Aanvullende FSR Inkoopvoorwaarden voor Cloudservices

VI. AANVULLENDE BEPALINGEN BETREFFENDE CLOUDSERVICES

24. Begripsbepalingen

24.1. Betrokkene: Degene op wie Persoonsgegevens betrekking heeft.
24.2. Clouddienst: De onder de Overeenkomst te leveren dienst waarbij leverancier op afstand en on-demand IT middelen (zoals servers, opslag, applicaties en diensten) aan de instelling beschikbaar stelt en houdt via internet of een ander (openbaar) netwerk.
24.3. Gebruiker: Een op enigerlei wijze aan Summa College verbonden (natuurlijke) persoon, zoals personeel, docenten en/of studenten, die door het Summa College geautoriseerd is tot (een bepaald deel) van de Clouddienst.
24.4. Gegevens: Alle gegevens, data, informatie en enig ander materiaal of content die de instelling en/of Gebruikers in het kader van de Overeenkomst invoeren, versturen, plaatsen of anderszins Verwerken met behulp van de Clouddienst, waaronder mede begrepen Persoonsgegevens.
24.5. Persoonsgegevens: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, die op welke wijze dan ook door leverancier verwerkt wordt of zal worden in het kader van de Overeenkomst.
24.6. Verwerken: Elke handeling of elk 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.

25. Wijzigingen

25.1. Indien een wijziging in de te Verwerken Persoonsgegevens of een risicoanalyse van de verwerking van Persoonsgegevens daartoe aanleiding geeft treden partijen op eerste verzoek van instelling in overleg over het aanpassen van de gemaakte afspraken binnen deze Overeenkomst.
25.2. De nieuw te maken afspraken dienen voorafgaand aan de toepassing daarvan schriftelijk te zijn vastgelegd en deel uit te maken van deze Overeenkomst.
25.3. De wijzigingen kunnen nooit tot gevolg hebben dat de instelling niet kan voldoen aan de Wet bescherming Persoonsgegevens (hierna: Wbp) en overige relevante wet- en regelgeving met betrekking tot Persoonsgegevens.

26. Beschikbaarheid gegevens

26.1. Contractant is verantwoordelijk voor de beschikbaarheid van de Clouddienst aan de instelling overeenkomstig het bepaalde in deze Overeenkomst en indien aanwezig de service level agreement (SLA).
26.2. Contractant zal zorgdragen voor adequate back-up en restore voorzieningen om beschikbaarheid van de Clouddienst (en daarmee van de statische en dynamische Gegevens) te waarborgen.

27. (Intellectuele) eigendomsrechten

27.1. Alle (intellectuele) eigendomsrechten - daaronder begrepen enig auteursrecht en databankenrecht - op (het bestand c.q. de bestanden van) de Gegevens blijven te allen tijde berusten bij instelling, de betreffende Gebruiker, dan wel hun respectievelijke licentiegever(s).
27.2. Contractant heeft geen zelfstandige zeggenschap over de Gegevens die door haar worden verwerkt. De zeggenschap over de Gegevens berust bij instelling en/of de betreffende Gebruiker.

28. Vertrouwelijkheid Cloudservices

28.1. In aanvulling op artikel 8.4 van deze voorwaarden is bij elke schending van zijn geheimhoudingsverplichting partijen een direct opeisbare boete van EUR 25.000 per overtreding verschuldigd, onverlet de overige rechten op schadevergoeding van de andere partij.
28.2. In aanvulling op artikel 8.3 van deze voorwaarden zullen partijen voor hen werkzame personen (waaronder werknemers) die betrokken zijn bij de verwerking van vertrouwelijke Gegevens contractueel verplichten tot geheimhouding van die vertrouwelijke Gegevens.
28.3. Partijen verlenen op verzoek van de andere partij hun medewerking aan het uitoefenen van toezicht door of namens de andere partij op de bewaring en het gebruik van vertrouwelijke Gegevens door de andere partij.
28.4. Ieder der partijen zal de andere partij onmiddellijk informeren nadat zij bekend is geworden met een vermoedelijk(e) of daadwerkelijk(e) (i) schending van de geheimhoudingsplicht; (ii) verlies van vertrouwelijke Gegevens; of (iii) schending van de beveiligingsmaatregelen. De nalatige partij zal op eigen kosten alle benodigde maatregelen nemen om de vertrouwelijke Gegevens veilig te stellen, de tekortkomingen in de beveiligingsmaatregelen te herstellen om verdere kennisneming, wijziging, en verstrekking te voorkomen, onverminderd enig recht van constaterende partij op schadevergoeding of andere maatregelen. De nalatige partij zal op verzoek van de andere partij meewerken aan het informeren van Betrokkenen.

29. Verwerking Persoonsgegevens

29.1. Voor zover Contractant in het kader van de uitvoering van deze Overeenkomst voor een instelling Persoonsgegevens verwerkt, is de instelling aan te merken als verantwoordelijke en Contractant als bewerker in de zin van de Wbp.
29.2. Contractant zal de Persoonsgegevens Verwerken op behoorlijke en zorgvuldige wijze en in overeenstemming met de Wbp en andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens.
29.3. Bij risicoklasse I en hoger wordt een tabel opgesteld waarbij is aangegeven welke (groepen) medewerkers toegang tot de Persoonsgegevens hebben en zij mogen uitsluitend de daarachter vermelde verwerkingen ten aanzien van de Persoonsgegevens uitvoeren. Het is verboden voor de (groep) medewerkers om andere verwerkingen ten aanzien van de Persoonsgegevens uit te voeren dan in de tabel is omschreven.

De volgende typering van de risicoklassen is van toepassing:

Risicoklasse 0 (publiek niveau)	Openbare Persoonsgegevens (bijv. zakelijk emailadres op internet). Voor de verwerking van deze Persoonsgegevens zijn geen specifieke maatregelen noodzakelijk naast de standaardregeling van de Wbp.
Risicoklasse I (Basis niveau)	Beperkt aantal Persoonsgegevens dat betrekking heeft op de relatie tussen Betrokkene en organisatie (bijv. de inschrijving van een student (sec)). Standaard informatiebeveiligingsmaatregelen zijn toereikend.
Risicoklasse II (verhoogd risico)	Hieronder vallen bijzondere Persoonsgegevens en bijvoorbeeld gegevens over de economische situatie van de Betrokkene of een dyslexieverklaring. De informatiebeveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basis niveau.
Risicoklasse III (Hoog risico)	Hieronder vallen bijzondere Persoonsgegevens en bijvoorbeeld rapporten over de psychologische gesteldheid of medische gegevens in het kader van onderzoek. Het risico dat de Betrokkene loopt bij onvoldoende beveiliging is dermate groot dat de informatiebeveiliging moet voldoen aan de hoogste normen.

29.4. Contractant zal de Persoonsgegevens uitsluitend Verwerken in opdracht en volgens de instructies van instelling. Aldus zal Contractant de Persoonsgegevens uitsluitend Verwerken voor de uitvoering van deze Overeenkomst. Contractant mag de Persoonsgegevens niet ten eigen nutte, ten nutte van derden, en/of voor eigen dan wel reclame doeleinden c.q. andere doeleinden Verwerken, behoudens op hem rustende afwijkende dwingendrechtelijke verplichtingen.
29.5. Contractant zal haar volledige medewerking verlenen opdat instelling kan voldoen aan zijn wettelijke verplichtingen in het geval dat een Betrokkene zijn rechten uitoefent op grond van de Wbp of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens.
29.6. Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten onder de Wbp direct contact opneemt met Contractant, dan gaat Contractant hier - behoudens uitdrukkelijke andersluidende instructie van instelling - in eerste instantie niet (inhoudelijk) op in, maar bericht hij dit onverwijld aan instelling met een verzoek om nadere instructies.
29.7. Contractant is verplicht de instelling onmiddellijk te informeren over toekomstige wijzigingen in de uitvoering van de Overeenkomst zodat de instelling kan toezien op de naleving van afspraken met de Contractant. Hieronder wordt mede begrepen de inschakeling van (nieuwe) hulpleveranciers. De procedure van artikel 25 wordt daarbij gevolgd.
29.8. Zonder de toestemming van de instelling verleent Contractant aan derden geen toegang tot de Persoonsgegevens. De instelling zal deze toestemming niet op onredelijke gronden onthouden. Bij het verlenen van toestemming is instelling gerechtigd voorwaarden te verbinden of de toestemming in tijd te beperken. De door instelling gegeven toestemming laat onverlet de verantwoordelijkheid en

Aanvullende FSR Inkoopvoorwaarden voor Cloudservices

aansprakelijkheid van de Contractant voor de nakoming van deze Overeenkomst.

29.9. Aan toestemming van de Opdrachtgever voor de inschakeling van derden bij de dienstverlening zullen in ieder geval de volgende voorwaarden worden verbonden:

29.9.1. De derde is rechtstreeks betrokken bij de levering van diensten onder deze Overeenkomst; en

29.9.2. Contractant heeft een schriftelijke overeenkomst met de betreffende derde waarin in ieder geval is opgenomen dat de betreffende derde eveneens handelt in overeenstemming met alle bepalingen van deze Overeenkomst met betrekking tot de verwerking van Persoonsgegevens.

29.10. Indien Contractant een derde inschakelt voor de verlening van de Clouddienst, ontheft dit Contractant niet van haar verplichtingen met betrekking tot de verwerking van de Persoonsgegevens.

29.11. Contractant vrijwaart Opdrachtgever voor alle aanspraken van derden, daaronder begrepen Betrokkenen, die jegens Opdrachtgever mochten worden ingesteld wegens een aan Contractant of door haar ingeschakelde derde, toe te rekenen schending van de Wbp of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens.

29.12. Indien het College Bescherming Persoonsgegevens in het kader van haar taak als handhaver een maatregel oplegt aan de Opdrachtgever en indien de oorzaak voor het opleggen van de maatregel te wijten is aan het niet nakomen van de in deze Overeenkomst gemaakt afspraken door Contractant, dan kan de Opdrachtgever de kosten voor deze maatregel verhalen op de Contractant. Tevens heeft de Opdrachtgever het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang te beëindigen zonder dat de Contractant aanspraak kan maken op enige vorm van schadevergoeding.

29.13. Contractant zal Persoonsgegevens die haar in het kader van deze Overeenkomst ter beschikking zijn gesteld niet langer bewaren dan noodzakelijk is (i) voor de uitvoering van deze Overeenkomst; of (ii) om een op hem rustende wettelijke verplichting na te komen.

30. Beveiliging

30.1. Contractant treft passende maatregelen om de fysieke en logische beveiliging van de Clouddienst adequaat in te richten tegen verlies of aantasting en tegen enige vorm van onbevoegde kennisneming, wijziging en verstrekking danwel anderszins onrechtmatige verwerking van de Persoonsgegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging daarvan, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen Persoonsgegevens meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van bedoelde Persoonsgegevens te voorkomen. Contractant legt de maatregelen schriftelijk vast en draagt er zorg voor dat de beveiliging zoals bedoeld in dit artikellid voldoet aan de beveiligingseisen op grond van de Wbp.

30.2. De Contractant zal de Opdrachtgever onmiddellijk informeren nadat zij bekend is geworden met een vermoedelijk(e) of daadwerkelijk(e) (i) onbevoegde kennisneming, wijziging of verstrekking van Persoonsgegevens; (ii) verlies van Persoonsgegevens; of (iii) schending van de beveiligingsmaatregelen. Contractant zal op eigen kosten alle benodigde maatregelen nemen om de Persoonsgegevens veilig te stellen, de tekortkomingen in de beveiligingsmaatregelen te herstellen om verdere onbevoegde kennisneming, wijziging, en verstrekking te voorkomen, onverminderd enig recht van de Opdrachtgever op schadevergoeding of andere maatregelen. Contractant zal al dan niet op verzoek van de Opdrachtgever onverwijld de bevoegde autoriteiten en Betrokkenen informeren, althans hier naar keuze van Opdrachtgever haar volledige medewerking aan verlenen.

30.3. Contractant zal Opdrachtgever desgevraagd onverwijld schriftelijk informatie verstrekken met betrekking tot de (organisatie van) de verwerking en beveiliging van Persoonsgegevens.

30.4. Bij risicoklasse I is Contractant verplicht periodiek maar minimaal tweejaarlijks door een door haar aan te wijzen onafhankelijke EDP-auditor of deskundige een onderzoek te laten uitvoeren ten aanzien van de organisatie van Contractant, teneinde te doen vaststellen dat:

30.4.1. Contractant aan het bepaalde met betrekking tot de bescherming van Gegevens (daar mede onder verstaan Persoonsgegevens) in deze Overeenkomst voldoet.

30.4.2. Contractant aan het bepaalde in deze Overeenkomst voldoet, ten aanzien van vertrouwelijkheid, integriteit, continuïteit, effectiviteit en efficiëntie van de door Contractant ter beschikking gestelde Clouddiensten.

30.5. Contractant is verplicht de bevindingen van de EDP-auditor of deskundige, in de vorm van een TPM-verklaring, na een verzoek ter zake aan Insteling ter beschikking te stellen.

30.6. Bij risicoklasse II is Contractant in afwijking van artikel 30.4 verplicht jaarlijks door een door haar aan te wijzen onafhankelijke EDP-auditor of deskundige een onderzoek te laten uitvoeren ten aanzien van de organisatie van Contractant, teneinde te doen vaststellen dat:

30.6.1. Contractant aan het bepaalde met betrekking tot de bescherming van Gegevens (daar mede onder verstaan Persoonsgegevens) in deze Overeenkomst voldoet.

30.6.2. Contractant aan het bepaalde in deze Overeenkomst voldoet, ten aanzien van vertrouwelijkheid, integriteit, continuïteit, effectiviteit en efficiëntie van de door Contractant ter beschikking gestelde Clouddiensten.

30.7. Bij risico klasse III is kan, indien de Opdrachtgever een redelijk vermoeden heeft van het niet-nakomen van bepalingen in deze Overeenkomst, de Opdrachtgever de Contractant verzoeken een kwaliteitstoetsing als bedoeld in artikel 30.4 en 30.6 te laten uitvoeren. De kosten van de kwaliteitstoetsing komen voor rekening van de Opdrachtgever, tenzij uit de bevindingen van de toetsing blijkt dat de Contractant de bepalingen uit de Overeenkomst niet is nagekomen. In dat geval komen de kosten voor rekening van Contractant. Deze bepaling laat de overige rechten van de Opdrachtgever, waaronder die op schadevergoeding, onverlet.

30.8. Bij risicoklasse I verzorgt Contractant maandelijks binnen vijf werkdagen na aanvang van de opvolgende kalendermaand een rapportage over beveiligingsbeheer waarbij minimaal de volgende onderdelen zijn opgenomen:

30.8.1. Aantal, status, voortgang en analyse van incidenten naar aanleiding van artikel 30.2;

30.8.2. Maatregelen genomen op het gebied van beveiligingsbeheer naar aanleiding van incidenten;

30.8.3. Algemene maatregelen genomen op het gebied van gegevensbeveiliging.

31. Doorgifte gegevens

31.1. Contractant garandeert dat iedere verwerking van Persoonsgegevens welke door of namens Contractant of een door hem ingeschakelde derde wordt verricht in verband met het uitvoeren van deze Overeenkomst binnen de Europese Economische Ruimte (EER) plaats zal vinden of naar of vanuit landen die een passend beschermingsniveau waarborgen in overeenstemming met de van zijnde privacyregelgeving, waaronder begrepen naar of vanuit vestigingen van Contractant of door haar ingeschakelde derden die de Veilige Haven Beginselen ("Safe Harbor Principles") hebben onderschreven.
In het geval van risicoklasse I zal Contractant in het laatste geval naar genoegen van de Opdrachtgever bewijs overleggen dat de Veilige Haven Beginselen ook daadwerkelijk worden nageleefd door vestigingen van Contractant of haar ingeschakelde derden. Indien de technische karakteristieken van een transmissiemedium een dergelijke garantie onmogelijk maken, zal de transmissie van Persoonsgegevens uitsluitend versleuteld plaatsvinden waarbij voor de versleuteling geavanceerde (zijnde minstens zo geavanceerd als in de markt gebruikelijk) technieken zullen worden gebruikt. Contractant verschaft op eerste verzoek inzicht in de locatie(s) waarop de Verwerking plaatsvindt.

31.2. Behoudens voorafgaande schriftelijke toestemming van de Opdrachtgever zal de Contractant in het kader van het verlenen van de Clouddienst geen Persoonsgegevens laten overbrengen naar of toegankelijk zal (laten) maken vanuit landen buiten de Europese Economische Ruimte (EER) die geen passend beschermingsniveau waarborgen in de overeenstemming met de van toepassing zijnde privacyregelgeving, waaronder begrepen naar of vanuit locaties van derde partijen die niet de Veilige Haven Beginselen ("Safe Harbour Principles") hebben onderschreven, die de doorgifte van de Persoonsgegevens legitimeert. Bij het vragen van de toestemming zal de Contractant de Opdrachtgever informeren over de landen respectievelijk derde partijen die het hier betreffen. Aan het verstrekken van de toestemming kan de Opdrachtgever nadere voorwaarden verbinden.

31.3. Indien Contractant een verzoek of een bevel van een Nederlandse of buitenlandse toezichthouder of een opsporings-, strafvorderings- of nationale veiligheidsinstantie ontvangt om (inzage in) Persoonsgegevens te verschaffen, waaronder maar niet beperkt tot een verzoek op grond van de USA PATRIOT Act, dan zal Contractant de Opdrachtgever onverwijld informeren. Bij de behandeling van het verzoek of bevel zal de Contractant alle instructies van de

Opdrachtgever in acht nemen (waaronder de instructie om de behandeling van het verzoek of bevel geheel of gedeeltelijk aan de Opdrachtgever over te laten) en alle redelijkerwijs benodigde medewerking verlenen.

31.4. Indien het Contractant op grond van het verzoek of bevel is verboden om te voldoen aan zijn verplichtingen op grond van artikel 31.3, dan zal Contractant de redelijke belangen van de Opdrachtgever behartigen. Contractant zal daartoe in ieder geval:
   a) juridisch laten toetsen in hoeverre (i) Contractant wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Contractant daadwerkelijk is verboden om aan haar verplichtingen jegens Opdrachtgever op grond van artikel 9.3 te voldoen;
   b) alleen aan het verzoek of bevel meewerken indien zij hiertoe wettelijk verplicht is en waar mogelijk (in rechte) bezwaar maken tegen het verzoek of bevel of het verbod om de Opdrachtgever hierover te informeren of haar instructies op te volgen;
   c) niet meer of andere Persoonsgegevens verstrekken dan strikt noodzakelijk om aan het verzoek of bevel te voldoen;
   d) indien sprake is van doorgifte naar een land buiten de EER: de mogelijkheden onderzoeken om te voldoen aan de artikelen 76 en 77 van de Wbp;
   e) de Opdrachtgever onverwijld informeren zodra dit is toegestaan.

31.5. In dit artikel wordt onder "wettelijk" niet alleen Nederlandse maar ook buitenlandse wet- en regelgeving verstaan. In afwijking van artikel 7.1 geldt Contractant als verantwoordelijke als zij zonder inhoudelijke tussenkomst van de Opdrachtgever beslist tot inzage in of verstrekking van Persoonsgegevens aan een toezichthouder of overheidsinstantie.

32. Toegang tot gegevens bij beëindiging

32.1. Bij beëindiging van deze Overeenkomst om welke reden ook, dan wel op eerste verzoek van Opdrachtgever gedurende de looptijd van de Overeenkomst, zal Contractant -tegen beperkte kosten in verhouding tot de voor de Clouddienst verschuldigde vergoeding- ervoor zorgdragen dat naar keuze van Opdrachtgever op werkbare wijze (i) alle of een door Opdrachtgever bepaalde gedeelte haar in het kader van de Clouddienst ter beschikking gestelde Gegevens worden vernietigd op alle locaties, (ii) alle of een door Opdrachtgever bepaalde gedeelte haar in het kader van de Clouddienst ter beschikking gestelde Gegevens aan een opvolgend dienstverlener ter beschikking worden gesteld, dan wel (iii) Opdrachtgever en/of Gebruikers in de gelegenheid worden gesteld om hun Gegevens of een door Opdrachtgever bepaalde gedeelte van de Gegevens aan de Clouddienst te onttrekken. Opdrachtgever kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging.

32.2. Contractant zal te allen tijde de in het vorig lid beschreven dataportabiliteit van de Gegevens waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de Gegevens.