hoe je medewerkers actief betrekt>.

## Opstellen van een overeenkomst, indien vereist of wenselijk

***Toelichting***

* *In deze stap beschrijf je hoe je elke gegevensverstrekking aan externe partijen zorgvuldig toetst aan de AVG. Je kunt hiervoor de Template Verstrekken van persoonsgegevens aan een andere partij van Kennisnet gebruiken. Maak je gebruik van een andere methode? Pas de beschrijving van de stap hieronder dan aan.*
* *Besteed je de verwerking van persoonsgegevens uit aan een derde partij? Dan blijf je als school volgens de AVG verantwoordelijk voor een veilige verwerking van persoonsgegevens. Je bent in dit geval verplicht om een verwerkersovereenkomst af te sluiten, zodat de privacy van medewerkers, leerlingen en ouders is gewaarborgd. Het afsluiten van een overeenkomst wordt in deze stap beschreven.*
* *In Stap 2.1 heb je de AVG-rol van alle partijen bepaald. Afhankelijk van deze rol bepaal je wie (eind)verantwoordelijk is en of er een verwerkersovereenkomst moet worden gesloten. De verwerkersovereenkomst documenteert de verdeling van taken en verantwoordelijkheden en onderbouwt zo de naleving van het verantwoordingsbeginsel uit de AVG.*
* *Voor scholen in het primair onderwijs (po), voortgezet onderwijs (vo) en middelbaar beroepsonderwijs (mbo) zijn er collectieve afspraken gemaakt met leveranciers van digitale leermiddelen. Deze zijn vastgelegd in het Privacyconvenant Onderwijs. Onderdeel hiervan is een* [*Model verwerkersovereenkomst*](https://www.privacyconvenant.nl/downloads/)*. Maak je gebruik van deze overeenkomst? Dan weet je zeker dat het de juiste inhoud bevat. Legt een partij jou een eigen overeenkomst voor? Dan moet je controleren of daar de juiste afspraken in zijn vastgelegd.*
1. Controleer altijd of de partij met wie een verwerkersovereenkomst wordt afgesloten is aangesloten bij het Privacyconvenant Onderwijs. Is de partij met wie een verwerkersovereenkomst wordt afgesloten niet aangesloten bij het convenant? Vraag deze partij dan om dit alsnog te doen. Bij voorkeur als deelnemer en anders als medestander. Is dit niet mogelijk? Leg dan de leverancier een passend model voor, afhankelijk van de AVG-rol van de leverancier.
2. Controleer of de inhoud van de verwerkersovereenkomst voldoet aan de AVG en of de overeenkomst de juiste afspraken bevat. Controleer bij een aanpassing door de partij met wie een verwerkersovereenkomst wordt afgesloten ook of deze is uitgelegd in een aparte bijlage. Heb extra aandacht voor de privacybijsluiter, met name voor de bijlage die beschrijft welke persoonsgegevens worden verwerkt en voor de bijlage die beveiligingsmaatregelen beschrijft.
3. Zijn de overeenkomsten correct opgesteld? Laat ze dan ondertekenen door het bevoegd gezag van <naam schoolbestuur of naam school> alle overeenkomsten tekenen.

## In kaart brengen en toetsen van gegevensuitwisselingen buiten de EER

***Toelichting***

* *Bij het in kaart brengen van gegevensuitwisselingen en het opstellen van een overeenkomst, is speciale aandacht vereist voor gegevensstromen buiten de EER. Van scholen wordt namelijk verwacht dat ze ook de gegevensuitwisselingen naar het buitenland in kaart brengen. Het gaat dan om doorgifte. In deze stap bepaal je of er sprake is van een gegevensuitwisseling buiten de EER en leg je vast wat je in dat geval moet doen om een veilige gegevensuitwisseling te garanderen.*
* *Doorgifte betekent dat je persoonsgegevens doorstuurt van Nederland naar een land buiten de EER, bijvoorbeeld als een school of leverancier gegevens opslaat in een datacenter in India. Dat mag meestal niet zomaar. Het mag alleen als het land buiten de EER goed omgaat met persoonsgegevens en genoeg bescherming biedt. Er zijn speciale regels om dit toch mogelijk te maken. Die regels heten “overdrachtsmechanismen”. Je leest er meer over op* [*de website van de Autoriteit Persoonsgegevens*](https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-buiten-de-eer)*.*
* *Waar mogelijk, is het raadzaam om zo veel mogelijk samen te werken met leveranciers die persoonsgegevens uitsluitend binnen de EER opslaan en verwerken. Dit voorkomt de noodzaak voor een Data Transfer Impact Assessment (DTIA) en het nemen van aanvullende maatregelen. Het sluit bovendien aan bij het principe van digitale autonomie: de vrijheid van scholen om zelf regie te voeren over hun digitale onderwijsomgeving.*
* *Let op dat* expliciet wordt vastgelegd *dat de gegevens daadwerkelijk binnen de EER blijven en niet zonder voorafgaande toestemming buiten deze regio worden doorgegeven.*
* *Je geeft in deze stap ook aan hoe je de stappen en beslissingen rondom gegevensverwerking buiten de EER vastlegt. Dat kan via het verwerkingsregister, evaluaties van verwerkersovereenkomsten en periodieke audits en controles. Het model verwerkingsregister van Kennisnet bevat een aparte kolom voor informatie over de doorgifte en het toegepaste doorgiftemechanisme.*
* *De doorgifte van persoonsgegevens naar een land buiten de EER is complex en vraagt om een zorgvuldige beoordeling. Win daarom advies in bij de functionaris gegevensbescherming (FG) of de informatiebeveiligings- en privacyfunctionaris (IBP’er) van je school. Voor leveranciersgerelateerde vragen kun je terecht bij SIVON. Zij beschikken over ruime ervaring met leveranciers en diepgaande kennis van relevante risico’s. Deze expertise is van belang bij het doorlopen van de stappen C tot en met F binnen dit proces.*
1. Controleer of er sprake is van het uitwisselen van gegevens met een land buiten de EER.
2. Leg de doorgifte van persoonsgegevens aan landen buiten de EER[[1]](#footnote-2) inclusief verwerkers en subverwerkers vast in <geef aan waar je dit vastlegt.> Maak hiervoor gebruik vanhet verwerkingsregister, verwerkersovereenkomsten en andere contracten, onderzoek naar software en clouddiensten die je in gebruik hebt, de (pre-)DPIA’s die je hebt uitgevoerd en doe navraag bij leveranciers en andere partijen met wie je gegevens uitwisselt*.* Hou daarbij ook rekening met indirecte doorgiftes, zoals cloudopslag of externe ondersteuning met toegang tot data. Beoordeel de effectiviteit van het gekozen overdrachtsmechanisme en neem indien nodig aanvullende maatregelen.
3. Voer indien nodig een Data Transfer Impact Analyse (DTIA) uit om mogelijke privacyrisico’s te identificeren en mitigeren. De DTIA vindt plaats op basis van publiek beschikbare informatie, in samenwerking met de gegevensontvanger. Identificeer en implementeer aanvullende contractuele, technische en/of organisatorische maatregelen, zoals versleuteling (encryptie) en pseudonimisering, om het beschermingsniveau op het vereiste niveau te brengen als uit de beoordeling blijkt dat dit onvoldoende is.
4. Verifieer of de verwerker de afgesproken technische en organisatorische maatregelen daadwerkelijk heeft geïmplementeerd en toepast. Volg alle noodzakelijke formele stappen bij de implementatie van aanvullende maatregelen.
5. Evalueer minimaal één keer per jaar of de gegevensdoorgifte nog in overeenstemming is met de geldende wet- en regelgeving en passen waar nodig de maatregelen aan of beëindigen de doorgifte als het vereiste beschermingsniveau niet langer kan worden gewaarborgd.
6. Leg alle stappen en beslissingen rond gegevensuitwisseling met landen buiten de EER goed vast.

## Controle en naleving

***Toelichting***

*Het is belangrijk dat je alles stappen en beslissingen die je neemt rond gegevensuitwisseling goed documenteert. Bijvoorbeeld in het verwerkingsregister, het systeem voor contractbeheer en de auditlog.*

1. Zorg ervoor dat alle stappen en beslissingen rond gegevensuitwisseling goed worden vastgelegd.
2. Controleer periodiek de samenwerking met externe partijen en check of de gegevensverwerking nog altijd voldoet aan de AVG en of de gegevensuitwisseling plaatsvindt volgens de gemaakte afspraken.

# Rollen en verantwoordelijkheden

***Toelichting***

* *Hier geef je aan welke rollen zijn betrokken bij het proces voor het uitwisselen van persoonsgegevens.*
* *Bij kleinere organisaties zullen verschillende verantwoordelijkheden worden gecombineerd of anders worden ingevuld.*

De volgende rollen zijn binnen <vul naam schoolbestuur in> bij het proces voor het verantwoord uitwisselen van persoonsgegevens.

|  |  |
| --- | --- |
| **Rol**  | **Verantwoordelijkheden** |
| **Eerste lijn** |
| Het schoolbestuur | * Ziet erop toe dat persoonsgegevens zorgvuldig worden gedeeld en dat daarbij passende overeenkomsten met externe partijen zijn afgesloten.
* Stelt het proces formeel vast voor de beoordeling en goedkeuring van doorgiftes.
* <Vul aan met verantwoordelijkheden>.
 |
| **Tweede lijn** |
| Proceseigenaar | * Bewaakt veilige en verantwoorde gegevensuitwisseling binnen diens processen.
* <Vul aan met verantwoordelijkheden>.
 |
| IBP’er (bijvoorbeeld ICT-coördinator, privacy en security officer/ coördinator/functionaris) afdeling administratie, afdeling inkoop/contractbeheer, juridische afdeling, informatiemanager | * Werken samen en delen verantwoordelijkheden bij een veilige en verantwoorde uitwisselingen van persoonsgegevens. Een aantal kernactiviteiten zijn:
	+ Bepalen van AVG-rollen van andere partijen.
	+ Inzicht in datastromen, betrokken systemen, leveranciers en andere partijen.
	+ Toetsen van gegevensuitwisselingen.
	+ In kaart brengen van doorgiftes, inclusief dataopslag en toegangsrechten.
	+ Opstellen en toetsen van contractuele afspraken, inclusief periodieke herbeoordeling.
	+ Toetsen van doorgiftes buiten de EU/EER, inclusief controle op doorgiftemechanismen, aanvullende beveiligingsmaatregelen (zoals encryptie) en documentatie.
 |
| Docenten, onderwijspersoneel | * Selecteren zorgvuldig welke persoonsgegevens worden gedeeld; de administratie voert doorgaans de uitwisseling uit. Er wordt geen data gedeeld met onbevoegden of via onbeveiligde kanalen.
* Medewerkers zijn getraind, risicobewust en stellen vragen bij twijfel over de juistheid van de gegevensuitwisseling.
 |
| **Derde lijn** |
| Functionaris gegevensbescherming | * Houdt toezicht op verantwoorde gegevensuitwisseling, adviseert over risico’s bij doorgifte buiten de EER en toetst periodiek bestaande doorgiftes (compliance).
* <Vul aan met verantwoordelijkheden>.
 |
| Interne audit | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |

1. EU en Noorwegen, Liechtenstein en IJsland [↑](#footnote-ref-2)