

Privacy by design en privacy by default

Voorbeelddocument

Versie: Maart 2025



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

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van eigen privacy by design en privacy by default principes. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen 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 de procesbeschrijving definitief maakt.
* Deze procesbeschrijving gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces uit te voeren bij de juiste personen belegd zijn. 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:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Geef hier aan wie het document vaststelt. Dat 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. Privacy by design-principes 5](#_Toc194329039)

[1.1 Proactief en preventief, niet reactief 5](#_Toc194329040)

[1.2 Privacy als standaardinstelling 5](#_Toc194329041)

[1.3 Privacy ingebouwd in het ontwerp 6](#_Toc194329042)

[1.4 Volledige functionaliteit zonder privacycompromissen 6](#_Toc194329043)

[1.5 Volledige beveiliging gedurende de gehele levenscyclus 7](#_Toc194329044)

[1.6 Zichtbaarheid en transparantie 7](#_Toc194329045)

[1.7 Respect voor de privacy van de gebruiker 8](#_Toc194329046)

[2. Privacy by default-principes 9](#_Toc194329047)

[2.1 Doelbinding 9](#_Toc194329048)

[2.2 Minimale gegevensverwerking 9](#_Toc194329049)

[2.3 Privacyvriendelijke standaardinstellingen 9](#_Toc194329050)

[2.4 Toegangsbeheer 10](#_Toc194329051)

[2.5 Transparantie 10](#_Toc194329052)

# Privacy by design-principes

De Algemene Verordening Gegevensbescherming (AVG) verplicht scholen om vanaf het begin van het gebruik van persoonsgegevens rekening te houden met privacy en gegevensbescherming. De beginselen *privacy by design* (gegevensbescherming door ontwerp) en *privacy by default* (gegevensbescherming door standaardinstellingen) uit de AVG zijn hierop van toepassing. Deze principes helpen om privacyrisico’s te beperken.

We houden als <naam schoolbestuur> de volgende 7 privacy by design-principes aan.

## Proactief en preventief, niet reactief

Privacy by design betekent dat je vooruitdenkt en proactief werkt aan privacybescherming, in plaats van achteraf problemen op te lossen.

Dat doen we als school door:

* Bij inkoop en selectie van nieuwe software te zorgen dat er eisen worden gesteld aan leveranciers. Dit kan door deze eisen van privacy by design en default als eis mee te nemen in een aanbesteding of offerte-uitvraag.
* Te controleren of een DPIA nodig is en dit uit te voeren vóórdat we nieuwe softwarepakketten gaan gebruiken. We houden een register van uitgevoerde pre-DPIA’s en DPIA’s bij.

## Privacy als standaardinstelling

Systemen zijn standaard zo ingesteld dat ze maximale privacybescherming bieden zonder dat de gebruiker daar iets voor hoeft te doen.

Dat doen we door:

* Vast te leggen dat voor gebruik van nieuwe software, updates en ieder systeem dat veel of gevoelige persoonsgegevens verwerkt, de privacyinstellingen zijn gecontroleerd <door de ICT-coördinator, ICT-beheerder of functioneel applicatiebeheerder> en er altijd voor de meest privacyvriendelijke instellingen is gekozen.
* Te zorgen dat leerlingen en medewerkers alleen toegang hebben tot informatie die zij nodig hebben voor hun les en hun werk, volgens het principe ‘*need to know, need to act*’.
* Bij gebruik van webapplicaties te zorgen voor zo min mogelijk tracking- en analysecookies.
* Het delen van persoonsgegevens standaard uit te zetten (zo veel mogelijk te beperken) en ook download- of exportmogelijkheden standaard uit te zetten.
* Te zorgen dat informatie altijd beschikbaar is om in te zien of te delen met leerlingen en hun ouders (recht van inzage).

## Privacy ingebouwd in het ontwerp

Privacy is geen toevoeging achteraf, maar een essentieel onderdeel dat vanaf het begin in systemen, processen en toepassingen wordt geïntegreerd. Dit principe gaat erom dat privacy en gegevensbescherming standaard zijn ingebouwd in alle technologie en alle werkwijzen die op school worden gebruikt.

Dit doen we als school door:

* Bij de selectie van nieuwe software, applicaties of diensten te kiezen voor leveranciers die kunnen aantonen dat privacy in hun producten is ingebouwd en dit te documenteren in ons verwerkingsregister.
* Voor aanschaf van nieuwe softwarepakketten altijd te vragen naar de technische en organisatorische maatregelen die de leverancier heeft genomen.
* Te controleren of leveranciers pseudonimisering of versleuteling toepassen in hun producten.
* Na te gaan of producten en diensten niet meer gegevens verzamelen dan strikt noodzakelijk is voor het onderwijsdoel.
* Privacyaspecten al in de ontwerpfase van onze eigen processen en projecten mee te nemen en deze overwegingen vast te leggen.
* Privacyvriendelijke alternatieven te overwegen wanneer standaardoplossingen onvoldoende privacybescherming bieden.
* Privacy-eisen expliciet op te nemen in verwerkersovereenkomsten met leveranciers.
* Periodiek te evalueren of de ingebouwde privacymaatregelen nog steeds effectief zijn en deze evaluaties te documenteren.

## Volledige functionaliteit zonder privacycompromissen

Een goede balans tussen functionaliteit en privacy betekent dat privacybescherming niet ten koste gaat van gebruiksgemak en dat gebruiksgemak geen excuus is voor het verzwakken van privacybescherming. Het gaat om een balans die beide waarden respecteert.

Dit doen we als school door:

* Bij de selectie van nieuwe software actief te onderzoeken of er privacyvriendelijke alternatieven bestaan voor populaire applicaties en deze afwegingen te documenteren.
* Ervoor te zorgen dat privacymaatregelen de bruikbaarheid van systemen niet beperken, zodat medewerkers en leerlingen niet geneigd zijn om deze maatregelen te omzeilen.
* Te onderzoeken of applicaties kunnen werken met minder persoonsgegevens of met gepseudonimiseerde informatie, bijvoorbeeld door waar mogelijk te kiezen voor anonieme of pseudonieme accounts zonder functionaliteitsverlies.
* Gebruikers te trainen in het effectief gebruik van privacyvriendelijke systemen, zodat privacymaatregelen niet als belemmerend worden ervaren.

## Volledige beveiliging gedurende de gehele levenscyclus

Dit principe vereist dat persoonsgegevens gedurende de gehele levenscyclus van verzameling tot verwijdering goed beveiligd zijn en blijven. Goede informatiebeveiliging is een essentiële voorwaarde voor privacybescherming en moet worden geïntegreerd in alle fasen van gegevensverwerking.

Dit doen we als school door:

* Een gedegen wachtwoordbeleid en tweefactorauthenticatie te implementeren en dit vast te leggen in ons IBP-beleid.
* Gevoelige en bijzondere persoonsgegevens te versleutelen bij zowel opslag als verzending, en hier periodiek op te controleren.
* Duidelijke afspraken te maken over de veilige verwijdering van gegevens aan het eind van de bewaartermijn en waar mogelijk automatische verwijdering in te stellen.
* Ervoor te zorgen dat software-updates en beveiligingspatches tijdig worden uitgevoerd.
* Regelmatig beveiligingstesten uit te voeren en de resultaten hiervan te documenteren.
* Over een uitgebreide procesbeschrijving te beschikken voor het tijdig melden en afhandelen van datalekken, inclusief een duidelijk stappenplan.
* Over een herstelplan voor het terugzetten van persoonsgegevens te beschikken voor het geval er zich toch een beveiligingsincident voordoet.
* Leveranciers te selecteren die gebruikmaken van het Privacyconvenant en in de beveiligingsbijlage aantoonbaar goede beveiligingsmaatregelen hebben genomen.

## Zichtbaarheid en transparantie

Transparantie betekent dat we open en eerlijk zijn over welke persoonsgegevens we verzamelen, waarom we dit doen en met wie we ze delen. Zichtbaarheid betekent duidelijk communiceren over onze gegevensverwerkingen, waardoor we vertrouwen opbouwen bij leerlingen, hun ouders en medewerkers.

Dit doen we als school door:

* Een duidelijk en actueel verwerkingsregister bij te houden waarin we vastleggen welke persoonsgegevens we verwerken, voor welke doeleinden we dit doen en met welke wettelijke grondslag.
* Een begrijpelijke en toegankelijke gelijkluidende privacyverklaring voor alle scholen op te stellen en deze duidelijk te delen op alle websites van het bestuur en alle scholen.
* Leerlingen en hun ouders actief te informeren over privacy en gegevensbescherming via de schoolgids, nieuwsbrieven, ouderavonden en onze website.
* Eenvoudige procedures te hanteren waarmee leerlingen, ouders en medewerkers inzage kunnen krijgen in hun gegevens die in onze systemen worden gebruikt.
* Jaarlijks (privacy by design en by default) te evalueren en hierover te rapporteren in het jaarverslag.
* Bij nieuwe gegevensverwerkingen proactief te communiceren met de betrokkenen.
* Een aanspreekpunt voor privacyvragen aan te wijzen en diens contactgegevens duidelijk te communiceren.

## Respect voor de privacy van de gebruiker

De belangen en rechten van leerlingen, hun ouders en medewerkers staan centraal bij alle beslissingen over gegevensverwerking. We erkennen dat persoonsgegevens aan mensen toebehoren en niet aan organisaties of leveranciers, en we handelen vanuit respect voor ieders privacyrechten.

Dit doen we als school door:

* De mens centraal te stellen bij het gebruik en inrichten van software.
* Privacy- en gegevensbescherming als prioriteit te stellen in ons beleid en onze dagelijkse werkzaamheden.
* Eenvoudige en toegankelijke procedures te ontwikkelen waarmee betrokkenen toestemming kunnen geven of intrekken voor verwerkingen die daarop zijn gebaseerd.
* Heldere toestemmingsformulieren te gebruiken, waarin we uitleggen waarvoor toestemming wordt gevraagd en wat de gevolgen zijn van het wel of niet geven van toestemming. Zonder dat aan het niet-geven van toestemming nadelige consequenties zijn verbonden.
* Actief te luisteren naar privacyzorgen van leerlingen, hun ouders en medewerkers, en hier serieus op te reageren met concrete verbeteracties.
* Extra beschermingsmaatregelen te treffen voor bijzondere persoonsgegevens zoals gezondheidsgegevens, waaronder versleuteling en striktere toegangscontrole.
* Een duidelijke procedure te hebben voor het uitoefenen van privacyrechten zoals inzage, correctie, verwijdering en bezwaar.
* Een register bij te houden van alle inzage- en andere verzoeken om privacyrechten uit te oefenen.
* De menselijke maat te behouden in een steeds verder digitaliserende onderwijsomgeving door kritisch te blijven op onnodige dataverzameling en -verwerking.

# Privacy by default-principes

Privacy by default gaat over de standaardinstellingen van systemen, maar ook over de manier waarop we omgaan met persoonsgegevens. We houden als <naam schoolbestuur> de volgende 5 privacy by default-principes aan.

## 2.1 Doelbinding

Doelbinding betekent dat we persoonsgegevens alleen verzamelen en gebruiken voor specifieke, vooraf bepaalde doelen. We gebruiken gegevens niet zomaar voor andere doeleinden dan waarvoor we ze oorspronkelijk hebben verzameld.

Dit doen we als school door:

* Vooraf duidelijk vast te leggen voor welk doel we welke persoonsgegevens verzamelen en deze doelen op te nemen in ons verwerkingsregister.
* Deze doelen op te nemen in ons verwerkingsregister.
* Bij het aanschaffen van nieuwe software of diensten te controleren of de gegevensverwerking past bij onze onderwijsdoelen.
* In verwerkersovereenkomsten duidelijke afspraken te maken over doelbinding.

## 2.2 Minimale gegevensverwerking

Minimale gegevensverwerking betekent dat we niet meer gegevens verzamelen dan strikt noodzakelijk is voor het beoogde doel. We bewaren gegevens niet langer dan nodig en zorgen dat alleen mensen die de gegevens nodig hebben er toegang toe hebben.

Dit doen we als school door:

* Kritisch te kijken welke gegevens we echt nodig hebben voor ons onderwijs, waarbij noodzakelijkheid het criterium is.
* Geen persoonsgegevens te gebruiken die ‘handig’ zijn.
* Bewaartermijnen vast te stellen en deze actief toe te passen.
* Regelmatig opschoning uit te voeren van gegevens die niet meer nodig zijn.
* Toegang tot persoonsgegevens te beperken tot de medewerkers die ze nodig hebben.
* Bij leveranciers te controleren of zij ook het principe van dataminimalisatie hanteren.

## 2.3 Privacyvriendelijke standaardinstellingen

Privacyvriendelijke standaardinstellingen betekent dat systemen standaard zo zijn ingesteld dat ze maximale privacybescherming bieden zonder dat gebruikers daar extra handelingen voor moeten verrichten. De meest privacyvriendelijke optie is altijd de standaardoptie.

Dit doen we als school door:

* Nieuwe gebruikersaccounts standaard te voorzien van minimale rechten.
* Onze ICT-systemen zo in te stellen dat ze standaard de minst mogelijke gegevens verzamelen.
* Bij aanschaf van nieuwe systemen te kiezen voor oplossingen met goede standaardinstellingen.
* Periodiek te controleren of de privacyvriendelijke instellingen nog steeds actief zijn.

## 2.4 Toegangsbeheer

Toegangsbeheer als standaardinstelling betekent dat we strikt controleren wie toegang heeft tot welke persoonsgegevens. We zorgen dat alleen bevoegde personen toegang krijgen tot de gegevens die zij voor hun functie nodig hebben, en niet meer dan dat.

Dit doen we als school door:

* Rolgebaseerde toegang toe te passen in al onze systemen.
* Regelmatig te controleren of toegangsrechten nog passend zijn.
* Geautomatiseerde processen in te richten waarbij accounts automatisch worden geblokkeerd zodra leerlingen of medewerkers de school verlaten.
* Automatische uitlogprocedures bij inactiviteit (schermvergrendeling) in te stellen en af te dwingen.
* Bestanden en databases standaard te versleutelen, beveiligen of vergrendelen.
* Een actueel gebruikersbeheerproces te onderhouden.
* Periodieke controles uit te voeren op inactieve accounts en onnodige rechten.

## 2.5 Transparantie

Transparantie betekent dat leerlingen, hun ouders en medewerkers duidelijk en begrijpelijk worden geïnformeerd over onze gegevensverwerkingen. We zijn open over onze gegevensverwerkingen en zorgen dat betrokkenen weten wat er met hun gegevens gebeurt.

Dit doen we als school door:

* Een heldere privacyverklaring op onze schoolwebsite te plaatsen.
* Informatie over gegevensverwerkingen in begrijpelijke taal aan te bieden.
* Ouders actief te informeren bij de start van het schooljaar en bij nieuwe verwerkingen.
* Leerlingen (op een bij hun leeftijd passende manier) uit te leggen waarom we bepaalde gegevens verzamelen.
* Een toegankelijk aanspreekpunt te hebben voor alle vragen over privacy.
* Regelmatig bewustwordingstrainingen te organiseren voor alle medewerkers over privacy en informatiebeveiliging.