

BIJLAGE 1: PRIVACYBIJSLUITER VOOR [naam product/dienst]

Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals onderwijsdeelnemers). Onderwijsinstellingen moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiters geeft onderwijsinstellingen informatie over de dienstverlening die Verwerker verleent en welke persoonsgegevens de Verwerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen van wie persoonsgegevens worden verwerkt.

In het kader van de herkenbaarheid is het wenselijk dat Verwerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacy bijsluiters. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 1A", "Bijlage 1B", etc.. Deze Bijlagen worden aan de Verwerkersovereenkomst gehecht.

A. Algemene informatie¹

Naam product en/of dienst	
Naam Verwerker en vestigingsgegevens	
Link naar <u>leverancier</u> en/of productpagina	
Beknopte uitleg en werking product en dienst	

B. Omschrijving specifieke diensten

1. Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen van Persoonsgegevens:	
a.	
b.	
c.	
2. Omschrijving van de optionele Verwerkingen die de Verwerker aanbiedt	
a.	
b.	

C. Doeleinden voor het verwerken van gegevens

--

¹ Geel in te vullen door de Verwerkers

D1. Categorieën Betrokkenen

(aankruisen welke categorieën Betrokkenen van toepassing zijn)

☐	1: Studenten
☐	2: Medewerkers
☐	3: Relaties

D2. Categorieën Persoonsgegevens

(aankruisen welke categorieën Persoonsgegevens van toepassing zijn)

☐	Contactgegevens beperkt (naam, e-mail adres en organisatorische eenheid)
☐	Contactgegevens overig (Naw, geboortedatum, titulatuur, etc.)
☐	Studenten- / personeelsnummer
☐	Nationaliteit en geboorteplaats
☐	Gezondheidsgegevens student
☐	Gesprekcyclus medewerkers
☐	Beeldmateriaal
☐	Burgerservicenummer (BSN)
☐	Medische gegevens: (beheersmaatregel)
☐	Godsdienst (beheersmaatregel)
☐	Examenresultaten
☐	Traject voortgang registratie
☐	Studentenbegeleiding rapportage
☐	Aanwezigheidsregistratie
☐	Werkervaring en opleiding
☐	Financiële informatie medewerkers / studenten / relaties

☐	Vertrouwelijkheid hoog. Dit betekent dat er een 2 way authentication, logging e.d. vereist is.
--------------------------	--

E. Te hanteren bewaartermijnen en afspraken

Door de Verwerker te hanteren specifieke bewaartermijn van Persoonsgegevens (of toetsingscriteria om dit vast te stellen) en de afspraken daarover:

F. Opslag Verwerking Persoonsgegevens:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

G. Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.

Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:

Partijnaam	Statutaire vestigingsplaats Subverwerker	Beknpte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt door deze Subverwerker	Plaats/land van opslag en Verwerking Persoonsgegevens

Opmerking: indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt én op welke wijze is gewaarborgd dat de gegevens rechtmatig kunnen worden doorgegeven.

H. Contactgegevens voor inhoudelijke contacten over de verwerking van Persoonsgegevens

Partij ²	Naam	Functie	E-mail adres	Telefoonnummer
Verwerkings-verantwoordelijke	Alex Peeters	Functionaris Gegevensbescherming	avg@leijgraaf.nl	088 017 9700
Verwerker				

I. Versie

Versie nummer	datum (laatste) aanpassing	Omschrijving wijziging(en)
1.0		

Creative commons

Naamsvermelding 3.0 Nederland (CC BY 3.0) originele auteur: Kennisnet



De gebruiker mag:

- Het werk kopiëren, verspreiden, doorgeven en remixen – afgeleide werken maken

Onder de volgende voorwaarde:

- Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

² Partijen vullen hun eigen contactgegevens in.

BIJLAGE 2: Beveiligingsbijlage

De Verwerker is overeenkomstig de AVG en artikel 6 en 7 van de Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Normen informatiebeveiliging

Verwerker is verplicht om aan Onderwijsinstelling aan te tonen of en op welke wijze passende technische en organisatorische maatregelen zijn genomen om te waarborgen en te kunnen aantonen dat de verwerking plaatsvindt in overeenstemming met de AVG en de Model Verwerkersovereenkomst.

Voor het toepassen en aantonen van de technische maatregelen, kan Verwerker gebruik maken van (de meest recente versie van) het in het onderwijs ontwikkelde 'Certificeringsschema informatiebeveiliging en privacy ROSA'

(https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/). Dat schema voorziet in een baseline van (beveiligings-)maatregelen waarmee organisaties dit aantoonbaar kunnen maken.

Verwerker kan ook gebruik maken van andere certificeringsmechanismen en/of (inter)nationaal erkende normen en standaarden voor informatiebeveiliging (zoals bijvoorbeeld maar niet beperkt tot de ISO 27001 en 27002), mits die een gelijkwaardig of hoger niveau van beveiliging bieden en de door Verwerker genomen maatregelen aan de Onderwijsinstelling inzichtelijk worden gemaakt.

Minimale beveiligingsmaatregelen

Verwerker neemt ter beveiliging van de Verwerking van Persoonsgegevens ten minste de volgende maatregelen:

- i. Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
- ii. Verwerker heeft de Persoonsgegevens die worden Verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken;
- iii. Verwerker neemt maatregelen om te waarborgen dat enkel geautoriseerde medewerkers van Onderwijsinstelling en Verwerker toegang hebben tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Hierbij heeft Verwerker procedures vastgesteld en gedeeld met de Onderwijsinstelling voor de identificatie, autorisatie en authenticatie van medewerkers alsmede rondom de registratie, aanmelding en afmelding van de medewerkers;
- iv. Verwerker zorgt dat de toegang tot het product of de dienst beveiligd is door middel van een passend beleid voor wachtwoorden dat aansluit bij de stand van de techniek;
- v. Verwerker heeft procedures voor het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke

- ISO-normering). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren;
- vi. Verwerker heeft maatregelen genomen om de Persoonsgegevens te beschermen tegen verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
 - vii. Verwerker maakt bij de beveiliging van de Verwerking van Persoonsgegevens gebruik van een (inter)nationale beveiligingsnorm;
 - viii. Verwerker heeft maatregelen genomen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

Aantoonbaarheid technische beveiligingsmaatregelen product of dienst

Verwerker verklaart periodiek dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens. Deze verklaring bevat ten minste:

- a. Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid;
- b. Een beschrijving in welke mate aan de hiervoor genoemde minimale beveiligingsmaatregelen wordt voldaan;
- c. Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.

H. Certificaten waarover Verwerker beschikt

(Vermeld uitsluitend certificaten die nog minstens 1 jaar geldig zullen zijn.)

Certificaten	Organisatieonderdeel / dienst waarop certificaat betrekking heeft	Geldigheidsduur certificaat	Verklaring van toepasselijkheid

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: [contactgegevens helpdesk/servicedesk voor beveiligingsincidenten.

Contactgegevens bij inbreuk in verband met Persoonsgegevens

Partij ²	Naam	Functie	E-mail adres	Telefoonnummer
Verwerkings-verantwoordelijke	Alex Peeters	Functionaris Gegevensbescherming	avg@leijgraaf.nl	088 017 9700
Verwerker				

Informereren over Datalekken en/of incidenten met betrekking tot beveiliging

Er is een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat ten minste te volgende punten:

1. De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
2. De wijze waarop informatie wordt gedeeld:
3. Op welke manier (via e-mail, telefoon);
4. Aan wie gericht (contactpersonen en contactgegevens);
5. Met wie kan (bij vervolgacties) contact worden opgenomen.
6. Informatie die in ieder geval over een incident gedeeld moet worden
7. De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
8. De oorzaak van het beveiligingsincident;
9. De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
10. Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
11. De omvang van de groep betrokkenen;
12. Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
13. Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

J. Versie

versie nummer	datum laatste aanpassing

Creative commons

Naamsvermelding 3.0 Nederland (CC BY 3.0) originele auteur: Kennisnet



De gebruiker mag:

- Het werk kopiëren, verspreiden, doorgeven en remixen – afgeleide werken maken

Onder de volgende voorwaarde:

- Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).