Juridische Normenkader Cloudservices Hoger Onderwijs

Definitieve versie 3 april 2014, aangepast februari 2016.

De geactualiseerde privacy bepalingen uit het normenkader zijn opgenomen in de SURF model bewerkersovereenkomst. De risicoclassificatie is in deze bewerkersovereenkomst tevens geactualiseerd. De verwijzing naar Safe Harbor is naar aanleiding van de uitspraak van het Europese Hof geschrapt.

De privacy bepalingen en de risicoclassificatie zijn in rood weergegeven in dit document, voor de toepassing van deze bepalingen wordt verwezen naar de SURF model bewerkersovereenkomst.

Inhoudsopgave

SURF taskforce Cloud
Vastgesteld door bestuur
Platform ICT & Bedrijfsvoering
3 april 2014

1. Oplegnotitie Normenkader HO

Dit hoofdstuk bevat een oplegnotitie bij het Normenkader voor het hoger onderwijs in Nederland op het gebied van vertrouwelijkheid, privacy, eigendom en beschikbaarheid ten aanzien van clouddiensten. Het Normenkader HO zelf is opgenomen als hoofdstuk 2. Bij het Normenkader hoort een bijlage, opgenomen als hoofdstuk 3, waarin in tabelvorm een toelichting wordt gegeven op de normen.

De indeling van deze Oplegnotitie is als volgt. Ten eerste worden enkele uitgangspunten geformuleerd van waaruit het Normenkader is opgesteld. Hierna zijn een aantal opmerkingen opgenomen met betrekking tot het uitvoeren van het contractmanagement door de instelling. Naast het gebruik van het Normenkader zijn er nog andere maatregelen die een instelling kan nemen om het Normenkader te effectueren. Zo kan er gebruik worden gemaakt van een gedragscode of reglement voor medewerkers en studenten die gebaseerd is op de uitgangspunten respecteren van eigendom, vertrouwelijkheid en privacy. SURFibo (nu SCIPR) heeft voorbeeld gedragscodes ontwikkeld voor medewerkers en studenten. In deze codes is ook rekening gehouden met de bovenstaande aspecten[1]. Ten slotte is een bronnenlijst opgenomen met wet- en regelgeving en relevante stukken die zijn gebruikt bij het opstellen van het Normenkader.

Uitgangspunten

Het Normenkader is gebaseerd op de op het moment van vaststellen van het Normenkader geldende wet- en regelgeving in ruime zin (inclusief richtsnoeren, zienswijze).

Bij het toepassen van het Normenkader is gebruik gemaakt van risicoklassen. De (persoons)gegevens worden ingedeeld in vier risicoklassen. Hoe hoger de risicoklasse, hoe strenger de maatregelen en dus ook de afspraken in een contract met een cloudleverancier voor een zorgvuldige omgang met de (persoons)gegevens dienen te zijn. Een korte typering van de risicoklassen volgt hieronder.[2]

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 1 (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.

[1] Zie http://www.surf.nl/nl/themas/securityenprivacy/informatiebeveiliging/Pages/Leidradeninformatiebeveiliging.aspx

[2] Voor meer informatie over de risicoklassen verwijzen wij u naar de publicatie *Beveiliging van persoonsgegevens* van de Registratiekamer uit 2001.

Contractmanagement

Voorafgaand aan het sluiten van de overeenkomst met de cloudleverancier en gedurende de looptijd van de overeenkomst is het noodzakelijk om een aantal handelingen uit te voeren zodat wordt en blijft voldaan aan relevante wet- en regelgeving. De volgende punten dienen te worden uitgevoerd:

Vóór het sluiten van de overeenkomst

1. Voorafgaand aan het contract dient een risicoanalyse te worden gemaakt van het verwerken van gegevens door een cloudleverancier (bewerker). Het is relevant na te gaan of de instelling zelf voldoende resources heeft om een risicoanalyse zelf uit te voeren of om deze te laten uitvoeren. De volgende vragen dienen hierbij aan de orde te komen:
   - Biedt de bewerker voldoende waarborgen ten aanzien van de technische en organisatorische beveiligingsmaatregelen voor de gegevens in de te verrichten verwerkingen? Hierbij is het relevant de cloudleverancier te vragen naar door de cloudleverancier ingeschakelde derde, de locatie(s) waar de (persoons)gegevens worden opgeslagen en informatie over de informatiebeveiliging. Hieronder wordt mede verstaan een verklaring van een onafhankelijke derde deskundige (TPM-verklaring).
   - Is de Instelling voldoende in staat is om op het gepaste niveau te monitoren en te controleren op de naleving van die beveiligingsmaatregelen? Eventueel kan de instelling hierbij overwegen om dit door een derde partij te laten uitvoeren.

   Voor meer informatie over het uitvoeren van een risicoanalyse willen wij verwijzen naar de richtsnoer 'Beveiliging van persoonsgegevens' van het CBP.[3] Uit de risicoanalyse volgt een risicoklasse. De normen in het Normenkader corresponderen met de risicoklassen.
2. Wanneer er sprake is van een door de cloudleverancier ingeschakelde derde partij (een derde die de cloudleverancier inschakelt bij de dienstverlening), dan dient de instelling hier uitdrukkelijk mee in te stemmen, voorafgaand aan het sluiten van een overeenkomst met de cloudleverancier. Dit kan worden vastgelegd door bijvoorbeeld deze instemming vast te leggen in de besluitvormingsdocumenten rondom het selecteren van een cloudleverancier.
3. Voorafgaand aan het contracteren van de leverancier dient de instelling zich ervan te vergewissen dat de leverancier voldoende beveiligingsmaatregelen heeft genomen ten aanzien van de verwerkingen. Het een en ander is afhankelijk van de risicoklasse van de gegevens die worden verwerkt.
4. In SURFverband zijn technische en organisatorische eisen opgesteld die vanuit beveiligingsoogpunt aan leverancier en diens datahostingspartij gesteld moeten worden. Een checklist hierover is opgenomen op de SURF-website over de Cloud.[4]
5. Naast bepalingen over de bescherming van de privacy worden bij clouddienstverlening vaak ook bepalingen rondom de beschikbaarheid van de dienstverlening vastgelegd. Deze bepalingen staan vaak in een onder de 'hoofdovereenkomst' hangende SLA (Service Level Agreement). Hieronder zijn een aantal voorbeeldbepalingen ten aanzien van de beschikbaarheid opgenomen:

1.1.	**Beschikbaarheid**: de mate waarin een component van de Clouddienst in kwantitatief en kwalitatief opzicht beschikbaar is, te meten met een overeengekomen eenheid in tijd, bandbreedte, aantallen of anderszins als bepaald in het Service Level Agreement, en uitgedrukt door middel van een percentage, gedurende een overeengekomen meetperiode in artikel <artikelnummer>.
1.2.	Het in de SLA aangegeven beschikbaarheidsniveau van de Clouddienst (en daarmee van de Gegevens) zal per kalendermaand worden gemeten op de wijze zoals in Bijlage <kenmerk bijlage> is aangegeven.
1.3.	Onbeschikbaarheid houdt in dat de Clouddienst of een component daarvan niet

[3] CBP Richtsnoeren, *Beveiliging van Persoonsgegevens*, College Bescherming Persoonsgegevens, 19 februari 2013, beschikbaar via: www.cbpweb.nl, pagina 29.
[4] Zie https://www.surf.nl/kennisbank/2013/checklist-cloud-computing-privacy-security-checklist-methoden-en-technieken.html

(volledig) beschikbaar, toegankelijk of bruikbaar is voor het beoogde gebruik.

1.4. De begintijd van de onbeschikbaarheid is (i) het moment dat onbeschikbaarheid wordt geregistreerd in de nader door partijen overeen te komen en in Bijlage <kenmerk bijlage> vast te leggen controlesystemen, dan wel (ii) het moment dat Instelling of Gebruiker melding maakt van onbeschikbaarheid, indien dit eerder was. De eindtijd van de onbeschikbaarheid is, wanneer leverancier en Instelling gezamenlijk vaststellen dat de Clouddienst weer beschikbaar is, dan wel - indien dat moment niet duidelijk is, maar de Clouddienst wel weer (volledig) beschikbaar is - het moment waarop volgens de overeengekomen controlesystemen de Clouddienst weer (volledig) beschikbaar werd.

1.5. Bij de meting van het beschikbaarheidsniveau zal onbeschikbaarheid wegens overeengekomen en op overeengekomen wijze aangekondigd onderhoud buiten beschouwing worden gelaten. Leverancier zal ervoor zorgdragen dat dergelijk onderhoud zo min mogelijk ongemak veroorzaakt. Leverancier zal onderhoud zoveel mogelijk verrichten buiten kantoor- of onderwijstijden (tussen 18:00 en 09:00 en in het weekend) of, indien de gebruiksintensiteit buiten kantoor- of onderwijstijden juist hoog blijkt te zijn, op andere tijdstippen waarop de gebruiksintensiteit meestal relatief laag is gebleken.

1.6. Leverancier zal zorgdragen voor adequate back-up en restore voorzieningen om beschikbaarheid van de Clouddienst (en daarmee van de statische en dynamische Gegevens) te waarborgen.

1.7. Instelling en/of de Gebruikers zijn zelf verantwoordelijk voor hun eigen toegang tot het internet en de apparatuur waarmee zij toegang kunnen krijgen tot de Clouddienst.

1.8. Indien de beschikbaarheid gedurende een bepaalde serviceperiode al dan niet voldoet aan de overeengekomen eisen, dan is een bonus- respectievelijk malusregeling van toepassing zoals opgenomen in de SLA. Leverancier verwerkt de in de SLA gespecificeerde bonus respectievelijk malus in de eerstvolgende factuur/facturen. De in de SLA opgenomen malusregeling laat de overige rechten van Instelling op grond van toerekenbare tekortkoming onverlet, waaronder maar niet beperkt tot het recht op schadevergoeding voor zover de schade het bedrag van de malus te boven gaat.

Gedurende de looptijd van de overeenkomst

De instelling dient ook gedurende de overeenkomst de bescherming van de (persoons)gegevens door de cloudleverancier te controleren. Dat betekent dat de instelling niet alleen vooraf maar ook gedurende de overeenkomst de dienstverlening van de cloudleverancier moet monitoren om er zeker van de zijn dat de gegevens conform de overeenkomst behandeld worden. In het Normenkader zijn hier een aantal bepalingen voor opgenomen (onder andere de artikelen 3, 7.7 en 9 van het Normenkader). Daaruit volgen acties voor de instelling die de instelling dan ook dient uit te voeren. Hieronder worden een aantal van deze acties besproken.

1. Mede afhankelijk van de risicoklasse en de overeengekomen afspraak in de overeenkomst levert de cloudleverancier periodiek een rapportage van een onderzoek van een onafhankelijke derde bij de instelling in (artikel 9 Normenkader). De instelling dient na te gaan of deze rapportages ook periodiek door de cloudleverancier worden ingeleverd. Deze rapportage dient door de instelling gecontroleerd te worden en indien nodig dient de instelling in onderhandeling met de cloudleverancier te treden om gemaakte afspraken te wijzigen (volgens artikel 3).
2. Daarnaast dient de instelling adequaat te reageren op de informatie die de instelling ontvangt van de cloudleverancier ten aanzien van voorgenomen wijzigingen in de dienstverlening en de (rapportages over) beveiligingsincidenten.
3. Naast de informatie die de instelling van de cloudleverancier ontvangt dient de instelling ook zelf na te gaan of de instelling zelf ook haar verplichting nakomt. Hierbij dient ook te worden onderzocht of niet

meer (categorieën) gegevens worden verwerkt bij de cloudleverancier dan in de overeenkomst is afgesproken.

4. De instelling kan een risicoanalyse ten aanzien van de clouddienstverlening uitvoeren. Dit kan naar aanleiding van een wijziging in de dienstverlening zelf, een wijziging in de behoefte van de instelling of een wijziging in van toepassing zijnde wet- en regelgeving. Daarnaast kan een risicoanalyse ook zonder aanleiding, ter controle en evaluatie worden uitgevoerd. Hierbij gaat het om periodiek vaststellen of er nog steeds sprake is van voldoende waarborgen ten aanzien van de technische en organisatorische beveiligingsmaatregelen en of de cloudleverancier nog steeds de verplichtingen nakomt die op de instelling rusten. Vervolgens geeft de instelling gevolg aan de uitkomsten van de risicoanalyse door bijvoorbeeld gemaakt afspraken te wijzigingen.

Bronnen

De volgende bronnen zijn geraadpleegd bij het opstellen van het Normenkader:

- College bescherming persoonsgegevens, CPB richtsnoeren, *Beveiliging van persoonsgegevens*, Den Haag, februari 2013.
- G.W. van Blarkom en drs. J.J. Broking, 'Beveiliging van persoonsgegevens', *Achtergrondstudies en verkenningen 23*, Registratiekamer, Den Haag, april 2001.
- Algemene rijksvoorwaarden bij IT-overeenkomsten (ARBIT), versie 2010, gepubliceerd op 19 juli 2010.
- CBP, *Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing diensten van een Amerikaanse leverancier*, 7 augustus 2012.
- WP29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012.
- Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce on July 21, 2000, < http://export.gov/safeharbor/eu/eg_main_018475.asp >.
- U.S.-EU Safe Harbor Framework Documents: C. Frequently Asked Questions, < http://export.gov/safeharbor/eu/eg_main_018493.asp >.
- Dr. Giles Hogben, Dr. Marnix Dekker, ENISA, *Procure secure: A guide to monitoring of security service levels in cloud contracts*, < http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts >.

2. Normenkader HO

Dit hoofdstuk bevat het Normenkader voor het hoger onderwijs in Nederland op het gebied van vertrouwelijkheid, privacy, eigendom en beschikbaarheid ten aanzien van cloudleveranciers.

De onderstaande normen dienen te worden opgenomen in gelijke of soortgelijke bewoordingen in de overeenkomst tussen de instelling en de cloudleverancier. In dit Normenkader is een verdeling gemaakt in risicoklassen. Deze risicoklassen verwijzen naar de klasse van de door de cloudleverancier te verwerken gegevens. Hoe hoger de risicoklasse, des te meer contractuele waarborgen van toepassing zijn op de te sluiten overeenkomst. Meer informatie over de risicoklassen is beschikbaar in het hoofdstuk Oplegnotitie bij dit Normenkader. Indien er sprake is van een breed scala aan persoonsgegevens die in verschillende risicoklassen worden ingedeeld en die tegelijkertijd door de cloudleverancier worden verwerkt, zal altijd moeten worden uitgegaan van de hoogste van toepassing zijnde risicoklasse die op die verwerking van toepassing is.

Een toelichting van de normen is beschikbaar in het hoofdstuk Bijlage Normenkader HO.

In dit document wordt onder Wbp verstaan: Wet bescherming persoonsgegevens.
Daar waar in het Normenkader tekst is weergegeven tussen haakjes < > dient afhankelijk van de toepassing in de concrete situatie tekst worden ingevuld of weggelaten.

ARTIKEL 1 DEFINITIES

1.1. **Betrokkene** is degene op wie Persoonsgegevens betrekking heeft.
1.2. **Clouddienst** is 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.
1.3. **Gegevens** zijn 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.
1.4. **Gebruiker** is een op enigerlei wijze aan instelling verbonden (natuurlijke) persoon, zoals personeel, docenten en/of studenten, die door de instelling geautoriseerd is tot (een bepaald deel) van de Clouddienst.
1.5. **Overeenkomst** is de onderhavige Overeenkomst die ziet op verlening van Clouddiensten en op grond waarvan leverancier ten behoeve van instelling Gegevens verwerkt.
1.6. **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.
1.7. **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.

ARTIKEL 2 DIENSTVERLENING

2.1. De leverancier verleent uitsluitend de volgende diensten aan de instelling: <omschrijving van de dienstverlening>
2.2. Voor de uitvoering van de in het voorgaande lid omschreven dienstverlening kunnen uitsluitend de volgende Persoonsgegevens worden verwerkt: <differentiatie van categorieën de Gegevens>

ARTIKEL 3 WIJZIGING

3.1. 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.
3.2. De nieuw te maken afspraken dienen voorafgaand aan de toepassing daarvan schriftelijk te zijn vastgelegd en deel uit te maken van deze Overeenkomst.
3.3. De wijzigingen kunnen nooit tot gevolg hebben dat de instelling niet kan voldoen aan de Wbp en overige relevante wet- en regelgeving met betrekking tot Persoonsgegevens.

ARTIKEL 4 BESCHIKBAARHED VAN DE GEGEVENS

4.1. Leverancier is verantwoordelijk voor de beschikbaarheid van de Clouddienst aan de instelling overeenkomstig het bepaalde in deze Overeenkomst <en de service level agreement (SLA) welke daarvan onderdeel uitmaakt>.
4.2. Leverancier zal zorgdragen voor adequate back-up en restore voorzieningen om beschikbaarheid van de Clouddienst (en daarmee van de statische en dynamische Gegevens) te waarborgen.

ARTIKEL 5 (INTELLECTUELE) EIGENDOMSRECHTEN EN ZEGGENSCHAP

5.1. 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).
5.2. Leverancier 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.

ARTIKEL 6 VERTROUWELIJKHEID

6.1. Partijen zullen alle Gegevens waarvan zij het vertrouwelijk karakter kennen of redelijkerwijs kunnen vermoeden en die hen in het kader van de uitvoering van deze Overeenkomst ter kennis of beschikking komen, geheimhouden en op geen enkele wijze verder intern of extern bekendmaken en/of aan derden verstrekken, behalve voor zover:
   a) bekendmaking en/of verstrekking van die Gegevens in het kader van de uitvoering van deze Overeenkomst noodzakelijk is;
   b) enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak partijen tot bekendmaking en/of verstrekking van die Gegevens of informatie verplicht, waarbij partijen eerst de andere partij hiervan op de hoogte stellen;
   c) bekendmaking en/of verstrekking van die Gegevens geschiedt met voorafgaande schriftelijke toestemming van de andere partij; dan wel
   d) het informatie betreft die al rechtmatig openbaar was op een andere wijze dan door het handelen of nalaten van een der partijen.
6.2. Bij elke schending van zijn geheimhoudingsverplichting zijn partijen een direct opeisbare boete van EUR 25.000 per overtreding verschuldigd, onverlet de overige rechten op schadevergoeding van de andere partij.
6.3. Partijen zullen voor hen werkzame personen (waaronder werknemers) die betrokken zijn bij de verwerking van vertrouwelijke Gegevens contractueel verplichten tot geheimhouding van die vertrouwelijke Gegevens.
6.4. 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.

6.5. Partijen stellen alle Gegevens die zij in het kader van de uitvoering van de Overeenkomst onder zich hebben, inclusief eventueel daarvan gemaakte kopieën, op eerste verzoek aan de andere partij ter beschikking.

6.6. 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.

ARTIKEL 7 PERSOONSGEGEVENS

7.1. Voor zover leverancier in het kader van de uitvoering van deze Overeenkomst voor een instelling Persoonsgegevens verwerkt, is de instelling aan te merken als verantwoordelijke en leverancier als bewerker in de zin van de Wet bescherming persoonsgegevens (hierna: Wbp).

7.2. Leverancier zal de Persoonsgegevens verwerken op behoorlijke en zorgvuldige wijze en in overeenstemming met de Wbp en andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens.

Toevoegen vanaf risicoklasse 1

7.3. Volgens de onderstaande tabel hebben de volgende (groepen) medewerkers toegang tot de Persoonsgegevens en mogen zij uitsluitende 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.

	(groep) medewerkers	**Verwerking**

7.4. Leverancier zal de Persoonsgegevens uitsluitend verwerken in opdracht en volgens de instructies van instelling. Aldus zal leverancier de Persoonsgegevens uitsluitend verwerken voor de uitvoering van deze Overeenkomst. Leverancier 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.

7.5. Leverancier 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.

7.6. Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten onder de Wbp direct contact opneemt met leverancier, dan gaat leverancier 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.

7.7. Leverancier 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 leverancier. Hieronder wordt mede begrepen de inschakeling van (nieuwe) hulpleveranciers. De procedure van artikel 3 wordt daarbij gevolgd.

7.8. Zonder de toestemming van de instelling verleent leverancier 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 aansprakelijkheid van de leverancier voor de nakoming van deze Overeenkomst.

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

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

7.9.2. Leverancier 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.

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

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

7.12. Indien het College bescherming Persoonsgegevens in het kader van haar taak als handhaver een maatregel oplegt aan de instelling 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 leverancier, dan kan de instelling de kosten voor deze maatregel verhalen op de leverancier. Tevens heeft de instelling het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang te beëindigen zonder dat de leverancier aanspraak kan maken op enige vorm van schadevergoeding.

7.13. Leverancier 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.

ARTIKEL 8 BEVEILIGING

8.1. Leverancier 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. Leverancier 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.

8.2. De leverancier zal de instelling 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. Leverancier 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 instelling op schadevergoeding of andere maatregelen. Leverancier zal op verzoek van de instelling meewerken aan het informeren van de bevoegde autoriteiten en betrokkene.

8.3. Leverancier zal instelling desgevraagd onverwijld schriftelijk informatie verstrekken met betrekking tot de (organisatie van) de verwerking en beveiliging van Persoonsgegevens.

Toevoegen vanaf risicoklasse 1
8.4. Leverancier is 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 leverancier, teneinde te doen vaststellen dat:
8.4.1. leverancier aan het bepaalde met betrekking tot de bescherming van Gegevens (daar mede onder verstaan Persoonsgegevens) in deze Overeenkomst voldoet.
8.4.2. leverancier aan het bepaalde in deze Overeenkomst voldoet, ten aanzien van vertrouwelijkheid, integriteit, continuïteit, effectiviteit en efficiëntie van de door leverancier ter beschikking gestelde Clouddiensten.
8.5. Leverancier 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.

Toevoegen vanaf risicoklasse 2 (ter vervanging van artikel 8.4)
8.6. Leverancier is 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 leverancier, teneinde te doen vaststellen dat:
8.6.1. leverancier aan het bepaalde met betrekking tot de bescherming van Gegevens (daar mede onder verstaan Persoonsgegevens) in deze Overeenkomst voldoet.
8.6.2. leverancier aan het bepaalde in deze Overeenkomst voldoet, ten aanzien van vertrouwelijkheid, integriteit, continuïteit, effectiviteit en efficiëntie van de door leverancier ter beschikking gestelde Clouddiensten.

Toevoegen vanaf risicoklasse 3
8.7. Indien de instelling een redelijk vermoeden heeft van het niet-nakomen van bepalingen in deze Overeenkomst, dan kan de instelling de leverancier verzoeken een kwaliteitstoetsing als bedoeld in artikel <8.4> te laten uitvoeren. De kosten van de kwaliteitstoetsing komen voor rekening van de instelling, tenzij uit de bevindingen van de toetsing blijkt dat de leverancier de bepalingen uit de Overeenkomst niet is nagekomen. In dat geval komen de kosten voor rekening van leverancier. Deze bepaling laat de overige rechten van de instelling, waaronder die op schadevergoeding, onverlet.

Toevoegen vanaf risicoklasse 1
8.8. Leverancier verzorgt maandelijks binnen vijf werkdagen na aanvang van de opvolgende kalendermaand een rapportage over beveiligingsbeheer waarbij minimaal de volgende onderdelen zijn opgenomen:
8.8.1. Aantal, status, voortgang en analyse van incidenten naar aanleiding van artikel 8.2;
8.8.2. Maatregelen genomen op het gebied van beveiligingsbeheer naar aanleiding van incidenten;
8.8.3. Algemene maatregelen genomen op het gebied van gegevensbeveiliging.

ARTIKEL 9 DOORGIFTE VAN GEGEVENS

9.1. Leverancier garandeert dat iedere verwerking van Persoonsgegevens welke door of namens leverancier 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 toepassing

zijnde privacyregelgeving.

Toevoegen vanaf risicoklasse 1 aan artikel 9.1
In het laatste geval zal leverancier naar genoegen van de instelling bewijs overleggen dat de Veilige Haven Beginselen ook daadwerkelijk worden nageleefd door vestigingen van leverancier 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. Leverancier verschaft op eerste verzoek inzicht in de locatie(s) waarop de Verwerking plaatsvindt.

9.2. Behoudens voorafgaande schriftelijke toestemming van de instelling zal de leverancier 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, die de doorgifte van de Persoonsgegevens legitimeert. Bij het vragen van de toestemming zal de leverancier de instelling informeren over de landen respectievelijk derde partijen die het hier betreffen. Aan het verstrekken van de toestemming kan de instelling nadere voorwaarden verbinden.

9.3. Indien leverancier 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 leverancier de Instelling onverwijld informeren. Bij de behandeling van het verzoek of bevel zal de leverancier alle instructies van de Instelling in acht nemen (waaronder de instructie om de behandeling van het verzoek of bevel geheel of gedeeltelijk aan de Instelling over te laten) en alle redelijkerwijs benodigde medewerking verlenen.

9.4. Indien het leverancier op grond van het verzoek of bevel is verboden om te voldoen aan zijn verplichtingen op grond van artikel 9.3, dan zal leverancier de redelijke belangen van de Instelling behartigen. Leverancier zal daartoe in ieder geval:

a) juridisch laten toetsen in hoeverre (i) leverancier wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het leverancier daadwerkelijk is verboden om aan haar verplichtingen jegens Instelling 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 Instelling 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 Instelling onverwijld informeren zodra dit is toegestaan.

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

ARTIKEL 10 TOEGANG TOT GEGEVENS BIJ BEEINDIGING

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

10.2. Leverancier 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.

3. Toelichting bij Normenkader HO

De onderstaande tabel (versie 2013) betreft een nadere uitwerking en toelichting op het Normenkader HO.
De van toepassing zijnde risicoklasse is zichtbaar in het normenkader.
Onder WBP wordt verstaan: Wet bescherming persoonsgegevens.

Artikel	Norm	Van toepassing zijnde regelgeving	Toelichting	Praktijk
Alg.	Alle afspraken over de beveiligingsmaatregelen die de bewerker moet treffen en wijze waarop de verantwoordelijke toeziet op de naleving van deze afspraken zijn vastgelegd in een schriftelijke overeenkomst, of in een daaraan gelijkwaardige vorm.	• Artikel 14 lid 5 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 32.	De Wbp stelt eisen aan de vorm van de afspraken die een onderwijsinstelling met een cloudleverancier maakt. Dit houdt in dat afspraken schriftelijk of in een vergelijkbare vorm worden vastgelegd.	Partijen leggen hun afspraken met betrekking tot informatiebeveiliging vast in een overeenkomst of in een bijlage bij deze overeenkomst. Deze overeenkomst kan via de elektronisch weg worden gesloten. Dit geldt ook voor wijzigingen van de gemaakte afspraken.
1	Er wordt gebruik gemaakt van definities en begrippen die aansluiten bij de bepalingen uit de Wbp.	Artikel 1 Wbp.	Door aan te sluiten bij definities die worden gebruikt in de Wbp kan er geen misverstand ontstaan over de toepassing van de Wbp en overige relevante wet- en regelgeving. Dit is met name relevant voor de begrippen persoonsgegeven, verwerken, verantwoordelijke en bewerker. Tevens sluiten dan de aan de in de wet gedefinieerde begrippen verbonden interpretaties aan bij de in de overeenkomst gedefinieerde begrippen.	Partijen kunnen in de overeenkomst de uitleg van gebruikte begrippen aan vastleggen.
2.1	Omschrijving van de dienst(en) die de cloudleverancier verleent en de persoonsgegevens die zij daarbij verwerkt.	CBP Richtsnoer beveiliging van persoonsgegevens pag. 33.	Door de diensten van de cloudleverancier te beschrijven, wordt de reikwijdte van de overeenkomst duidelijk. Wanneer de cloudleverancier andere werkzaamheden uitvoert dan is afgesproken, dan komt de cloudleverancier de verplichtingen niet na en kan de instelling de cloudleverancier hierop aanspreken.	Het verdient aanbeveling aan te sluiten bij het begrip ‘verwerken’ zoals in artikel 1 van het normenkader is bepaald. Bijvoorbeeld: Opslag van de door de Instelling aangewezen gegevens. Deze bepaling wordt vaak in hoofddeel van de overeenkomst opgenomen (dat artikel heeft doorgaans de titel ‘Voorwerp van de Overeenkomst’).
2.2	Omschrijving van de soorten persoonsgegevens die in het kader van de overeenkomst door de cloudleverancier	• CBP Richtsnoer beveiliging van persoonsgegevens pag. 33;	Door de in het kader van deze overeenkomst te verwerken persoonsgegevens te categoriseren, is gedurende de looptijd van de	Bij het differentiëren van de persoonsgegevens kan worden aangesloten bij de categorisering die het CBP

	wordt verwerkt.	• NEN-ISO/IEC 27002:2007 nl, paragraaf 7.2.	overeenkomst voor de instelling duidelijk welke soorten persoonsgegevens in de dienstverlening van de cloudleverancier zijn betrokken. Dat is gemakkelijk bij een controle op uitvoering van de overeenkomst en bij eventuele aanpassing van van toepassing zijnde wet- en regelgeving of wijzigingen gedurende de looptijd van de overeenkomst.	aanhoudt (bijzondere persoonsgegevens als bedoeld in artikel 16 Wbp, gegevens over de financiële of economische situatie van de betrokkene/instelling, (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van betrokkene, gegevens die betrekking hebben op mensen uit kwetsbare groepen, gebruikersnamen, wachtwoorden en andere inloggegevens, gegevens die kunnen worden misbruikt voor (identiteits)fraude), of een andere categorisering. Het hanteren van risicoklassen raden we af omdat cloudleveranciers hier misschien niet bekend mee zijn.
3.1	Dit artikel geeft de mogelijkheid om een wijziging in de bepalingen van de overeenkomst te initiëren door de instelling.		Gedurende de looptijd van de overeenkomst kan door gewijzigde wet- en regelgeving of gewijzigde behoefte van de instelling aanleiding zijn voor het aanpassen van de bepalingen in de overeenkomst. Dit met het oog op de controle die de instelling als verantwoordelijke op de verwerking van persoonsgegevens dient te houden.	De instelling in de rol als verantwoordelijke kan gedurende de looptijd van de overeenkomst de verwerking door de cloudleverancier periodiek te evalueren in de vorm van een risicoanalyse zoals genoemd in het normenkader. Afhankelijk van de uitkomst dienen de bepalingen uit de overeenkomst hierop worden aangepast. Een wijziging kan het gevolg zijn van een wijziging in de categorieënindeling van artikel 2.2
3.2	Alle afspraken over de beveiligingsmaatregelen die de bewerker moet treffen en wijze waarop de verantwoordelijke toeziet op	• Artikel 14 lid 5 Wbp; • CBP Richtsnoer beveiliging van persoonsgegeven	De Wbp stelt eisen aan de vorm van de afspraken die een onderwijsinstelling met een cloudleverancier maakt. Dit houdt in dat afspraken schriftelijk of in een vergelijkbare vorm worden	Partijen leggen hun afspraken met betrekking tot informatiebeveiliging vast in een overeenkomst of in een bijlage bij deze

	de naleving van deze afspraken zijn vastgelegd in een schriftelijke overeenkomst, of in een daaraan gelijkwaardige vorm.	s pag. 32.	vastgelegd. Een wijziging in de afspraken tussen instelling en cloudleverancier dienen voor de toepassing van de wijziging schriftelijk te zijn vastgelegd.	overeenkomst. Deze overeenkomst kan via de elektronisch weg worden gesloten. Dit geldt ook voor wijzigingen van de gemaakte afspraken. Zie ook Alg.
3.3	De cloudleverancier moet de persoonsgegevens verwerken in overeenstemming met de Wbp.	Artikel 14 lid 3 Wbp.	De instelling is verplicht zich aan de Wbp te houden. Echter, de instelling is vaak (mede-) aansprakelijk voor schendingen van de Wbp door de cloudleverancier. Indien naleving van de Wbp door de cloudleverancier als een contractuele verplichting is opgenomen, ook ten aanzien van wijzigingen, kan de instelling de overeenkomst makkelijker beëindigen of schadevergoeding vorderen in het geval van een schending van de Wbp.	
4.1	De dienstverlening vindt plaats overeenkomstig de vastgelegde afspraken.		Met deze bepaling stemt de cloudleverancier uitdrukkelijk (expliciet) in met de bepalingen in de overeenkomst. Wanneer de instelling constateert dat de dienstverlening niet aan de bepalingen voldoet, geeft dit artikel een extra mogelijkheid (naast de al niet nagekomen bepaling) om de cloudleverancier in juridische zin aan te spreken.	Met verwijzing naar onder andere deze bepaling kan een ingebrekestelling worden opgesteld in het geval de cloudleverancier de bepalingen niet nakomt. De tussen haakjes gezette tekst kan worden weggelaten indien er geen sprake is van een SLA (Service Level Agreement).
4.2	De gegevens dienen voor het geval de dienstverlening om welke reden dan ook niet beschikbaar is te zijn opgeslagen en vervolgens weer opgestart kunnen worden.	CBP Richtsnoer beveiliging van persoonsgegevens pag. 33.	De cloudleverancier is verplicht de gegevens of een kopie van de gegevens te bewaren voor het geval de dienstverlening uitvalt (om welke reden dan ook). Ook is de cloudleverancier verplicht een recente back-up te kunnen gebruiken om de dienstverlening na de uitval weer te kunnen opstarten (restore-en). De gegevens blijven hierdoor beschikbaar voor de instelling.	De cloudleverancier bewaart een kopie van de gegevens apart van de dienstverlening. De back-up en de restore voorzieningen dienen adequaat te zijn. Dit houdt in dat de gegevens in de back-up actueel (of zoveel als mogelijk) dienen te zijn. Zo vindt geen of zo weinig mogelijk gegevensverlies plaats.
5.1	Het intellectuele eigendom van de gegevens worden beschermd.		Het intellectuele eigendom op de gegevens (uitdrukkelijk alle gegevens en niet slechts persoonsgegevens) gaat nooit over naar de cloudleverancier, maar blijft in handen van de instelling, gebruiker of de licentiegevers van de gebruiker of de instelling. Met deze bepaling is	Het intellectuele eigendom van gegevens, bijvoorbeeld van papers van studenten, behoort toe aan de student en/of instelling. Dit kan nooit overgaan op de cloudleverancier.

			vastgelegd dat de cloudleverancier de intellectuele eigendomsrechten dient te respecteren.	
5.2	De cloudleverancier heeft geen zeggenschap over de gegevens		Door de zeggenschap over de gegevens (uitdrukkelijk alle gegevens en niet slechts persoonsgegevens) vast te leggen bij de gebruiker en/of de instelling is expliciet vastgelegd dat de gegevens alleen worden verwerkt voor zover de gebruiker/instelling daar opdracht toe geeft.	De gegevens die worden verwerkt blijven onder de zeggenschap van de instelling en/of gebruiker. In het Nederlands recht is de term eigendom en daarmee eigenaarschap verbonden met fysieke zaken. Nu van fysieke zaken bij clouddienstverlening geen sprake is, hebben we hier niet voor de term eigenaarschap gekozen, maar voor termen die met betrekking tot gegevens gezamenlijk dezelfde lading dekken: (intellectuele) eigendomsrechten en zeggenschap.
6.1	Vertrouwelijke gegevens dienen vertrouwelijk behandeld te worden door de cloudleverancier. Hiervoor geldt een interne en externe geheimhoudingsplicht voor de cloudleverancier.		Daar waar het persoonsgegevens betreft dient te worden voldaan aan de wbp. Persoonsgegevens kunnen worden onderscheiden van vertrouwelijke gegevens (soms kunnen persoonsgegevens tegelijkertijd ook vertrouwelijke gegevens zijn). Met toepassing van dit artikel worden gegevens die als vertrouwelijk worden bestempeld door de instelling of door de gebruiker als zodanig te worden behandeld. Ook gegevens waarvan de cloudleverancier redelijkerwijs kan vermoeden dat het vertrouwelijke gegevens betreft, dienen als zodanig te worden behandeld. De vertrouwelijkheid van gegevens heeft tot gevolgd dat de cloudleverancier deze gegevens geheim dient te houden en niet mag verspreiden/bekendmaken (zowel intern als extern).	De instelling of gebruiker kan expliciet aangeven dat gegevens vertrouwelijk zijn. Op dat moment vallen de gegevens onder de regeling van dit artikel. Wanneer de vertrouwelijkheid niet expliciet is aangegeven, maar daar de cloudleverancier wel kan vermoeden dat het vertrouwelijke gegevens betreft dienen de gegevens ook als vertrouwelijk behandeld te worden. In de praktijk is het aan te bevelen de vertrouwelijkheid van gegevens expliciet aan te geven, zodat daaromtrent geen discussie kan ontstaan. Een oordeel van vertrouwelijkheid ligt in dat geval bij de instelling en/of gebruiker zelf. Daar waar het gaat om gegevens waarvan redelijkerwijs

				vermoed kan worden dat de gegevens vertrouwelijk zijn, is dat uiteindelijk ter beoordeling van de rechter. Voor de cloudleverancier betekent de geheimhoudingsplicht dat de vertrouwelijke gegevens niet door de cloudleverancier verder worden verspreid dan nodig voor de uitvoering van de dienstverlening. Deze gegevens mogen niet intern of extern bekend worden gemaakt of verder worden verspreidt.
6.1.a	Bekendmaking van vertrouwelijke gegevens mag alleen indien dat noodzakelijk is voor de uitvoering van de overeenkomst.		Het kan voorkomen dat bekendmaken of verstrekking van vertrouwelijke gegevens noodzakelijk is voor de uitvoering van de dienstverlening en/of de overeenkomst. In dat geval en tot zover is bekendmaking en verspreiding van vertrouwelijke gegevens toegestaan.	Hierbij kan gedacht worden aan bankgegevens die de cloudleverancier nodig heeft voor het incasseren van de vergoeding die voor de dienstverlening moet worden betaald.
6.1.b	Dwingendrechtelijke wet- en regelgeving en gerechtelijke uitspraak kan de vertrouwelijkheid van gegevens 'verbreken'.		De vertrouwelijkheid van gegevens mag niet in de weg staan aan het voldoen van de cloudleverancier aan dwingendrechtelijke wet- en regelgeving. Ook hier geldt weer dat bekendmaking en verstrekking van de vertrouwelijk gegevens tot zo ver is toegestaan dat de cloudleverancier voldoet aan de dwingendrechtelijke wet- en regeling.	Een voorbeeld van dwingendrechtelijke wet- en regelgeving kan zijn gerechtelijke uitspraak in het kader van strafvordering.
6.1.c	Vertrouwelijke gegevens mogen alleen wanneer de instelling daar toestemming voor geeft bekend worden gemaakt.		Alleen met schriftelijke toestemming mogen vertrouwelijke gegevens worden bekendgemaakt/ verstrekt. Ook hier geldt weer dat de bekendmaking en de verspreiding alleen mag conform de schriftelijke toestemming en niet verder dan waarvoor de toestemming gegevens is.	
6.1.d	Daar het vertrouwelijke gegevens betreft die al bekend zijn gemaakt of zijn verspreidt is de geheimhouding niet van toepassing.		Wanneer vertrouwelijke gegevens al openbaar zijn (door toedoen of nalaten van de instelling) is de geheimhouding niet meer van toepassing.	Wanneer de instelling zelf vertrouwelijke gegevens openbaar bekend maakt, dan vervalt de geheimhoudingsverplichting ten aanzien van de openbaar bekend gemaakte

				gegevens.
6.2	Wanneer de geheimhoudingverplichting wordt geschonden is een directe boete opeisbaar voor de instelling.		Op het schenden van de geheimhoudingsplicht staat een direct opeisbare boete, daar schending van de geheimhoudingsplicht niet meer kan worden teruggedraaid. Bij de hoogte van de boete is ook gekeken naar de ARBIT-voorwaarden. Deze is niet overgenomen. Er is besloten een lager bedrag van €25.000,-- per overtreding te hanteren.	Wanneer de cloudleverancier de geheimhoudingsplicht schendt is een direct opeisbare boete op zijn plaats. Een schending van de geheimhoudingsplicht kan vaak niet worden teruggedraaid. Er is dan al direct sprake van schade.
6.3	Werknemers van de cloudleverancier dienen een geheimhoudingsverklaring te ondertekenen ten aanzien van vertrouwelijke gegevens.		Niet alleen de cloudleverancier maar ook de voor haar werkzame personen dienen een geheimhoudingsverklaring te ondertekenen om aan dit artikel te kunnen voldoen. Dit om de geheimhoudingsplicht verder te effectueren en de aansprakelijkheid ten aanzien van het schenden van de geheimhoudingsverplichting vast te leggen.	Dit dient voorafgaand aan het starten van de dienstverlening gecontroleerd te worden. Dat kan door de betreffende contractuele verplichting op te vragen bij de cloudleverancier. Zie ook 6.4.
6.4	De instelling heeft de mogelijkheid om de uitvoering van de bepalingen ten aanzien vertrouwelijkheid bij de cloudleverancier te controleren		Ter zekerstelling van een juiste uitvoering van de geheimhoudingverplichting door de cloudleverancier is de cloudleverancier verplicht medewerking te verlenen aan het toezicht dat de instelling hierop uit kan voeren. De cloudleverancier is op grond van deze bepaling verplicht mee te werken aan het toezicht op de naleving van deze geheimhoudingsverplichting.	De instelling heeft toezicht op de naleving van de geheimhoudingsverplichting uitvoeren door bijvoorbeeld geheimhoudingsverklaring met medewerkers van de cloudleverancier op te vragen of in procedures die betrekking hebben op de uitvoering van de geheimhoudingsverplichting in te zien.
6.5	De instelling heeft het recht vertrouwelijke gegevens op te vragen bij de cloudleverancier.		De instelling kan (vertrouwelijke) gegevens op verzoek opvragen. Ook eventuele kopieën van de gegevens zodat vertrouwelijke gegevens niet meer worden verwerkt bij de cloudleverancier. Op deze wijze kan de instelling de verwerking van de (vertrouwelijk) gegevens controleren en beheersen. Zie ook artikel 5.	
6.6	Informatieplicht ten aanzien van beveiligingsincidenten betreffende de geheimhoudingsplicht.		Voor de cloudleverancier geldt een onmiddellijk informatieplicht ter zake van beveiligingsincidenten betreffende vertrouwelijke gegevens. Het gaat hierbij om vermoedelijke en daadwerkelijk incident zodat de geheimhoudingsplicht zoveel als mogelijk kan worden gewaarborgd. Onder incidenten vallen onbevoegde	

			kennisneming, verlies of schending van beveiligingsmaatregelen. Naast de informatieplicht is de cloudleverancier verplicht om te reageren op de incidenten door de vertrouwelijke gegevens veilig te stellen, maatregelen nemen om het incident te beëindigen en/of te voorkomen en meewerken aan verder afhandeling van een incident.	
7.1	De instelling is de verantwoordelijke en de cloudleverancier de bewerker.	Artikel 1 Wbp.	In het kader van de overeenkomst wordt expliciet bepaald dat, voor zover de leverancier Persoonsgegevens verwerkt, de instelling de verantwoordelijke is en de cloudleverancier de bewerker in de zin van de Wbp. Door dit expliciet te benoemen is duidelijk welke rechten en plichten van de Wbp van toepassing zijn op de instelling en de cloudleverancier.	Zie ook de definities in artikel 1 voor verantwoordelijke en bewerker.
7.2	De persoonsgegevens worden alleen verwerkt in overeenstemming met van toepassing zijnde wet en regelgeving.	Artikel 14 lid 3 Wbp.	De instelling is verplicht zich aan de Wbp te houden. Echter, de instelling is vaak (mede-) aansprakelijk voor schendingen van de Wbp door de cloudleverancier. Indien naleving van de Wbp door de cloudleverancier als een contractuele verplichting is opgenomen, ook ten aanzien van wijzigingen, kan de instelling de overeenkomst makkelijker beëindigen of schadevergoeding vorderen in het geval van een schending van de Wbp.	
7.3	Vastgelegd is welke (groepen)medewerkers van de cloudleverancier bevoegd zijn tot welke verwerkingen van de persoonsgegevens.	Pag. 33 richtsnoer.	Ter beveiliging van de persoonsgegevens dient in de overeenkomst te worden vastgelegd welke medewerkers (functionarissen) of welke groepen medewerkers welke verwerkingen mogen uitvoeren ten aanzien van de persoonsgegevens. Er geldt een expliciet verbod op het uitvoeren van verwerkingen door andere medewerkers dan de genoemde (groepen) medewerkers in dit artikel.	Voor de verwerkingen kan worden gekeken naar artikel 2. Afhankelijke van invulling van de clouddienstverlening in hoeverre dit kan worden ingevuld.
7.4	De verwerking van de persoonsgegevens vindt alleen plaats in opdracht van de instelling en zoverre noodzakelijk voor uitvoering	Artikel 12 en 14 Wbp.	De cloudleverancier mag de persoonsgegevens van de instelling alleen verwerken voor zover dat noodzakelijk is om de dienstverlening aan de instelling te leveren. De	Op grond van deze bepaling mag de cloudleverancier persoonsgegevens verwerken voor zover dat is

	van de overeenkomst.		cloudleverancier mag de persoonsgegevens niet voor eigen doeleinden gebruiken.	bepaald in de overeenkomst. Het is daarom belangrijk de overeenkomst en eventuele bijlagen te controleren op mogelijke doeleinden voor verwerking. Daarnaast geldt een meldingsplicht indien de verwerking een verzoek of een bevel van een toezichthouder of een opsporings-, strafvorderings- of nationale veiligheidsinstantie betreft (zie artikel 9.3 van het normenkader).
7.5	De cloudleverancier is verplicht mee te werken aan het uitvoeren van rechten van betrokkenen	Artikel 35 en 36 Wbp.	Op grond van de Wbp hebben betrokkenen inzage en correctierechten wanneer het hun eigen persoonsgegevens betreft. Daartoe kan een betrokkene een verzoek doen bij de verantwoordelijke (instelling). Met deze bepaling wordt de cloudleverancier verplicht mee te werken om aan de rechten van betrokkenen te voldoen.	Bij het meewerken van de cloudleverancier is het handig rekening te houden met de termijnen die gelden voor het behandelen en afhandelen van inzage en correctieverzoeken. Deze termijnen kunt u vinden in de artikelen 35 en 36 en verder van de Wbp.
7.6	De cloudleverancier is verplicht mee te werken aan het uitvoeren van rechten van betrokkenen	Artikel 35 en 36 Wbp.	Ter bescherming van de rechten van betrokkenen en de beveiliging van de persoonsgegevens is het voor de cloudleverancier verboden om in te gaan op verzoeken van betrokkenen. Dergelijke verzoeken dienen eerst op rechtmatigheid getoetst te worden door de verantwoordelijke (de instelling dus). In uitzonderingsgevallen kan de instelling een andersluidende instructie geven aan de cloudleverancier.	Nadat een betrokkene een inzage of correctieverzoek bij de instelling heeft ingediend, beoordeelt de instelling dit verzoek. Afhankelijk van deze beoordeling zal de instelling vervolgens de cloudleverancier instrueren.
7.7	De cloudleverancier is verplicht de instelling te informeren over toekomstige wijzingen in de dienstverlening.	CBP Richtsnoer beveiliging van persoonsgegevens pag. 35.	Om de taak als verantwoordelijke uit te kunnen voeren dient de instelling zich ervan te vergwissen dat persoonsgegevens overeenkomstig het vooraf bepaalde risiconiveau worden verwerkt. Wanneer de verwerking wijzigt (de dienstverlening van de cloudleverancier) moet de instelling voorafgaand aan de wijziging kunnen controleren of de verwerking overeenkomstig het passende niveau plaatsvindt. Daartoe is deze informatieplicht van dit artikel opgenomen.	De cloudleverancier geeft voorafgaand aan de toepassing van de wijziging aan dat de uitvoering van zijn dienstverlening gaat wijzigen. Deze wijzigingen dient beoordeeld te worden door de instelling (worden gegevens nog wel goed beveiligd en volgens de juiste normen verwerkt?). Afhankelijk van dit oordeel kan de procedure van artikel 3 worden gestart.

7.8	Derden hebben geen toegang tot de persoonsgegevens zonder toestemming van de instelling.	Artikelen 8, 9 12 13 en 14 Wbp.	De cloudleverancier (en degenen die onder zijn gezag handelen zoals personeel) is in beginsel verplicht om persoonsgegevens geheim te houden. Er zijn uitzonderingen bijvoorbeeld rechtmatige inzageverzoeken van bevoegde autoriteiten.	Zie ook artikel 6 en 7.3.
7.9	Wanneer de cloudleverancier derde partijen inschakelt bij de uitvoering van dienstverlening gelden de voorwaarden in dit artikel.	• Artikelen 12, 13 en 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 33 en 34.	Derden mogen alleen deelnemen aan de verwerking van de persoonsgegevens als de derde partij *rechtsreeks* betrokken is bij de uitvoering van de dienstverlening. Derde partijen die niet rechtsreeks betrokken zijn bij de verwerking van persoonsgegevens behoeven dan ook niet te voldoen aan de in deze overeenkomst bepaalde voorwaarden. Daarnaast dient de cloudleverancier een schriftelijke overeenkomst met de derde partij te hebben waarin is opgenomen dat de derde partij voldoet aan alle in deze overeenkomst opgenomen bepalingen. Alleen op deze wijze kan de instelling als verantwoordelijke zich vergewissen van een voldoende niveau van bescherming van persoonsgegevens.	Derde partijen zijn net als de cloudleverancier bewerkers in de zin van de Wbp. Daarom gelden voor hen dezelfde verplichtingen als voor de cloudleverancier. Wanneer er sprake is van derde partijen dient de instelling voorafgaand aan het sluiten van de overeenkomst met de cloudleverancier de schriftelijke overeenkomsten tussen de cloudleverancier en de derde partij in te zien en te beoordelen.
7.10	Een derde partij ontheft de cloudleverancier niet van verplichtingen en de cloudleverancier vrijwaart de instelling voor aanspraken van derden voor schending van de wbp.	CBP Richtsnoer beveiliging van persoonsgegevens pag. 34.	Wanneer de cloudleverancier een derde partij inschakelt voor de verwerking van persoonsgegevens betekent dat niet dat de cloudleverancier zich niet meer hoeft te houden aan de verplichting ten aan zien van de persoonsgegevens. Daarnaast is in deze bepaling een vrijwaring opgenomen. Wanneer een derde (bijvoorbeeld een betrokkene) de instelling aanspreekt op een schending van de Wbp (of andere wet- en regelgeving m.b.t. persoonsgegevens) en de schending is te wijten aan de cloudleverancier of een derde die door de cloudleverancier is ingeschakeld dan vrijwaart de cloudleverancier de instelling voor deze aanspraak.	
7.11	De kosten van een door het CBP opgelegde maatregel kan door de instelling worden verhaald op de		Wanneer de instelling een maatregel van het CBP (College bescherming persoonsgegevens) opgelegd krijgt vanwege een schending van de Wbp	Wanneer het CBP bijvoorbeeld een boete oplegt aan de instelling dan kan de instelling deze boete

	cloudleverancier		en de schending is ontstaan doordat de cloudleverancier (of een door hem ingeschakelde derde) zich niet gehouden heeft aan de afspraken in de overeenkomst dan kan de instelling de kosten voor de maatregel verhalen op de cloudleverancier.	verhalen op de cloudleverancier. Een opgelegde boete of last onder dwangsom valt hier ook onder. Een bepaling als deze kan worden opgenomen in het hoofddeel van de overeenkomst, namelijk het artikel betreffende de aansprakelijkheid.
7.12	De cloudleverancier mag de persoonsgegevens niet langer bewaren dan noodzakelijk voor het leveren van de dienstverlening.	• Artikel 10 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 34.	De instelling moet er zorg voor dragen dat de cloudleverancier de persoonsgegevens niet langer bewaart dan noodzakelijk voor de uitvoering van de dienstverlening. Dat betekent dat bij de beëindiging van de overeenkomst de persoonsgegevens niet meer verwerkt mogen worden (vernietigen of overdragen zie artikel 10). Uitzondering op deze bepaling is een dwingendrechtelijke wettelijk verplichting waaraan de cloudleverancier moet voldoen.	Doorgaans worden standaard bewaartermijnen gehanteerd door de cloudleverancier. Het is raadzaam deze termijnen te vergelijken met dit artikel en artikel 10 van het normenkader. Dan kan geconcludeerd worden of de cloudleverancier ten aanzien de te sluiten overeenkomst een uitzondering op haar procedures moet maken.
8.1	De cloudleverancier moet de gegevens adequaat beveiligen. Daarnaast moeten de beveiligingsmaatregelen omschreven zijn in de overeenkomst.	• Artikel 13 en 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 33.	De instelling moet als verantwoordelijke zorgdragen voor een adequate beveiliging van de persoonsgegevens door de cloudleverancier. Ten aanzien van de beveiliging geldt dat de instelling op basis van een risicoanalyse moet bepalen of de cloudleverancier voldoende waarborgen biedt voor de bescherming van persoonsgegevens. In de bepaling is aangegeven dat de beveiliging passend is bij het risico van de verwerking van de gegevens. Daarnaast wordt de cloudleverancier verplicht de beveiligingsmaatregelen schriftelijk vast te leggen. Ook dient de beveiliging van de gegevens conform de Wbp te zijn. Rekening moet worden gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging daarvan.	Voorafgaand aan het sluiten van de overeenkomst dient de instelling een risicoanalyse uit te voeren (zie hiervoor de oplegnotitie). Aan de hand van de risicoanalyse kan worden gecontroleerd of de cloudienstverlener voldoende waarborgen omtrent de beveiliging van persoonsgegevens in acht neemt. Om dit goed te kunnen beoordelen dient de instelling voorafgaand aan het sluiten van de overeenkomst relevante informatie op te vragen bij de cloudleverancier. Zie hiervoor ook artikel 7.9 van dit normenkader.
8.2	Informatieplicht ten aanzien van beveiligingsincidenten.	• Artikel 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegeven	Voor de cloudleverancier geldt een onmiddellijk informatieplicht ter zake van beveiligingsincidenten. Het gaat hierbij om vermoedelijke en	

		s pag. 33 en 35. • NEN-ISO/IEC 27002:2007 nl, paragraaf 10.2.3.	daadwerkelijk incident zodat de bescherming zoveel als mogelijk kan worden gewaarborgd. Onder incidenten vallen onbevoegde kennisneming, verlies of schending van beveiligingsmaatregelen. Naast de informatieplicht is de cloudleverancier verplicht om te reageren op de incidenten door de persoonsgegevens veilig te stellen, maatregelen nemen om het incident te beëindigen en/of te voorkomen en meewerken aan verder afhandeling van een incident.	
8.3	Onverwijlde informatieplicht over de beveiliging	• Artikel 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 33.	Omdat de instelling als verantwoordelijke moet kunnen controleren of de persoonsgegevens adequaat worden beveiligd is de cloudleverancier verplicht om op verzoek van de instelling onverwijld schriftelijke informatie over de informatiebeveiliging te verstrekken.	Vaak wordt voor de beveiliging verwezen naar certificaten van onafhankelijke derde te overleggen. Zie hiervoor artikel 8.4 en verder.
8.4 / 8.6	Controle op de beveiliging van de cloudleverancier	• Artikel 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 33 en 35.	Afhankelijk van de risicoklasse dient de dienstverlening van de cloudleverancier door de instelling te worden gecontroleerd. Dit kan worden gedaan door een periodieke controle door een onafhankelijke deskundige. Voor risicoklasse 1 is een tweejaarlijkse controle minimaal vereist. Voor risicoklasse 2 en 3 is een jaarlijkse controle vereist.	Dit is een van de belangrijkste bepalingen in dit normenkader. Deze bepaling geeft de instelling een instrument om haar taak als verantwoordelijk te kunnen uitvoeren. Ook voorafgaand aan het sluiten van de overeenkomst dient een dergelijk onderzoek te hebben plaatsgevonden zodat de instelling de dienstverlening door de cloudleverancier heeft onderzocht. Gedurende de looptijd van de overeenkomst is het dan ook noodzakelijk dat jaarlijks of tweejaarlijks een dergelijk onderzoek wordt uitgevoerd. Dit dient de instelling te monitoren. Zie hiervoor ook artikel 8.5 van het normenkader.
8.5	Controle op de beveiliging van de cloudleverancier	• Artikel 14 Wbp; • CBP Richtsnoer	De conclusies van het onderzoek door de onafhankelijke derde dient	

		beveiliging van persoonsgegevens pag. 33 en 35.	onverwijld door de cloudleverancier beschikbaar worden gesteld aan de instelling. Vaak is dit verwerkt in een zogenaamde TPM-verklaring (Third Party Mededeling).	
8.7	Controle op de beveiliging van de cloudleverancier	• Artikel 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 33 en 35.	Daar waar de risico's hoog zijn, is een periodiek onderzoek niet voldoende. Wanneer de instelling een redelijk vermoeden heeft van schending van gemaakte afspraken door de cloudleverancier, dient de instelling dit vermoeden te onderzoeken. Hierbij gaat het om een (beperkte) kwaliteitstoetsing die een direct verband heeft met het vermoeden van niet nakoming. De scope van dit onderzoek is dus beperkt tot de afspraken waarvan een instelling het redelijke vermoeden heeft dat deze zijn geschonden. Ook in dat geval is een onderzoek als bedoeld in artikel 8.4 / 8.6 van dit normenkader van toepassing. De uitvoering van het onderzoek wordt in eerste instantie bekostigd door de instelling. Wanneer uit het onderzoek blijkt dat er inderdaad sprake is van een schending van gemaakte afspraken dan kan de instelling de kosten voor het onderzoek verhalen op de cloudleverancier.	Het vermoeden van niet nakoming van de gemaakte afspraken kan bijvoorbeeld ontstaan wanneer de uitvoering van de dienstverlening is gewijzigd. Zie hiervoor ook de artikelen 3 en 7.7 van dit normenkader.
8.8	De cloudleverancier rapporteert ten aanzien van gegevensbeveiliging en beveiligingsincidenten aan de instelling.	• Artikel 14 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 33 en 35. • NEN-ISO/IEC 27002:2007 nl, paragraaf 10.2.3.	Als verantwoordelijke moet de instelling de informatiebeveiliging van de cloudleverancier controleren. Door een periodieke rapportage over informatiebeveiliging en beveiligingsincidenten kan op overstijgend niveau de dienstverlening van de cloudleverancier gecontroleerd worden.	In een driemaandelijkse rapportage geeft de cloudleverancier aan de stand van zaken ten aanzien van beveiligingsincidenten over de afgelopen periode. Daarnaast rapporteert de cloudleverancier over genomen maatregelen naar aanleiding van de incidenten en algemene maatregelen op het gebied van informatiebeveiliging. Het is raadzaam een vergelijking te maken met de voorgaande rapportage(s) om de voortgang van maatregelen

				en het beveiligingsniveau te monitoren. (8.2) Kan ook in SLA worden opgenomen.
9.1	Verwerking alleen in landen van EER of landen met een passend beschermingsniveau.	• Artikel 76 en 77 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 34.	Landen van de EER (Europees Economische Ruimte) hebben allen hoog niveau van privacybescherming. De Europese Commissie heeft tevens een lijst gepubliceerd waarop landen staan die een passend beschermingsniveau hebben (zogenaamde witte lijst via: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm) .	De instelling dient voorafgaand aan het contracteren van de cloudleverancier na te gaan waar de gegevens worden opgeslagen.
9.2	Verwerking alleen in landen van EER of landen met een passend beschermingsniveau.	• Artikel 76 en 77 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 34.	Wanneer dienstverlening van de cloudleverancier plaatsvindt in een land zonder een passend beschermingsniveau dan dient de cloudleverancier dit voorafgaand aan de toepassing daarvan dit te melden bij de instelling. De instelling kan dan haar taak als verantwoordelijke adequaat uitoefenen door de informatie over die landen en/of partijen na te gaan en indien de bescherming van persoonsgegevens in het geding is kan de instelling de overeenkomst beëindigen (zie ook artikel 3).	
9.3	Verplichtingen ingeval van onderzoek van autoriteiten	CBP Richtsnoer beveiliging van persoonsgegevens pag. 34 en 35.	Bij clouddienstverlening worden gegevens niet op locatie van de instelling bewaart. Wanneer autoriteiten een verzoek tot inzage in gegevens doen, dan dient de instelling als verantwoordelijk hierop adequaat te reageren. Wanneer de cloudleverancier een dwingendrechtelijke verzoek of bevel daartoe ontvangt, dan is de cloudleverancier verplicht om de instelling hierover te informeren. Hierbij dienen instructies van de instelling in acht worden genomen, waaronder de	

			behandeling van het verzoek of bevel over te laten aan de instelling. Als verantwoordelijke van de (persoons)gegevens dient de instelling het aanspreekpunt voor dergelijke verzoeken of bevelen te zijn.	
9.4	Verplichtingen ingeval van onderzoek van autoriteiten	CBP Richtsnoer beveiliging van persoonsgegevens pag. 34 en 35.	In sommige gevallen is het voor de cloudleverancier door dwingendrechtelijke wet- en regelgeving verboden om te voldoen aan artikel 9.3. In die gevallen dient de instelling alsnog de beveiliging van de gegevens te waarborgen. Daarom is de cloudleverancier verplicht een aantal handelingen uit te voeren die normaliter door de verantwoordelijke worden uitgevoerd. Met het uitvoeren van de genoemde punten wordt de bescherming van de persoonsgegevens zoveel als mogelijk gewaarborgd.	De instelling dient nadat zij op de hoogte is gebracht van een dergelijk verzoek of bevel na te gaan of de cloudleverancier de genoemde handelingen heeft uitgevoerd.
10.1	Toegang tot de gegevens bij beëindiging van de overeenkomst	• Artikel 10 Wbp; • CBP Richtsnoer beveiliging van persoonsgegevens pag. 35.	Bij het beëindigen van de overeenkomst dienen de gegevens (uitdrukkelijk alle gegevens en niet slechts persoonsgegevens) die zijn verwerkt door de cloudleverancier of te worden vernietigd of te worden overgedragen aan een nieuwe leverancier of de aan de instelling zelf. Elke andere mogelijkheid biedt geen passende bescherming voor de gegevens. Daarnaast kan de instelling ook op verzoek gedurende de looptijd van de overeenkomst gegevens laten vernietigen of buiten de dienstverlening van de cloudleverancier halen. Op deze wijze behoudt de instelling de controle en de beheersing over de gegevens.	
10.2	Dataportabiliteit van de gegevens		De dataportabiliteit betreft mogelijkheid om de gegevens te kunnen verplaatsen in de cloud. Wanneer er geen sprake is van dataportabiliteit kunnen de gegevens niet meer door de instelling teruggehaald worden.	

4. Classificatie persoonsgegevens

Uitgaande van de HORA (Hoger Onderwijs Referentie Architectuur) is door de Werkgroep Architectuur van het Project Regie in de Cloud een uitwerking gegeven van de classificatie van bedrijfsobjecten in het algemeen, en van persoonsgegevens in het bijzonder. Het onderstaande is de rapportage daarover uit HORA. Daarin wordt de classificatie O, L, M en H. gehanteerd. Deze komen overeen met respectievelijk risicoklasse O, I, II en III van het Normenkader. Voor de verwijzingen wordt verwezen naar de HORA-site.[5]

Een BIV-classificatie geeft aan welke mate van beschikbaarheid, integriteit en vertrouwelijkheid gewenst is voor een bepaald gegeven. Het is de basis voor het bepalen van passende informatiebeveiligingsmaatregelen, die op zowel processen, organisatie als technologie impact zullen hebben. Er is in dit project een generieke BIV-classificatie opgesteld. Deze is terug te vinden als een set van attributen bij de bedrijfsobjecten in het informatiemodel en is direct toegankelijk als rapport. Het is aan instellingen zelf om deze generieke BIV-classificatie te vertalen naar hun eigen classificaties en maatregelen. Hiervoor zijn standaard technieken beschikbaar zoals bijvoorbeeld de SPRINT methode voor risicoanalyse.

Een BIV-classificatie bestaat uit drie scores: een B-score, I-score en V-score. De waardes van deze scores kunnen zijn: hoog, middel of laag. Voor vertrouwelijkheid is er ook een “openbaar” die aangeeft dat specifieke gegevens publiek beschikbaar zijn. Gegevens die een grote rol spelen in de dagelijkse operatie van een instelling zijn geclassificeerd met een hogere B-score. Gegevens die nodig zijn voor geplande bijeenkomsten zoals toetsmateriaal scoren de hoogste B-score. De integriteit van sturende en financiële gegevens scoren een verhoogde I score. De gegevens die nodig zijn voor een goede uitvoering van het onderwijs scoren de hoogste I score. De vertrouwelijkheidsscore wordt bepaald door de bedrijfseconomische waarde en door de regelgeving rond de bescherming van persoonsgegevens. Gegevens die de identiteit, nationaliteit of ras vastleggen en gegevens die een economische situatie beschrijven scoren een hogere V-score. Gegevens die de medische, psychische of sociale situatie beschrijven van een persoon krijgen de hoogste V-score.

De V-score wordt in een aantal gevallen sterk beïnvloedt door specifieke attributen. Dit geldt met name voor bedrijfsobjecten met persoonsgegevens doordat de Wet Bescherming Persoonsgegevens allerlei eisen stelt aan vertrouwelijkheid. Het College Bescherming Persoonsgegevens (nu Autoriteit Persoonsgegevens) heeft specifieke richtsnoeren opgesteld voor het publiceren van persoonsgegevens op internet. Zuivere persoonsgegevens bevinden zich in de bedrijfsobjecten deelnemer, medewerker en individu. Er zijn bedrijfsobjecten die de relatie tussen de instelling en de personen weergeven. Zo bestaan er rond een deelnemer de gevoelige bedrijfsobjecten onderwijsovereenkomst, examenprogramma, onderwijseenheiddeelname, leer- en lesgroep, toetsresultaat en onderwijseenheidresultaat. Dit zijn alle transactiegeoriënteerde gegevenssets met een beperkte set aan attributen. Het heeft geen zin dergelijke bedrijfsobjecten nader te bestuderen op attribuutniveau.

Hieronder is een verkenning gemaakt van de attribuutgroepen die kenmerkend zijn voor de bedrijfsobjecten deelnemer en medewerker. In tabelvorm zijn de attribuutgroepen benoemd en is de bijbehorende V-score weergegeven. In het algemeen geldt, gegevens die van een persoon:

1. de identiteit, nationaliteit of ras vastleggen scoren M
2. een economische situatie beschrijven scoren M
3. de medische, psychische of sociale situatie beschrijven scoren H

Attribuutgroep	V-score
object-id	L
DUO-nummer	L
onderwijsnummer / BSN	M
naamsgegevens	L
geslacht	L

[5] Zie http://www.wikixl.nl/wiki/hora

e-mailadres	L
nationaliteit	M
verblijfsstatus	M
geboortedatum / plaats	M
datum / status overlijden	L
pasfoto	M
adressen (incl. status geheim)	L
telefoonnummer(s) (incl. status geheim)	L
bankrekeningnummer	M
vooropleidingen	L
toeganggevens diploma met cijferlijst	L
studiegerelateerde communicatie	M
functiebeperking	H
studie- en deelnemergerelateerde aantekeningen van begeleiders	H

Tabel 1 V-score voor attribuutgroepen van bedrijfsobject deelnemer

Attribuutgroep	**V-score**
object-id	L
BSN	M
naamsgegevens	L
geslacht	L
burgerlijke staat	L
gegevens kinderen	L
e-mailadres	L
nationaliteit	M
werkvergunningsgegevens	M
geboortedatum / plaats	M
datum / status overlijden	L
pasfoto	M
kopie paspoort	M
adressen (incl. status geheim)	L
telefoonnummer(s) (incl. status geheim)	L
bankrekeningnummer	M
opleidingen met diploma's	L
meest relevante diploma	L
beperkingen uit religie	M
verlof	M
ziekteverzuim / arbo-gegevens	H
dienstbetrekkinggerelateerde communicatie	M
functiebeperking / afspraken daarover	H

Tabel 2 V-score voor attribuutgroepen van bedrijfsobject medewerker

Ook applicaties kunnen worden voorzien van een BIV-classificatie als basis voor informatiebeveiligingsmaatregelen. De BIV-classificatie van bedrijfsobjecten kan gebruikt worden om een BIV-classificatie voor applicaties af te leiden. Cruciaal voor het bepalen van de BIV-classificatie van een applicatie is de vraag of een applicatie die geen bronsysteem voor een bepaald bedrijfsobject is, de gevoelige attributen van dat bedrijfsobject ontsluit. Als die gevoelige attributen niet ontsloten worden kan de BIV-classificatie van dat bedrijfsobject buiten beschouwing worden gelaten bij de classificatie van die applicatie. Als voorbeeld is in de volgende tabel de BIV-classificatie van het bibliotheeksysteem volgens dat principe uitgewerkt. De bedrijfsobjecten die alleen worden geraadpleegd door het bibliotheeksysteem zijn schuingedrukt weergegeven.

Bedrijfsobject	**B-score**	**I-score**	**V-score**
uitleen	L	L	L
werk	L	L	O
expressie	L	L	O
manifestatie	L	L	O
item	L	L	O
deelnemer	M	H	H
medewerker	M	H	H
vordering	L	M	L
inkomende betaling	L	M	L
kostenplaats	L	M	L
BIV-classificatie	L	L	L

Tabel 1 Voorbeeldclassificatie van het bibliotheeksysteem

Als het bibliotheeksysteem wel gevoelige attributen van deelnemer en/of medewerker ontsluit, moet de classificatie van dit systeem aangepast worden. Het is te overwegen om specifieke attributen die veel impact hebben op de BIV-classificatie van een applicatie te verplaatsen naar een aparte applicatie om te voorkomen dat er mogelijk zware informatiebeveiligingsmaatregelen noodzakelijk zijn voor de applicatie. Zo zouden bijvoorbeeld de gegevens over functiebeperkingen van deelnemers en studie- en deelnemergerelateerde aantekeningen van begeleiders kunnen worden weggelaten uit het studentinformatiesysteem om te voorkomen dat deze een V-score van hoog zou krijgen. Of een dergelijke afsplitsing zinvol is dient per situatie te worden beschouwd.

5. Aanbevolen gedragsregels medewerkers/studenten

Door het SURF Informatie Beveiligers Overleg van het Platform ICT en Bedrijfsvoering is een nieuwe versie (4.0) 'Model Acceptable Use Policy' (AUP) opgesteld voor zowel medewerkers als voor studenten[6]. Het Reglement/AUP stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door werknemers en studenten. Doel van de regels is de goede orde te bepalen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik
- tegengaan van seksuele intimidatie, discriminatie, inbreuk op rechten van derden en (andere) strafbare feiten
- bescherming van privacy gevoelige informatie waaronder persoonsgegevens van de Instelling en haar werknemers, en van studenten en ouders
- bescherming van vertrouwelijke informatie van de Instelling en haar werknemers, en van studenten en ouders
- bescherming van de intellectuele eigendomsrechten van de Instelling en derden waaronder het respecteren van licentie-afspraken die van toepassing zijn binnen de Instelling
- voorkomen van negatieve publiciteit
- kosten- en capaciteitsbeheersing

In de nieuwe versie 4.0 zijn de regels opgenomen die speciaal ingaan op de aspecten van eigendom, vertrouwelijkheid en privacy, relevant in het kader van dit Normenkader. De toelichting op de regels wordt hier geciteerd. De aanbeveling is om deze regels te verwerken in de betreffende reglementen van de instelling.

Medewerkers

Vertrouwelijke informatie

De bescherming van vertrouwelijke informatie wordt nu expliciet genoemd in de reglementen. De volgende tekst is opgenomen:
De werknemer dient vertrouwelijke informatie en privacygevoelige informatie waaronder persoonsgegevens, waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.
De werknemer besteedt bijzondere aandacht aan het treffen van maatregelen indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via E-mail, in niet Instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.).
Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft opgesteld zal werknemer deze strikt naleven.

Intellectueel eigendom

Met betrekking tot het gebruik van internet waren de bepalingen al in eerdere versies[7] opgenomen. De algemene regel is toegevoegd met de volgende tekst:
De werknemer maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling of derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

Zeggenschap

Met betrekking tot de zeggenschap over informatie was niets opgenomen. Onderstaande tekst is nu als optie in de nieuwe voorbeeldreglementen opgenomen.

---

[6] Zie onder http://www.surf.nl/nl/themas/securityenprivacy/informatiebeveiliging/Pages/Leidradeninformatiebeveiliging.aspx

[7] De al opgenomen bepaling is als volgt:
Bij het gebruik van internet is het verboden om:
- *films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enig illegale bron of wanneer de werknemer daadwerkelijk weet dat dit in strijd met auteursrechten is;*
- *films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.*

De zeggenschap over de informatie van de Instelling berust bij Instelling. De werknemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling..

Studenten

Ook het reglement voor de studenten is uitgebreid met de bepalingen m.b.t. Vertrouwelijkheid, privacy en intellectueel eigendom. Enerzijds door toevoegingen in bestaande teksten en tevens door het opnemen in een aparte paragraaf 'Intellectueel eigendom en vertrouwelijke informatie'. De teksten zijn in overeenstemming met de teksten die zijn opgenomen voor werknemers.

Ook hier is er optioneel de mogelijkheid tot het regelen van de zeggenschap over informatie opgenomen.

Privégebruik en overlast

In de inleiding is '*inbreuk maken op rechten van Instelling of derden*' ook als overlast genoemd.

Beveiliging door de Instelling én de student

In de inleiding zijn '*criminele activiteiten*' en '*schending van intellectuele eigendomsrechten*' en privacy-rechten toegevoegd.