CLOUD COMPUTING & PRIVACY

Checklist privacy afspraken

Wanneer een onderwijsinstelling een cloud dienst wil afnemen, zal daarvoor een contract moeten worden gesloten met de cloud leverancier. Van belang is om te weten welke privacy afspraken verplicht en welke wenselijk zijn in het aangaan van een contract met een cloud leverancier. De checklist privacy afspraken is hierbij een handig hulpmiddel.

In het contract staan afspraken over het gebruik van de dienst en de voorwaarden (kosten, service levels, juridische voorwaarden, etc.) waaraan dit gebruik is gebonden.

Het is belangrijk dat in het contract wordt verankerd dat de cloud leverancier persoonsgegevens verwerkt in overeenstemming met bepaalde verplichtingen uit de Wet bescherming persoonsgegevens (Wbp).

Als niet aan deze verplichtingen wordt voldaan, dan loopt de onderwijsinstelling het risico dat zij zelf in strijd handelt met de Wbp. Het is daarom van belang de contracten van leveranciers goed te bestuderen en zo mogelijk te vergelijken.

In deze checklist wordt aangegeven welke privacy afspraken verplicht en welke wenselijk zijn in het aangaan van een contract met een cloud leverancier. Het betreft hier dus contractuele verplichtingen aangaande persoonsgegevens.

Deze checklist is bedoeld om naast een contract van een cloud leverancier te leggen of om contracten van verschillende leveranciers met elkaar te vergelijken.

**De checklist is geen juridisch advies.
Voor een sluitend juridisch advies kan het beste contact worden opgenomen met een in IT-recht gespecialiseerd (advocaten)kantoor.**

CHECK	AFSPRAAK	VERPLICHT/ WENSELIJK	WBP	ALGEMENE TOELICHTING	IN DE PRAKTIJK	VOORBEELDBEPALING dit zijn willekeurige voorbeelden van veel voorkomende bepalingen uit Engelstalige cloud contracten.	TOELICHTING OP VOORBEELDBEPALING
☐	**1. Schriftelijke overeenkomst** De onderwijsinstelling en de cloud leverancier zijn verplicht een schriftelijke overeenkomst te sluiten met betrekking tot de bescherming van persoonsgegevens*.	Verplicht	Art. 14	De Wbp noemt degene die ten behoeve van de verantwoordelijke* gegevens verwerkt een bewerker. Cloud leveranciers zullen in de meeste gevallen als een bewerker* aangemerkt kunnen worden. Art. 14 Wbp stelt eisen aan de vorm en inhoud van de afspraken die de onderwijsinstelling met de bewerker maakt.	Partijen leggen hun afspraken doorgaans vast in het cloud contract of een bijlage bij dit contract. Een afzonderlijke privacy overeenkomst is dus niet nodig. Het cloud contract kan ook langs elektronische weg worden gesloten.	Supplier may make commercially reasonable changes to the URL Terms from time to time. If Supplier makes a material change to the URL Terms, Supplier will inform Customer sending an email to the Notification Email Address.	Soms worden privacy bepalingen opgenomen in URL-terms* of in online privacy policies, die eenzijdig kunnen worden gewijzigd door de cloud leverancier, zonder dat de onderwijsinstelling hiervan op de hoogte wordt gesteld. Risico hiervan is dat de cloud leverancier het contract zodanig aanpast dat de onderwijsinstelling niet langer voldoet aan de Wbp. De onderwijsinstelling moet de overeenkomst daarom kunnen beëindigen als zij het niet eens is met dergelijke wijzigingen. Het contract dient bij voorkeur te verwijzen naar Nederlands recht en de Nederlandse rechter.
☐	**2. Adequaat beveiligen** De cloud leverancier moet de persoonsgegevens adequaat beveiligen. Het gaat hierbij zowel over beveiliging tegen dataverlies als over bescherming van de toegang tot persoonlijke gegevens door onbevoegden.	Verplicht	Art. 13 en 14	De onderwijsinstelling moet zorgdragen dat de cloud leverancier de persoonsgegevens adequaat beveiligt.	De perceptie bestaat dat cloud computing onveilig is. Naast beveiligingsrisico's kent cloud computing echter ook beveiligingsvoordelen. De onderwijsinstelling zal op basis van een risicoanalyse* moeten beoordelen of de leverancier voldoende waarborgen biedt. Daarbij geldt: hoe hoger het risico, hoe hoger het vereiste beveiligingsniveau. Als de onderwijsinstelling bijvoorbeeld verzuimgegevens van leerlingen wil opslaan in de cloud, dan is een hoger beveiligingsniveau vereist dan wanneer het gaat om adresgegevens van medewerkers.	We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of your data.	De meeste cloud leveranciers hebben in hun contract een algemene verplichting opgenomen om de persoonsgegevens adequaat te beveiligen. Een dergelijke bepaling alleen is niet voldoende. De beveiligingsmaatregelen moeten ook worden omschreven (zie hierna sub 3).
☐	**3. Omschrijven beveiligingsmaatregelen** De beveiligingsmaatregelen m.b.t. persoonsgegevens van de leverancier moeten worden omschreven in het cloud contract.	Verplicht	Art. 13 en 14	Bij beveiligingsmaatregelen kan worden gedacht aan firewalls, wachtwoorden, encryptie van gegevens en een omschrijving van beveiligingsbeleid.	Vanuit beveiligings- en concurrentieoogpunt zijn cloud leveranciers vaak terughoudend in het verschaffen van informatie over hun beveiligingsmaatregelen. In de praktijk wordt vaak verwezen naar certificering van de diensten of worden de maatregelen in algemene bewoordingen omschreven. Of dit voldoende is zal afhangen van de risicoanalyse die de onderwijsinstelling moet maken. De onderwijsinstelling mag bijvoorbeeld eerder volstaan met een algemene omschrijving van beveiligingsmaatregelen in het geval van verwerking van adresgegevens van medewerkers, dan wanneer er verzuimgegevens van leerlingen worden verwerkt.	Supplier has implemented at least industry standard systems and procedures to ensure the security and confidentiality of customer data, protect against anticipated threats or hazards to the security or integrity of customer data, and protect against unauthorized access to or use of customer data.	In de voorbeeldbepaling zijn de beveiligingsmaatregelen in algemene bewoordingen omschreven. Afhankelijk van de uitkomst van de risicoanalyse zou dit voldoende kunnen zijn, bijvoorbeeld in geval van verwerking van adresgegevens van medewerkers.

CHECK	AFSPRAAK	VERPLICHT/ WENSELIJK	WBP	ALGEMENE TOELICHTING	IN DE PRAKTIJK	VOORBEELDBEPALING dit zijn willekeurige voorbeelden van veel voorkomende bepalingen uit Engelstalige cloud contracten.	TOELICHTING OP VOORBEELDBEPALING
☐	**4. Controleren beveiliging** De cloud leverancier moet de onderwijsinstelling in staat stellen om erop toe te zien of hij zijn verplichting tot adequate beveiliging nakomt.	Verplicht	Art. 14	De onderwijsinstelling moet controleren of de cloud leverancier zijn beveiligingsverplichtingen nakomt.	Veel cloud leveranciers hebben er bezwaar tegen dat klanten de beveiliging op locatie van leverancier komen controleren (audit). Ook hier wordt vaak verwezen naar certificering of wordt de leverancier verplicht om regelmatig aan de onderwijsinstelling te rapporteren in hoeverre hij aan zijn beveiligingsverplichtingen voldoet. Of dit voldoende is zal ook hier afhangen van de risicoanalyse die de onderwijsinstelling moet maken.	An independent third party auditor issued supplier an unqualified SAS70 Type II certification. Supplier is proud to provide administrators the peace of mind knowing that their data is secure under the SAS70 auditing industry standard. The independent third party auditor verified that supplier has the following controls and protocols in place [...].	Deze voorbeeldbepaling staat niet in het cloud contract, maar in de zogenaamde Frequently Asked Questions. Risico daarvan is dat de cloud leverancier de FAQ zodanig aanpast (zonder de onderwijsinstelling op de hoogte te stellen) dat de onderwijsinstelling niet langer voldoet aan de Wbp. De onderwijsinstelling moet de overeenkomst daarom kunnen beëindigen als zij dit te weten komt en het niet eens is met de wijzigingen van de FAQ.
☐	**5. Verwerken in opdracht** De cloud leverancier mag de persoonsgegevens van de onderwijsinstelling slechts in opdracht van de onderwijsinstelling verwerken.	Verplicht	Art. 12 en 14	De cloud leverancier mag de persoonsgegevens van de onderwijsinstelling alleen verwerken voor zover dat noodzakelijk is om de cloud diensten aan de onderwijsinstelling te leveren. De cloud leverancier mag de persoonsgegevens niet voor eigen doeleinden gebruiken, zoals het rechtstreeks benaderen van studenten voor direct marketingdoeleinden.	In de praktijk zal het niet vaak voorkomen dat een cloud leverancier zich het recht voorbehoudt om persoonsgegevens van gebruikers van de cloud dienst (bijv. studenten) voor eigen doeleinden te gebruiken.	Supplier shall process the personal data on the instructions of Customer and in accordance with the provisions of the Agreement.	Op grond van deze bepaling mag de leverancier persoonsgegevens verwerken voor zover dat is bepaald in de overeenkomst. Het is daarom belangrijk de overeenkomst en eventuele bijlagen te controleren op mogelijk doeleinden voor verwerking.
☐	**6. Geen toegang derden** Zonder toestemming van de onderwijsinstelling mag de cloud leverancier derden geen toegang geven tot de persoonsgegevens.	Verplicht	Art. 8, 9, 12, 13 en 14	De cloud leverancier (en degenen die onder zijn gezag handelen, zoals bijvoorbeeld personeel), is in beginsel verplicht om persoonsgegevens geheim te houden. Er zijn uitzonderingen, bijvoorbeeld rechtmatige inzageverzoeken van bevoegde autoriteiten.	In de meeste cloud contracten is een geheimhoudingsverplichting voor de leverancier opgenomen waarin dit aspect is geregeld.	Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates who need to know it and who have agreed in writing to keep it confidential.	In deze geheimhoudsbepaling is opgenomen dat de cloud leverancier "Confidential Information" (waaronder ook persoonsgegevens worden verstaan) niet aan derden mag verstrekken, tenzij het gaat om groepsmaatschappijen van de cloud leverancier met wie hij een schriftelijke overeenkomst heeft gesloten waarin een geheimhoudingsverplichting is opgenomen. Dit laatste is toegestaan, zie hierna sub 7.

CHECK	AFSPRAAK	VERPLICHT/ WENSELIJK	WBP	ALGEMENE TOELICHTING	IN DE PRAKTIJK	VOORBEELDBEPALING dit zijn willekeurige voorbeelden van veel voorkomende bepalingen uit Engelstalige cloud contracten.	TOELICHTING OP VOORBEELDBEPALING
☐	**7. Groepsmaatschappijen en onderaannemers** De cloud leverancier mag bij het verwerken van de persoonsgegevens alleen groepsmaatschappijen en onderaannemers inschakelen met wie hij een schriftelijke overeenkomst heeft gesloten waarin geheimhoudings- en beveiligingsverplichtingen zijn opgenomen.	Verplicht	Art. 12, 13 en 14	Groepsmaatschappijen en onderaannemers zijn, net als de cloud leverancier, bewerkers in de zin van de Wbp en voor hen gelden in beginsel dezelfde verplichtingen als voor de cloud leverancier.	De meeste cloud leveranciers zullen alleen groepsmaatschappijen en onderaannemers inschakelen die vergelijkbare geheimhoudings- en beveiligingsverplichtingen accepteren. Veel cloud contracten bevatten een bepaling waarin dit aspect is geregeld.	Supplier only shares personal information with other companies or individuals outside of supplier's organisation in the following limited circumstances: [...] We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.	Veel cloud leveranciers maken gebruik van buitenlandse groepsmaatschappijen en onderaannemers. Daarvoor gelden aanvullende regels, zie sub 10.
☐	**8. Persoonsgegevens niet langer bewaren dan noodzakelijk** De cloud leverancier mag de persoonsgegevens niet langer bewaren dan noodzakelijk om de cloud diensten aan de onderwijsinstelling te leveren.	Verplicht	Art. 10	De onderwijsinstelling moet er als verantwoordelijke voor zorgdragen dat de cloud leverancier persoonsgegevens niet langer bewaart dan noodzakelijk.	De cloud leverancier hanteert doorgaans een standaardbewaartermijn als onderdeel van zijn standaarddienstverlening waarin is geregeld dat de gegevens na beëindiging van de overeenkomst worden vernietigd.	We will retain your information for as long as your account is active or as needed to provide you services. If you wish to cancel your account or request that we no longer use your information to provide you services, you may delete your account. We may retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.	Deze bepaling laat de cloud leverancier te veel ruimte om de gegevens na beëindiging te bewaren. Beter zou zijn om een absoluut recht op verwijdering van de data op te nemen in het contract.
☐	**9. Data ook weer uit de cloud** De cloud leverancier moet ervoor zorgen dat de onderwijsinstelling de persoonsgegevens bij het einde van de overeenkomst weer uit de cloud kan halen. De persoonsgegevens moeten daarna worden verwijderd uit de systemen van de leverancier.	Verplicht	Art. 10	Bij het einde van de overeenkomst zal de onderwijsinstelling de persoonsgegevens zelf weer willen beheren of willen onderbrengen bij een andere cloud leverancier.	Veel cloud leveranciers geven hun klanten de mogelijkheid om hun gegevens (na beëindiging van de overeenkomst) uit de cloud te halen. Er zijn verschillende initiatieven in ontwikkeling die dit proces voor klanten proberen te vereenvoudigen. Zie bijvoorbeeld www.dataliberation.org.	Upon termination of the Agreement Supplier will retain the Customer Data for 28 days. After this period Supplier may permanently delete the Customer Data without prior notice. In that event Supplier can no longer provide a copy of the Customer Data to Customer.	Deze bepaling laat ongeregeld of de leverancier medewerking moet verlenen aan de onderwijsinstelling. Het verdient aanbeveling hier nadere afspraken over te maken. Ook is het zinvol om afspraken te maken over het bestandsformaat waarin de onderwijsinstelling de gegevens ontvangt.

CHECK	AFSPRAAK	VERPLICHT/ WENSELIJK	WBP	ALGEMENE TOELICHTING	IN DE PRAKTIJK	VOORBEELDBEPALING dit zijn willekeurige voorbeelden van veel voorkomende bepalingen uit Engelstalige cloud contracten.	TOELICHTING OP VOORBEELDBEPALING
☐	**10. Verwerking alleen binnen Europese Unie of land met 'passend beschermings-niveau'** De cloud leverancier mag de persoonsgegevens alleen verwerken in de Europese Unie of een land met 'passend beschermingsniveau'.	Wenselijk	Art. 76	Alle landen van de Europese Unie hebben een hoog niveau van privacybescherming. Daarnaast heeft de Europese Commissie een aantal landen aangewezen die een passend beschermingsniveau bieden (de zogenaamde 'witte lijst'). Er gelden geen bijzondere regels voor verwerking van persoonsgegevens in deze landen. Is de cloud leverancier (of een van zijn datacenters) in een ander land gevestigd, dan gelden aanvullende, veelal complexe regels.	Lokalisatie of regionalisatie* is een relatief eenvoudige oplossing voor een complex probleem onder de Wbp. Steeds meer leveranciers komen klanten hierin tegemoet, omdat andere oplossingen vaak onvoldoende toereikend zijn.	Supplier and its U.S. subsidiaries are participants in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. These US group companies have certified that they adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. The Safe Harbor certification for Supplier and its U.S. subsidiaries can be viewed on the U.S. Department of Commerce's Safe Harbor Web site.	Amerikaanse cloud leveranciers die Safe Harbor gecertificeerd zijn worden geacht passende waarborgen te bieden (witte lijst). Momenteel is dit echter onderwerp van discussie. Meer informatie zie Internationale regelgeving.
☐	**11. Informeren over beveiligingsincidenten** De cloud leverancier moet de onderwijsinstelling onmiddellijk informeren over beveiligingsincidenten en de mogelijke impact daarvan op de verwerking van persoonsgegevens.	Wenselijk		In geval van een beveiligingsincident (bijv. een datalek) wil de onderwijsinstelling kunnen beoordelen wat de gevolgen daarvan zijn en welke maatregelen kunnen worden getroffen om deze gevolgen te beperken (bijv. informeren van studenten).	Cloud leveranciers zullen hier niet snel mee akkoord gaan, omdat ze niet graag naar buiten treden met beveiligingsincidenten.	Supplier shall promptly notify customer if it detects or reasonably suspects any incident in which the security, confidentiality or integrity of any customer data has been breached.	Het is aan te bevelen om ook afspraken te maken over de inhoud van de waarschuwing. Bijvoorbeeld door de leverancier te verplichten informatie te verschaffen over de omvang van het datalek en welke maatregelen zijn en worden getroffen om de gevolgen van het datalek te beperken.
☐	**12. Verwerking in overeenstemming Wbp** De cloud leverancier moet de persoonsgegevens verwerken in overeenstemming met de Wbp.	Wenselijk		De Nederlandse cloud leverancier is zelfstandig verplicht zich aan de Wbp te houden. Echter, de onderwijsinstelling is vaak (mede-)aansprakelijk voor schendingen van de Wbp door de cloud leverancier. Indien naleving van de Wbp als een contractuele verplichting is opgenomen, kan de onderwijsinstelling het cloud contract makkelijker beëindigen of schadevergoeding vorderen.	Aangezien de Nederlandse cloud leverancier ook zelfstandig verplicht is om zich aan de Wbp te houden, heeft deze hier doorgaans geen bezwaar tegen.	Customer shall be the data controller and Supplier shall be the data processor that processes personal data on behalf of Customer. Customer warrants that it will process its personal data in accordance with the Dutch Act on the Protection of Personal Data.	Hoewel deze bepaling duidelijk maakt dat de cloud leverancier slechts een bewerker is in de zin van de Wbp, verklaart de leverancier niet expliciet dat hij de persoonsgegevens zal verwerken in overeenstemming met de Wbp.

CHECK	AFSPRAAK	VERPLICHT/ WENSELIJK	WBP	ALGEMENE TOELICHTING	IN DE PRAKTIJK	VOORBEELDBEPALING dit zijn willekeurige voorbeelden van veel voorkomende bepalingen uit Engelstalige cloud contracten.	TOELICHTING OP VOORBEELDBEPALING
☐	**13. Verplichtingen in geval van onderzoek autoriteiten** Indien de cloud leverancier door een autoriteit wordt verzocht om persoonsgegevens van de onderwijsinstelling te verstrekken, dan moet hij (i) de onderwijsinstelling onmiddellijk informeren, (ii) de onderwijsinstelling in staat stellen om zijn rechten te verdedigen en (iii) alle medewerking verlenen om de toegang zo beperkt mogelijk te houden.	Wenselijk		Bij cloud computing worden persoonsgegevens niet meer op lokatie van de onderwijsinstelling verwerkt. De onderwijsinstelling zal daarom door de cloud leverancier geïnformeerd moeten worden over eventuele verzoeken van autoriteiten wil de onderwijsinstelling daar adequaat op kunnen reageren.	Cloud leveranciers kunnen hier bezwaar tegen hebben, omdat het extra inspanning van ze vraagt die geen onderdeel is van hun standaard dienstverlening.	Each party may disclose the other party's Confidential Information when required by law, or a binding legal request from a supervisory authority, but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.	Deze bepaling verplicht de cloud leverancier om zich in te spannen de onderwijsinstelling tijdig te informeren over een inzageverzoek van een overheidsinstantie*. Het is de leverancier soms wettelijk verboden om de onderwijsinstelling te informeren. Dat kan bijvoorbeeld het geval zijn bij strafrechtelijke onderzoeken en de US Patriot Act.
☐	**14. Meewerken aan inzageverzoeken** De cloud leverancier moet meewerken aan verzoeken van betrokkenen (bijv. studenten) om inzage en correctie van hun persoonsgegevens.	Wenselijk	Art. 35 en 36 Wbp	De betrokkenen hebben recht op inzage en correctie van hun persoonsgegevens.	Bij sommige typen cloud diensten zal de onderwijsinstelling de medewerking van de cloud leverancier nodig hebben om aan verzoeken om inzage of correctie te voldoen. Gedacht kan worden aan diensten waarbij een onderwijsinstelling zelf geen toegang heeft tot de persoonsgegevens van leerlingen.	Supplier shall promptly assist customer to (i) provide customer or the data subject access to the customer personal data, (ii) remove, block or correct the customer personal data, or (iii) demonstrate that the customer personal data that was incorrect has been removed, blocked or corrected.	De onderwijsinstelling is verplicht om binnen vier weken te reageren op inzageverzoeken. Het is aan te bevelen om deze tijdslijnen ook op te leggen aan de leverancier.

BEGRIPPENLIJST

Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt zonder dat hij onder het gezag van de verantwoordelijke staat.
Inzageverzoek van overheidsinstantie	Bijvoorbeeld een verzoek van politie of justitie om in het kader van een strafrechtelijk onderzoek gegevens, informatie of documenten te verstrekken over cq. van een persoon. Hierbij kan gedacht worden aan het verstrekken van identiteit die behoort bij een bepaald door de instelling verstrekt e-mailadres.
Lokalisatie/ Regionalisatie	Het lokaal (bijvoorbeeld in Nederland) of regionaal (bijvoorbeeld in Europa) opslaan van gegevens.
Persoonsgegevens	Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon (zoals naam, geboortedatum, geslacht). Een persoon is identificeerbaar als de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning kan worden vastgesteld.
Risicoanalyse	Een inventarisatie van de te verwerken persoonsgegevens en een beoordeling van het risico op verlies of onzorgvuldige verwerking van die gegevens en de gevolgen daarvan voor de betrokkene.
URL-terms	(Algemene) voorwaarden die gepubliceerd zijn op een website (URL) waarnaar verwezen wordt in bijvoorbeeld een contract. Omdat de voorwaarden op een website zijn te vinden, kan moeilijk worden nagegaan welke versie van de voorwaarden van toepassing zijn.
Verantwoordelijke	Degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit zal vaak de instelling zijn.

Deze checklist is opgesteld in opdracht van het SURFnet/Kennisnet innovatieprogramma in samenwerking met Project Moore Advocaten.

SURFnet Kennisnet INNOVATIEPROGRAMMA

PROJECT MOORE