Samenwerkingsplatform Informatie Onderwijs

Checklist

Digitaal overstap- of doorstroomdossier vo-mbo

Kennisnet, december 2014
Auteurs: Robert Klein (security-officer), Job Vos (jurist en functionaris gegevensbescherming)

Inhoud

1. Inleiding

1.1. Aanleiding

De verschillende onderwijsketens wisselen steeds meer informatie van en over leerlingen digitaal uit. Ook bij de overstap van het voortgezet onderwijs naar het middelbaar beroepsonderwijs groeit de behoefte om leerlinggegevens van de middelbare school te hergebruiken en digitaal uit te wisselen. Scholen willen de leerling op zijn nieuwe school immers het onderwijs geven dat het best bij hem past, en daarbij efficiënt en zorgvuldig omgaan met beschikbare gegevens. Als je bestaande gegevens geautomatiseerd overneemt, voorkomt je nodeloos overtypen. Dat bespaart tijd en typfouten in het intakeproces.

1.2. Doel en doelgroep

Dit document is bedoeld voor onderwijsinstellingen waarvan leerlingen overstappen van het vo naar het mbo.

Scholen noemen de gegevensuitwisseling tussen onderwijsinstellingen vaak het overstap- of doorstroomdossier. Daarbij wordt gebruik gemaakt van de Gegevensstandaard VO-MBO-overstapdossier. Maar hoe die moet worden toegepast, is soms de vraag. Dit document biedt richtlijnen voor medewerkers binnen de onderwijsinstelling die zich bezighouden met informatiebeveiliging en (toezicht op) de afspraken die hierover worden gemaakt binnen de instelling en met leveranciers.

Met deze checklist kunnen onderwijsinstellingen nagaan of de digitale uitwisseling van leerlinggegevens tussen een vo-school en mbo-instelling voldoet aan het normenkader (de technische en juridische eisen) rond privacy en beveiliging. Er wordt gewerkt aan integratie van dit document met het mbo-informatiebeveiligingsbeleid en de algemene formats die in dat kader worden ontwikkeld.

In de hoofdstukken 4 en 5 staan vereisten die specifiek gelden bij de uitwisseling van leerlinggegevens. Dat neemt niet weg dat een groot deel van deze eisen ook van toepassing zijn op andere soorten uitwisselingen. De inhoud en opzet van dit toetsingskader zijn niet geschreven voor specialisten, maar enige achtergrondkennis is wel noodzakelijk. Hoofdstuk 3 beschrijft welke juridische kaders van toepassing zijn. Dit deel van het document zal vooral nuttig zijn voor de juridische afdeling of het bestuursbureau. Hoofdstuk 4 bevat vooral technische specificaties en normen, dus dat deel is relevant voor de ict-beheerder of -coördinator of voor de afdeling interne automatisering.

Deze checklist staat niet los van het door de onderwijsinstelling gevoerde informatiebeveiligingsbeleid. Verder gaat niet om de keuze voor het studentinformatiesysteem (SIS), maar over (de keuze voor) het technische platform dat de uitwisseling van leerlinggegevens tussen scholen mogelijk maakt. Dit platform kan ook onderdeel uitmaken van een bestaand SIS.

1.3. Scope

De uitwisseling van gegevens zoals we in dit document bespreken, behelst overigens ook de uitwisseling van zorggegevens. Uiteraard alleen voor zover noodzakelijk voor het leren en begeleiden van de leerling.

Recent is Passend onderwijs ingevoerd. De daaruit volgende specifieke eisen voor uitwisseling van gegevens omtrent gedrag en gezondheid van leerlingen verwerken we op een later tijdstip in dit document.

1.4. Verantwoording

Deze checklist is tot stand gekomen binnen het Samenwerkingsplatform Informatie Onderwijs (SION) in samenwerking met saMBO-ICT en de volgende onderwijsinstellingen:

Arcus College
Nova College
Hoornbeeck College
Citaverde College
Aventus
ROC West-Brabant
Grafisch Lyceum Rotterdam
Parkstad College Limburg

Als basis voor de checklist is gebruik gemaakt van de volgende initiatieven.

- **Toetsingskaders MBO Taskforce Informatiebeveiliging voor instellingen**
  De checklist is tot stand gekomen in nauwe samenwerking met de taskforce die vanaf 2015 de checklist verder zal beheren en doorontwikkelen.

- **Gegevensstandaard VO-MBO-overstapdossier**
  De gegevensstandaard VO-MBO-overstapdossier[1] is de afspraak voor de uitwisseling van (de gegevens in) het overstapdossier tussen vo-en mbo-instellingen. Deze standaard – die binnen SION is ontwikkeld – doet recht aan de behoefte van instellingen om te beschikken over al die concrete informatie die nodig is voor een goede plaatsing en begeleiding in het mbo.

  In de gegevensset staat wat geleverd kan worden, én wat (juridisch gezien) geleverd mag worden. Daarom is een concrete eis in deze checklist dat de leverancier voldoet aan de standaard VO-MBO-overstapdossier. Deze standaard wordt beheerd door Edustandaard.

- **Certificeringsschema Edukoppeling voor leveranciers**
  Het Certificeringsschema Edukoppeling – dat ook binnen SION is ontwikkeld – is bedoeld voor leveranciers van clouddiensten. Het maakt gebruik van de normen uit de Cloud Control Matrix van de Cloud Security Alliance (CSA[2]). Het doel van certificering is om vertrouwen te creëren in de leveranciers van clouddiensten. Het certificeringsschema schrijft daarom ook voor op welke wijze de leverancier dient aan te tonen dat hij aan de normen voldoet of zal voldoen. Het schema is reeds in gebruik voor de webservices van DUO voor digitaal aanmelden. Het zal ook worden toegepast bij Facet en de (toekomstige) uitwisseling met BRON.

  In deze checklist verwijzen we naar de normen uit dit schema, waar het gaat om eisen die onderwijsinstellingen moeten stellen aan cloudleveranciers. Het normenkader in het schema wordt beheerd door Edustandaard.

1.5. Leeswijzer

Hoofdstuk 2 beschrijft welke risico's er zijn bij het uitwisselen van gegevens. In de daarop volgende hoofdstukken staat welke maatregelen je als onderwijsinstelling kunt nemen om deze risico's te beperken.

Hoofdstuk 3 geeft een algemene inleiding in privacy. Wat moet een onderwijsinstelling regelen om de privacy goed te waarborgen? Hierbij gaan we ook in op specifieke regels die zijn afgeleid uit onderwijswetgeving.

[1] http://www.edustandaard.nl/standaarden/afspraken/afspraak/vo-mbo-overstapdossier/0.3

[2] https://cloudsecurityalliance.org/

Daarnaast schetsen we concrete maatregelen om de risico's te beperken. De maatregelen hebben de vorm van een af te vinken checklist: wel of niet geregeld.

Hoofdstuk 4 beschrijft de technische normen die van toepassing zijn op de uitwisseling van gegevens. Wat moet er technisch zijn gerealiseerd om de risico's uit hoofdstuk 3 te beperken? Dit hoofdstuk beschrijft de maatregelen die de school zelf moet nemen, maar ook wat een leverancier van een extern systeem moet doen.

Aan de inhoud van dit toetsingskader is veel zorg en aandacht besteed. Ondanks de betrokkenheid van verschillende experts en ervaringsdeskundigen, kunnen aan het gebruik van de checklists en de opgenomen informatie, conclusies en aanbevelingen geen rechten worden ontleend. Het verdient aanbeveling om in specifieke situaties deskundig (juridisch of technisch) advies in te winnen.

2. Risico's

2.1. Algemeen

Als je als onderwijsinstelling in beeld wil krijgen wat je moet regelen, kun je kijken naar de risico's die gegevensuitwisseling met zich meebrengt. Welke maatregelen kunnen die risico's beperken? Deze handreiking beperkt zich tot risico's van gegevensoverdracht bij de overstap van vo naar mbo.

Om een beleid voor informatiebeveiliging te formuleren, zijn de vier fasen van de Demingcirkel (plan-do-check-act) bruikbaar:

Fase 1 (plan): Inventariseer de risico's, kaders en principes en de normen of maatregelen
Fase 2 (do): Richt je beleid in op basis van risico's, modellen, leidraden en bijv. starterkits.
Fase 3 (check): Toets dit beleid aan normenkaders (op basis van bijv. selfassessment, peeraudit, of externe audit of benchmark).
Fase 4 (act): Voer het beleid uit en controleer het jaarlijkse om het te kunnen verbeteren.

2.2. Soorten schade

Als je gegevens uitwisselt, zijn er verschillende soorten schade mogelijk. De ene schade heeft meer impact dan de andere. Voorbeeld van schades zijn:

- Vertrouwens- of reputatieschade: als examenfraude of misbruik van persoonsgegevens bekend wordt via de media, dan wordt het imago van een school of de sector aangetast. Omdat mbo-instellingen belangrijke waardepapieren afgeven (diploma's), kan reputatieschade grote gevolgen hebben.
- Financiële schade: als data niet juist worden geïmporteerd (waardoor onjuiste gegevens worden gebruikt), dan wordt niet de juiste bekostiging verkregen. Ook kunnen fraude en gegevenslekken tot boetes leiden.
- Overige schade: als onderwijsinstelling moet je voldoen aan bepaalde wet- en regelgeving. Op een aantal onderdelen volgt controle door de accountant. Als er iets mis gaat, dan kan dit leiden tot de feitelijke constatering dat een instelling handelt in strijd met de wet, tot reputatieschade en tot het uitblijven van de accountantsverklaring. Dit alles kan gevolgen hebben voor de financiering en zelfs de continuïteit van de instelling.

2.3. Specifieke risico's voor gegevensuitwisseling

Bij de uitwisseling van gegevens bij de overstap van het vo naar het mbo doen zich verschillende risico's voor, zowel op privacy- als op techniekniveau:

<u>Privacy (risico's die kunnen leiden tot inbreuk op wetgeving, reputatieschade, boetes en schade voor betrokkenen):</u>

a) Onrechtmatige verwerking van gegevens: als er geen doel/doelbinding/grondslag is, of geen toestemming van de betrokkenen (zie toelichting in paragraaf 3.2);
b) Onvoldoende borging en bewustzijn: als er geen interne procedures zijn voor onderwerpen als: 'Wie mag welk dossier inzien', 'Hoe informeren we ouders en leerling over het inzage- en correctierecht', en 'Hoe is de procedure geregeld om bezwaar te maken?';
c) Onrechtmatige toegang: als er onvoldoende beveiliging is (lekken, hacken) of bij onjuiste autorisaties (autorisatiematrix);
d) Verwerking in strijd met de wet: als de instelling gegevens ontvangt en verwerkt waar ze geen recht op heeft;

e) Onrechtmatige verspreiding: als er gegevens worden gedeeld met derden die daartoe niet gerechtigd zijn of waarmee niet de juiste afspraken zijn gemaakt (de bewerkersovereenkomst, zie toelichting in paragraaf 3.2 en de bijlage);
f) Beveiliging en controle: als er onvoldoende controle is (doordat er niet gelogd wordt) kan het gebeuren dat fraude niet te ontdekken is (belangrijk: functiescheiding, vierogenprincipe);
g) Geen archief- en bewaarbeleid: als een instelling gegevens langer bewaart dan nodig of toegestaan is,
h) Gebrek aan afspraken en procedures: dit kan leiden tot onrechtmatig gebruik van de applicatie;
i) Onvoldoende bewustzijn: als medewerkers hun wachtwoorden opschrijven of hun monitor niet locken, dan faalt de beveiliging. Ook kunnen gebruikers onbedoeld de beveiliging uitschakelen;
j) Onvoldoende afspraken toeleveranciers en derden: als de aanleverende of verrijkende dienstenleverancier (bijv. van mentorgegevens) wordt gehackt, kunnen er via een zijdeur vertrouwelijke gegevens lekken;
k) Onvoldoende afstemming en gegevensdefinitie: dossieruitwisselingen gaan (vaak) fout, er worden verkeerde gegevens uitgewisseld. Ook: als er geen centrale regie is over de uitwisselingen kunnen de partijen bij een dispuut onderling vast komen te zitten in besluiteloosheid.

Techniek (risico's die kunnen leiden tot integriteitsrisico's of tot het niet beschikbaar zijn van de dienst):

l) Beschikbaarheid: risico op uitval of defecten door een gebrek aan redundante (dubbele) uitvoer, of door falende beveiliging;
m) Geen toegangsbeheer/autorisatie: als er geen organisatorische functiescheiding is binnen de onderwijsinstelling dan kan dit leiden tot onvoldoende identiteitscontrole. Daarmee ontstaat het risico op ongeoorloofd gebruik of toegang (bijvoorbeeld door hackers of fraudeurs). Dit kan gevolgen hebben voor de beschikbaarheid of integriteit. Gevolg: reputatieschade.
n) Onvoldoende beveiliging: het gehele proces moet beveiligd zijn, dus ook bijvoorbeeld netwerkverkeer tussen gebruiker en dienst en tussen diensten onderling. Zo voorkom je dat hackers toegang kunnen krijgen;
o) Gebrekkige programmatuur of apparatuur: onbetrouwbare programma's of hardware kunnen leiden tot verlies van data of tot fouten;
p) Back-up- en exitstrategie: als er in de applicatie niet genoeg maatregelen zijn opgenomen (zoals dagelijkse back-up) kunnen data verloren gaan. Ook afspraken met leveranciers zijn belangrijk;
q) Onvoldoende scheiding test en productie: door te testen met 'productiegegevens' krijgen testers en ontwikkelaars onnodig inzage in persoonlijke gegevens van leerlingen. Ook ontstaat er een kans op fouten (bijvoorbeeld het lekken van echte data in de testfase);
r) Beheerproces niet gestructureerd: kans op verstoringen en datalekken is groot.

We bespreken de maatregelen om de juridische risico's te beperken in het hoofdstuk juridische kaders (hoofdstuk 3); de technische oplossingen worden in het daarop volgende hoofdstuk geschetst (hoofdstuk 4). We benaderen deze thema's apart, maar ze zijn onlosmakelijk met elkaar verbonden. Zo zal een onderwijsinstelling technische beveiligingsmaatregelen moeten nemen om te kunnen voldoen aan de juridische kaders voor uitwisseling van persoonsgegevens.

3. Juridische eisen en maatregelen

3.1. Algemeen

Om goed in beeld te krijgen welke eisen gelden bij de uitwisseling van gegevens bij de overstap van vo naar mbo, is het belangrijk de algemene uitgangspunten te kennen die gelden bij álle vormen van uitwisseling van persoonsgegevens. Het gaat daarbij om de rechten en plichten van de leerling, zijn ouders, de onderwijsinstelling (bevoegd gezag, medewerkers), én die van leveranciers. Daaruit is af te leiden welke eisen gelden.

Bij de uitwisseling van gegevens tussen onderwijsinstellingen gaat het om privacy, gevolgd een aantal voorschriften uit de onderwijswetgeving. De eisen voor gegevensoverdracht zijn dus gebaseerd op zowel de privacy- als de onderwijswetgeving.

Als het om privacy van leerlingen gaat, dan gaat het ook om hun ouders. Als een leerling jonger is dan 16 jaar, dan beslissen zijn wettelijke vertegenwoordigers over de privacy. Daarom: als we in dit document over ‘leerling’ of ‘betrokkene’ spreken, bedoelen we bij een leerling onder de 16 jaar (ook) zijn wettelijk vertegenwoordigers.

3.2. Checklist deel A: Privacy

Bij privacy gaat het wettelijk gezien om alle gegevens die te herleiden zijn tot een bepaald persoon. Alles wat met die persoonsgegevens wordt gedaan, wordt in de wet ‘verwerken’ genoemd. Dus: verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen, enzovoort. Ook het uitwisselen van persoonsgegevens valt onder deze definitie. De verwerking van persoonsgegevens is geregeld in de Wet bescherming persoonsgegevens (Wbp). Deze wet geeft alleen algemene uitgangspunten. Het gaat daarbij over zowel offline als online verwerking van persoonsgegevens.

De wet onderscheidt drie partijen bij de verwerking van persoonsgegevens:

1. De **verantwoordelijke**. In het onderwijs is dit vaak de directie of het bestuur: het bevoegd gezag. Deze verantwoordelijke stelt vast welke persoonsgegevens worden verwerkt en met welk doel. De verantwoordelijke is ook daadwerkelijk eindverantwoordelijk voor de verwerking.
2. De **bewerker**. Dit is de partij die namens de verantwoordelijke de persoonsgegevens verwerkt, bijvoorbeeld de leverancier van leermiddelen. De bewerker mag met de persoonsgegevens alleen dat doen wat de verantwoordelijke heeft opgedragen.
3. De **betrokkene**. Dit is de persoon over wie de persoonsgegevens gaan: de leerling. Als de betrokkene jonger is dan 16 jaar, beslissen zijn wettelijk vertegenwoordigers (ouders) over de gegevens.

Als de school een leverancier inschakelt om de leerlingenadministratie te verzorgen, dan is deze leverancier van het studentinformatiesysteem (SIS-leverancier) een *bewerker* voor de school. Ook bij gegevensuitwisseling met educatieve uitgeverijen is de school de verantwoordelijke en de leverancier de bewerker: de school blijft eindverantwoordelijk voor de gegevens die zij verstrekt. Daarbij is de beveiliging van de persoonsgegevens een belangrijk issue: de verantwoordelijke moet dit met de leverancier regelen. Daarnaast vereist de wet dat de verantwoordelijke met een bewerker altijd een overeenkomst sluit (zie verder paragraaf 3.4).

Voorwaarden om persoonsgegevens uit te wisselen
Om persoonlijke informatie te mogen verwerken, moet aan een aantal voorwaarden worden voldaan. Deze wettelijke eisen uit de Wbp zijn terug te brengen tot de vijf vuistregels:
1. **Doel**: persoonsgegevens worden altijd verzameld met een vooraf vastgesteld doel. In het onderwijs gaat het om het leren en begeleiden van de leerling op de oude én nieuwe school;

2. **Doelbinding**: persoonsgegevens mogen alleen worden verwerkt voor zover dat nodig is om het vastgestelde doel te bereiken. Gegevens die daarmee niet in verband staan, mogen dus niet worden uitgewisseld. Ook de juiste beveiligingsmaatregelen zorgen er voor dat de gegevens niet voor een verkeerd doel worden gebruikt;
3. **Grondslag**: persoonsgegevens mogen alleen verwerkt worden als de Wbp hier een grond voor noemt. Voor het onderwijs zijn de relevante gronden:

a) Toestemming: als de betrokkene toestemming geeft (bijvoorbeeld een vinkje of akkoord aanklikt);
b) Overeenkomst: gegevens mogen verwerkt worden als dat nodig is voor de uitvoering van de overeenkomst met betrokkene, bijvoorbeeld de onderwijsovereenkomst;
c) Wet: als de wetgeving eist dat persoonsgegevens verwerkt worden (bijvoorbeeld uitwisseling met DUO);
d) Publiekrechtelijke taak: op basis de aan de school opgedragen publieke taak is gegevensverwerking noodzakelijk. Bijvoorbeeld voor het geven van onderwijs of het uitgeven van diploma's;
e) Gerechtvaardigd belang: het verzamelen van de persoonsgegevens is belangrijker dan het privacybelang van de betrokkene. Dit vereist een belangenafweging en de betrokkene mag zich verzetten.

4. **Dataminimalisatie**: de persoonsgegevens die de school verwerkt moeten redelijkerwijs nodig zijn om het doel te bereiken; ze moeten in verhouding staan tot het doel (proportioneel) en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt (subsidiair). Het gaat niet om het zo min mogelijk gegevens verzamelen, maar om het verkrijgen van alleen die gegevens die echt nodig zijn om het doel te bereiken;
5. **Transparantie en rechten betrokkene:** de betrokkene (dus: de leerling en/of zijn ouders) is vooraf geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. Dit moet gebeuren in voor hem begrijpelijke taal. Dit kan bijvoorbeeld in de schoolgids of via de website zijn, of er is een privacyprotocol. De betrokkene heeft recht op inzage, correctie en soms verzet of zelfs verwijdering van zijn persoonsgegevens.

Bij het omgaan van persoonsgegevens van en over leerlingen, wordt ook rekening gehouden met de gevoeligheid van die gegevens. Dit noemen we risicoklassen. Tot enkele jaren terug golden er strikt van elkaar gescheiden classificaties (met de klassen 0 tot en met III). Maar tegenwoordig bekijkt men gegevens meer in de context waarbinnen ze worden gebruikt. Een voorbeeld: een adres van een leerling kan misschien een vrij algemeen en veelvoorkomend persoonsgegevens zijn (voorheen klasse I). Weinig gevoelige informatie dus. Maar als een leerling met één van zijn ouders in bijvoorbeeld een blijf-van-mijn-lijfhuis woont, dan wordt zijn adres een uitermate gevoelig persoonsgegeven dat alleen bij een strikte groep bekend mag zijn.

Kwalificatie van informatie
Om persoonsgegeven overzichtelijk in te delen, gebruikt de wet drie categorieën informatie:

- **Publieke informatie:** deze deel je met de wereld. Denk aan de website van Kennisnet. Bedoeld voor het publiek zonder onderscheid in rollen.
- **Gevoelige informatie:** is bestemd voor een beperkt publiek. Deze informatie scherm je zo af dat derden er geen inzage in hebben en de informatie ook niet kunnen wijzigen.
- **Zeer gevoelige informatie:** is bestemd voor een beperkt publiek en is absoluut niet bedoeld om met derden te delen. Bedrijfsgevoelige informatie, accountgegevens, bijzondere persoonsgegevens zoals medische informatie, etc.

Maatregelen
De veiligheidsmaatregelen die je als onderwijsinstelling treft, moeten aansluiten bij de categorie gegevens. Ook moet de autorisatie binnen de onderwijsorganisatie hierop zijn ingericht. Bijvoorbeeld: inzage in medische informatie hebben docenten niet (te allen tijde) nodig, maar bijvoorbeeld een zorgcoördinator weer wel. De instelling moet hiervoor een beleid opstellen: wat wordt waar geregistreerd? En wie heeft waarin inzage?

Verder vereist de wet dat persoonsgegevens niet onbeperkt of zomaar worden bewaard. Een standaard bewaartermijn is twee jaar (na het eindigen van de opleiding door de deelnemer), tenzij een (onderwijs)wet een andere termijn voorschrijft (zoals bijvoorbeeld voor het bewaren van diploma's). Binnen het mbo schrijft de

Archiefwet voor een aantal gegevens en documenten bewaar- én de vernietigingstermijnen voor. Zie voor meer informatie de Kennisnetpublicatie “Hoe?Zo! Documentmanagement”. Misschien lijkt het handig om aanmeldgegevens te bewaren van leerlingen die zich niet inschrijven? Wees voorzichtig: de wet verbiedt het onbeperkt opslaan van die gegevens.

✓✗	WAT DE WET VOORSCHRIJFT VOOR DE ONDERWIJSINSTELLING
	Is duidelijk met welk doel de gegevens worden uitgewisseld?
	Is er een beschrijving (‘doelbinding’), wat is de grondslag, op welke manier zijn de rechten van betrokkenen geborgd?
	Is de beschrijving beschikbaar voor betrokkenen (hun ouders) en leveranciers? Is die beschrijving begrijpelijk?
	Zijn de rollen van iedereen duidelijk? Wie is de verantwoordelijke, welke partijen zijn bewerkers, wie is de betrokkene? (let op: de ouders bij jongeren onder de 16 jaar)
	Wordt er onderscheid gemaakt in de gevoeligheid van de verzamelde persoonsgegevens, en hanteert de instelling aparte inzagerechten voor verschillende soorten medewerkers (‘autorisatiematrix’)?

3.3. Checklist deel B: Onderwijswetgeving

De Wet op het voortgezet onderwijs (WVO) en Wet educatie en beroepsonderwijs (WEB) schrijven voor welke gegevens moeten worden gevraagd aan leerlingen (en hun ouders) bij inschrijving op een nieuwe school. Het ‘Besluit uitwisseling leer- en begeleidingsgegevens’ geeft een aantal kaders voor de typen uit te wisselen gegevens.

Aanmelden en inschrijven
De onderwijspraktijk maakt een onderscheid tussen aanmelden (de fase waarin een leerling kenbaar maakt dat hij zich wil inschrijven op de betreffende school) en inschrijven (de fase waarin de school heeft beslist dat de leerling wordt toegelaten). De onderwijswetten maken dit onderscheid niet; daar is alleen sprake van inschrijven. Dit verschil houdt in dat het aanmelden op een school gezien wordt als een soort ‘precontractuele fase’ van het inschrijven. Er mogen bij aanmelden wel gegevens worden uitgewisseld, maar dit zijn er minder dan de gegevens dan die nodig zijn voor inschrijven. Dit sluit aan bij de vierde vuistregel: dataminimalisatie (zie paragraaf 3.2). Scholen mogen alleen die informatie vragen die nodig is voor de betreffende fase van aanmelding/inschrijving.

Toestemming vragen en registreren
Een belangrijk uitgangspunt bij uitwisseling van leerlinggegevens tussen scholen, is dat deze uitwisseling alleen mag plaatsvinden met toestemming van de betrokken leerling (en als die jonger is dan 16 jaar: zijn ouders). Dit betekent ook dat de ouders voorafgaand inzage hebben gehad in de gegevens die worden uitgewisseld. De oude (latende[3]) school moet de toestemming vastleggen. In de context van deze checklist is dat dus de vo-school. Als de ouders bij de nieuwe (mbo-)school bezwaar maken tegen uitgewisselde gegevens, dan is het de oude (latende) school die moet aantonen dat de leerling of zijn ouders wél toestemming hebben gegeven voor uitwisseling. Ze kunnen die toestemming mondeling geven, maar ook schriftelijk (bijvoorbeeld handtekening), of digitaal (bijvoorbeeld door het tonen van de gegevens en aansluitend afvinken of aanklikken van de akkoordknop). Het kan dus handig zijn dat het systeem dat voorziet in de uitwisseling, een ‘invoerveld’ heeft waarop de toestemming kan worden aangevinkt, plus de datum en wijze van toestemming. Het is belangrijk dat de nieuwe (ontvangende) school kan vertrouwen op de juiste wijze van vastlegging van toestemming van de leerling of zijn ouders.

Burgerservicenummer
Het Burgerservicenummer (BSN) van de leerling is één van de gegevens die uitgewisseld moet worden. Dit nummer is ook noodzakelijk voor de uitwisselingen met OCW/DUO. Het doel van de uitwisseling van het BSN is

[3] Met ‘latende school’ bedoelen we de vo-school waar de leerling vandaan komt. De ‘ontvangende school’ is de mbo-instelling die de leerling (mogelijk) zal inschrijven.

een soepel doorlopende leerlijn voor elke leerling. Alleen de scholen mogen gebruik maken van het BSN. Als de school een leverancier inschakelt voor de administratie of uitwisseling van gegevens, dan kan dat alleen als de leverancier bewerker is voor de school. Een bewerker wordt dan namelijk gezien als het 'verlengstuk' van de school. Een bewerker mag dus niet allerlei bewerkingen uitvoeren met het BSN die niet in opdracht van de verantwoordelijke school worden uitgevoerd. Het BSN mag niet door een leverancier zelf worden gebruikt als identificerend gegeven. Een intern identificatienummer toekennen, een e-mailadres gebruiken of bijvoorbeeld communiceren met de ouders mag de bewerker dus niet. Het BSN is alleen bestemd voor gebruik door en ten behoeve van de school voor het leren en begeleiden van leerlingen.

Edustandaard
De inhoud van de uit te wisselen gegevens, is gedefinieerd in de gegevensset van Edustandaard (zie paragraaf 1.4). Het gebruik van deze standaard voorkomt dat er verkeerde, onjuiste of zelfs verboden gegevens worden uitgewisseld. Deze Edustandaard wordt besproken met nagenoeg alle (keten)partijen die betrokken zijn bij uitwisseling van overstapgegevens, zodat binnen de hele keten overeenstemming bestaat over de gegevens.

Niet meer gegevens dan nodig
Een andere wettelijke beperking die geldt bij het uitwisselen van gegevens, is dat uit de wetgeving volgt dat er niet meer gegevens mogen worden uitgewisseld dan strikt noodzakelijk is voor het leren en begeleiden van de leerling op de nieuwe school. Het uitgangspunt is om zo min mogelijk gegevens uit te wisselen: alleen de gegevens die relevant zijn voor de nieuwe school. Dus de oude school mag niet het gehele leerlingdossier (ongezien) doorsturen, maar alleen die gegevens die men relevant vindt voor de nieuwe school. Hierbij gaat het om een specifieke set gegevens die de docent/directeur (van de oude school) heeft geselecteerd. Het systeem dat de uitwisseling faciliteert, moet hierin dus kunnen voorzien.

Niet meer gebruikers dan nodig
Alleen scholen mogen gebruikmaken van een uitwisselingsservice (en dus ook de leveranciers die bewerker zijn van de school). Zo'n uitwisselingsservice mag geen centraal schakelpunt of postbus zijn, waar iedere onderwijsdienstverlener uit kan putten. Ook koppeling met andere dossiers (zoals het EPD, Jeugdzorg- of kinddossier) is verboden. Ook mogen er geen (aanvullende) gegevens aan de overheid worden geleverd, centraal bewaren mag niet en ook voor het verrijken van de leerlinggegevens is geen ruimte. Gegevens mogen dus niet eindeloos centraal opgeslagen worden, maar alleen tijdelijk en alleen in het kader van de uitwisseling.

Checklist
De volgende checklist beschrijft wat de instelling zelf moet regelen (met bijvoorbeeld de leverancier). Gebruik en beheer van deze checklist zal bijvoorbeeld bij een bestuursbureau belegd kunnen worden (eerder dan bij de interne it-afdeling). Hieronder bedoelen we met 'latende school' de vo-school. De 'ontvangende school' is de mbo-instelling die de leerling (mogelijk) zal inschrijven.

✓✗	**WAT DE WET VOORSCHRIJFT VOOR ONDERWIJSINSTELLINGEN**
	Zijn er afspraken met de leverancier (zie paragraaf 3.2 en 3.4)? • *Er is een bewerkersovereenkomst (zie bijlage voor een voorbeeld).* • *De leverancier is bewerker van de school, de bewerker doet zelf niets met de gegevens of het BSN.*
	Wordt er aan de leerling of diens ouders door de latende school toestemming gevraagd voor uitwisseling? • *Niet verplicht maar wenselijk: wordt de datum en wijze waarop de toestemming is verleend ook doorgegeven?*
	Controleert de uitwisselingsservice of het veld 'toestemming' door de latende school is ingevoerd of aangevinkt? • *Zonder toestemming mag het dossier niet worden uitgewisseld.*
	Wisselt de leverancier de gegevens alleen uit? • *Het is niet toegestaan dat de gegevens na aanlevering door de latende school worden gewijzigd of*

	verrijkt met andere data. • *Technisch ordenen is wel toegestaan, maar muteren door de leverancier niet.*
	Worden de uit te wisselen gegevens alleen samengesteld door de latende school? • *Scholen mogen alleen die gegevens uitwisselen die strikt noodzakelijk zijn voor het leren en begeleiden van de leerling op de nieuwe school.* • *Scholen mogen niet standaard het hele leerlingdossier van de latende school uitwisselen.* • *Het moet mogelijk zijn om alleen bepaalde gegevensvelden te selecteren om uit te wisselen.* • *Er worden geen (aanvullende) gegevens aan derden geleverd of centraal bewaard.*
	Zijn de gegevens alleen in te zien door de ontvangende school? • *Gegevens worden niet centraal opgeslagen maar gescheiden per latende school.* • *Alleen ontvangende scholen waar de kandidaat leerling zich heeft aangemeld, hebben inzage in de gegevens van deze leerling.* • *Er is geen inzage in persoonsgegevens over leerlingen van de gehele regio (ten behoeve van statistiek bijvoorbeeld).*
	Is (contractueel) geregeld dat er alleen scholen gebruikmaken van de diensten van deze leverancier? • *Alleen scholen mogen met het BSN gegevens uitwisselen.* • *Geen koppeling met andere dossiers of dienstverleners.* • *Andere organisaties dan scholen mogen geen gebruikmaken van de gegevens.*
	Worden de gegevens tijdelijk opgeslagen? • *Geen centrale database of postbus.* • *Tijdelijke opslag (vernietiging gegevens geborgd).* • *Opslag alleen ten behoeve van de uitwisseling vo en mbo.*
	Wordt gebruikgemaakt van de ‘gegevensstandaard VO-MBO-overstapdossier’?

3.4. Checklist deel C: Juridische afspraken met leveranciers

De school moet met iedere leverancier die gegevens ontvangt namens de school een bewerkersovereenkomst sluiten (zie paragraaf 3.2). Bijlage 1 bij dit document bevat een voorbeeld van zo’n bewerkersovereenkomst. Een leverancier kan ook een eigen model of sjabloon gebruiken, maar daar moeten dan wel een aantal wettelijk voorgeschreven elementen in staan. In de volgende checklist staan alle elementen die volgens de Wbp moeten terugkomen in de afspraken met de leverancier. Deze checklist is deels overgenomen uit het ‘Juridisch normenkader cloudservices’ van SURF.

Dit is de checklist voor afspraken met de leverancier die de uitwisselingsservice aanbiedt (dit kan de SIS-leverancier zijn, maar ook een aparte leverancier).

✓✗	**WAT DE WET VOORSCHRIJFT WAT DE ONDERWIJSINSTELLING MOET REGELEN**
	Volgens de wet moet er een overeenkomst zijn, liefst een schriftelijke. Is die er?
	Het moet duidelijk zijn tussen wie er afspraken zijn, en waar de partijen bereikt kunnen worden. Zijn de partijen en hun contactgegevens opgenomen? • *De leverancier is bewerker en de school is de verantwoordelijke.* • *Zijn er andere partijen betrokken (bijvoorbeeld subleveranciers)? Zo ja, zijn die genoemd, wat is hun taak?*
	Is beschreven welke gegevens door de leverancier worden verwerkt? • *Voeg eventueel een specificatie als bijlage toe, of verwijs daarnaar .*
	Is er geregeld dat de leverancier alleen in opdracht van en volgens instructies van de school persoonsgegevens verwerkt? • *Is er een beschrijving wat de bewerker wel en niet mag? Bijvoorbeeld dat de gegevens alleen voor dienstverlening van de school mogen worden gebruikt?* • *Is vastgelegd dat hetzelfde geldt voor eventueel ingeschakelde subleveranciers?*

	De bewerker hoort gebonden te zijn aan een geheimhoudingsbeding. Is dat er? • *Is ook vastgelegd dat derden alleen na toestemming van de school toegang krijgen tot de persoonsgegevens?* • *Is afgesproken dat de school direct geïnformeerd wordt bij een verzoek van derden?*
	Bij de uitwisseling van gegevens in het kader van een overstap van de ene naar de andere school, mogen deze niet in een 'centrale postbus' worden opgeslagen of (eindeloos) worden bewaard. Is dit gegarandeerd door technische maatregelen of een bewaar- of vernietigingstermijn? En zijn er afspraken gemaakt over het beëindigen van de software/dienst? • *Krijgt de school zelf de gegevens aangeleverd of zijn ze te downloaden bij einde van de dienst?* • *Is afgesproken in welk bestandsformaat de school de gegevens krijgt?* • *Verwijdert de leverancier/bewerker de persoonsgegevens direct of enige tijd na beëindiging van de dienstverlening?*
	Adequate beveiligingsmaatregelen zijn noodzakelijk. Wordt de leverancier verplicht die te nemen? • *Zijn er specifieke normen of certificaten waaraan de leverancier/bewerker moet voldoen en zijn die benoemd?* • *Voor meer informatie zie de 'Richtsnoeren – Beveiliging van persoonsgegevens' die door het College bescherming persoonsgegevens zijn opgesteld.* • *Wordt er aangesloten bij een standaard, zie bijvoorbeeld de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002), die standaard is bij ict-dienstverleners?*[4]
	Is afgesproken dat de school de beveiligingsmaatregelen mag controleren (of een audit mag laten uitvoeren)? • *Is ook vastgelegd voor wie de kosten van zo'n controle zijn?* • *Of laat de leverancier/bewerker zelf een onafhankelijke audit uitvoeren en levert hij daarvan een rapport/verklaring op?*
	Een leverancier kan zaken ook uitbesteden aan subleveranciers, maar dat mag geen verschil maken voor de school. Dus: heeft de leverancier een (schriftelijke) overeenkomst gesloten met zijn subleverancier waarin dezelfde verplichtingen zijn opgenomen als die voor hemzelf gelden? • *Zijn de subleveranciers ook verplicht tot geheimhouding en adequate beveiliging?* • *Mogen de subleveranciers ook alleen in opdracht van de school gegevens verwerken?*

Tot slot een aantal uitgangspunten die niet in de wet staan, maar waar een school wel rekening mee moet houden om op een verantwoorde wijze gegevens te kunnen uitwisselen:

✓ ✗	**WAT AANGERADEN WORDT OM TE REGELEN MET EEN LEVERANCIER**
	Let op of de gegevens alleen binnen Europa (Europese Economische Ruimte) worden opgeslagen en verwerkt. Wanneer een leverancier een vestiging in de Verenigde Staten heeft, ga dan na of deze leverancier gecertificeerd is onder de Amerikaanse Safe Harbour Principles. Zo niet, dan gelden namelijk aanvullende, vaak complexe regels.
	Is de leverancier/bewerker contractueel verplicht om beveiligingsincidenten te melden? Is duidelijk dat de school (vroegtijdig) op de hoogte wordt gesteld? • *Wordt de leverancier verplicht om op eigen kosten alle benodigde maatregelen te nemen om gegevens veilig te stellen, tekortkomingen in beveiliging te herstellen en verder onbevoegde kennisneming, wijziging en verstrekking te voorkomen?* • *Zal de leverancier op verzoek van de school meewerken aan het informeren van de bevoegde autoriteiten en de leerlingen/ouders?*
	Back-ups van de gegevens zijn belangrijk. Zijn daar dingen over vastgelegd? Bijvoorbeeld over hoe vaak ze gemaakt worden? En over hoe snel of eenvoudig een back-up teruggezet kan worden?
	Is afgesproken dat de leverancier verplicht is om mee te werken aan verzoeken van leerlingen/ouders voor

[4] http://www.surf.nl/binaries/content/assets/surf/nl/2010/SURFIbo+Starterkit+informatiebeveiliging+definitief.pdf

	inzage/correctie/verwijdering van de persoonsgegevens? • *Als de leverancier daar een rechtstreeks verzoek voor krijgt, neemt die dan direct contact op met de school?* • *Wordt de school geïnformeerd als autoriteiten (zoals politie) om informatie vragen bij de leverancier?*
	Is er een boeteclausule als de leverancier/bewerker de afspraken niet nakomt? • *Is ook geregeld dat als de school aansprakelijk wordt gehouden voor een tekortkoming in de naleving van de bewerkersovereenkomst, dat verhaald kan worden op de leverancier?*
	Is afgesproken dat school en leverancier de Wet bescherming persoonsgegevens volledig en zorgvuldig nakomen? • *Het klinkt vreemd, maar het kan in het kader van de bewustwording soms helpen om letterlijk te benoemen dat iedereen de wet zal nakomen.*
	Het is raadzaam op te nemen dat Nederlands recht van toepassing is op de overeenkomst en ook welke rechter bevoegd is. Is dat gebeurd? • *Zo niet: is duidelijk welk recht van toepassing is en welke rechters bevoegd zijn te oordelen over een geschil met de leverancier?*

4. Beveiligingseisen en maatregelen

4.1. Algemeen

Binnen systeembeveiliging zijn er drie kernbegrippen. Deze worden samen afgekort de BIV-classificatie genoemd:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid

Daarnaast is controleerbaarheid toegevoegd als vierde criterium.

Beveiligingseisen en maatregelen kunnen aan een viertal kwaliteitsaspecten worden getoetst:

Beschikbaarheid: de mate waarin beheersmaatregelen de continuïteit en ongestoorde voortgang van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de IT-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar verschillende technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Controleerbaarheid: de mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de IT-dienstverlening.
Deelaspecten hiervan zijn:

- Testbaarheid: de mate waarin de integere werking van de IT-dienstverlening te testen is;
- Meetbaarheid: zijn er voldoende meet- en controlepunten aanwezig;
- Verifieerbaarheid: de mate waarin de integere werking van een IT-dienstverlening te verifiëren is.

4.2. Checklist deel D: Beveiliging instellingen

Als je als mbo-instelling gebruikmaakt van een leverancier die een uitwisselingsservice biedt, dan is het het eenvoudigst om deze leverancier te verplichten om zich te certificeren voor de standaard voor uitwisseling van persoonsgegevens. Dat kan met het Certificeringsschema Edukoppeling (zie paragraaf 1.4). Heb je als

onderwijsinstelling zelf een dienst ontwikkeld die voorziet in uitwisseling? Dan is het raadzaam om zelf te voldoen aan deze standaard. Mocht je als onderwijsinstelling of je leverancier niet aan Edukoppeling kunnen of willen voldoen, dan kun je de checklist gebruiken van paragraaf 4.3.

Voldoe je als onderwijsinstelling wel aan Edukoppeling, en geldt dat ook voor de leverancier? Dan geeft de checklist hieronder een opsomming van waar de onderwijsinstelling zelf aan moet denken.

De letter in de eerste kolom verwijst naar het begrip waaraan de vraag refereert: beschikbaarheid, integriteit, vertrouwelijkheid, controleerbaarheid.

✓✗	**Beveiliging van organisatie, proces en techniek geldend voor de onderwijsinstelling**
C	Is er een beveiligingsbeleid, is dat voldoende bekend en up-to-date? • *Wordt bij het beveiligingsbeleid gebruikgemaakt van een herhalen/terugkerend proces, zoals bijvoorbeeld de vier fasen van de Demingcirkel (plan-do-check-act) zodat het beleid actueel blijft?* • *Een ISO- en/of NEN-certificering is niet verplicht, maar dekt wel al een groot aantal basisbeveiligingsthema's af. Met name ISO 27001 of ISO 27002 vormen een goede start voor een beveiligingsbewuste organisatie.* • *Is er bewustwording binnen de eigen organisatie?*
C	Vinden er reguliere (security)audits plaats? • *Dit kunnen self-assessments zijn, maar ook peer-audits of externe audits* • *Een audit geeft inzicht in procesbeschrijvingen, status van de ICT-infrastructuur, opvolging van de beschreven processen en procedures in de praktijk.*
B	Zijn er reguliere basisbeveiligingsscans op de eigen hard- en software? • *Reguliere scans vormen een goed middel om bekende veiligheidsgaten te vinden. Ook al maakt de instelling gebruik van een leverancier, het is goed te testen hoe het gebruik van de programmatuur binnen de onderwijsinstelling gaat.* • *Door minimaal elk kwartaal een up-to-date gehouden scan uit te voeren, worden de grootste softwarelekken snel gevonden.*
V	Is duidelijk hoe binnen de instelling wordt omgegaan met back-up data? • *Back-upbestanden moeten veilig worden opgeslagen. Deze geback-upte data zijn immers even gevoelig als data die in het systeem aanwezig zijn. Het openstellen van back-updata aan onbevoegden is een groot en onzichtbaar risico. Dat moet je afdekken.*
I	Zijn er duidelijke afspraken over het verzamelen en de inhoud van het overdrachtsdossier? • *Een goed gestructureerd dossier waarvan de inhoud volledig vaststaat, voorkomt dat niet toelaatbare gegevens (onbedoeld) getransporteerd kunnen worden. Ook zorgt dit ervoor dat dossiers goed verwerkt kunnen worden tussen de systemen.*
V	Zijn er duidelijke afspraken over de dossieroverdracht? • *Een veilige overdracht van dossiers valt of staat met het duidelijk vastleggen hoe dossiers getransporteerd moeten worden en welke functionele, technische en functionele eisen hierbij komen kijken. Als hier geen goede afspraken over zijn, dan is er een risico dat dossiers in verkeerde handen kunnen vallen of dat het transport onverwachts uitvalt.*
V	Zijn de gebruikers van het systeem bij de school voldoende opgeleid voor het gebruik ervan? Wordt dit afgedwongen? • *Gedegen kennis van het systeem en de procedures zorgt ervoor dat gebruikers minder fouten maken. Dat beperkt de kans op het lekken van gegevens uit het systeem. Tevens voorkomt voldoende opleiding vragen van gebruikers en verbetert dit de kwaliteit van de informatie in het systeem.* • *In het informatiebeveiligingsbeleid of de arbeidsovereenkomst is opgenomen dat iedereen zich aan de instructies houdt.*
I en V	Zijn de gebruikers van het systeem zich voldoende bewust van ict-veiligheid en de daarbij horende gedragsregels? • *Een gedegen bewustzijn van een aantal basisregels voor ict-veiligheid is cruciaal bij het gebruik van*

	webdiensten. Hiermee voorkom je een groot deel van de veelvoorkomende beveiligingsproblemen. • *Kies veilige wachtwoorden.* • *Maak gebruik van een autorisatiematrix die rechten toekent aan de verschillende categorieën gebruikers.* • *Log uit als het systeem niet wordt gebruikt* • *Gebruik alleen vertrouwde wifi-netwerken (zoals eduroam) en apparaten om mee in te loggen*
V	Is er een overkoepelende organisatie die het dossier en overdrachtsproces beheert en bewaakt? • *Een overkoepelende organisatie draagt zorg voor de dossier- en overdrachtsstandaarden en houdt de ontwikkelingen, beheer en veiligheid van overdrachten nauwlettend in de gaten.*
V	Heeft de school inzage in de informatiestromen bij de dossieroverdracht? • *Het is belangrijk om te weten of er naast de latende en ontvangende school nog andere partijen zijn die inzage hebben in over te dragen dossiers of zelfs de mogelijkheid hebben om de dossiers te bewerken. Dat is namelijk niet toegestaan.*
V	Is er voldoende duidelijk aan welke systemen het systeem van de leverancier gekoppeld is? • *Bijvoorbeeld: met Google Analytics. Maar daarbij kan het gebeuren dat je privacygevoelige gegevens deelt met Google.* • *Of meer algemeen: er worden rapportages gedraaid met een externe webdienst, maar op die manier worden (incomplete) dossiers naar een derde gestuurd.* • *Dit zijn niet per definitie 'illegale' handelingen, maar het is wel noodzakelijk dat school en leverancier hierover afspraken maken.*

V	Hebben de school en de leverancier een duidelijke gebruikersautorisatieprocedure?
	• *Wie mag accounts (laten) aanmaken?*
	• *Welke procedure wordt gevolgd voor het intrekken van accounts?*
	• *Wie bepaalt welke rechten er worden verleend?*
	  ○ *Hier geldt het principe van het zo laag mogelijke privilegeniveau.*
	• *Vindt er reguliere accountcontrole plaats?*
	• *Op welke wijze worden accountgegevens verstrekt?*
	  ○ *Dit moet veilig gebeuren (persoonlijke post, telefoon, sms), op zo'n manier dat derden niet de beschikking kunnen krijgen over gebruikersaccounts.*
	• *De juiste autorisatieprocedure voorkomt dat de verkeerde gebruikers en rechten worden ingesteld. Ook voorkomt dit dat gebruikers die geen toegang meer mogen hebben toch nog toegang houden.*
	• *Is er bijvoorbeeld een autorisatiematrix die inzicht geeft in alle toegangsrechten? Niet iedere docent of mentor hoeft inzage te hebben in overstapgegevens.*
	• *Is het vierogenbeginsel toegepast? (Zijn er meerdere personen betrokken bij het opstellen van de autorisatiematrix? Dit kan belangrijk zijn bij bijvoorbeeld toetsen en examens (die gegevens mogen niet eenzijdig te wijzigen zijn.)*

V	Ondertekenen personeel, externen en andere partijen die toegang hebben tot de gegevens in het systeem van de leverancier een geheimhoudingsverklaring? • *Een geheimhoudingsverklaring zorgt ervoor dat boven het reeds wettelijk bepaalde, partijen ervan doordrongen worden dat zij te maken hebben met gevoelige gegevens en dat het lekken ervan op sancties kan komen te staan.*
C	Wordt er afdoende logging bijgehouden in het eigen computersysteem (toegang tot het systeem van de leverancier verloopt via het interne netwerk)? En wordt deze ook veilig bewaard? • *Logging bestaat uit o.a. gebruikersacties, dossiertransacties, login-pogingen, systeemmeldingen, etc.* • *Logging is essentieel om incidenten te kunnen oplossen. Daarnaast is het in het geval van een forensisch onderzoek noodzakelijk om bewijslast te kunnen verzamelen.* • *Om logging betrouwbaar te maken, dient de logging vanuit het systeem veilig weggeschreven te worden, zodat kwaadwillenden de logging niet kunnen aanpassen.*

4.3. Checklist deel E: Beveiliging leveranciers[5]

Mocht u of uw leverancier niet aan het Certificeringsschema Edukoppeling kunnen of willen voldoen, dan kunt u de volgende checklist gebruiken om na te gaan of de leverancier de juiste maatregelen heeft getroffen.

Hierbij is dus uitdrukkelijk gebruikgemaakt van het Certificeringsschema waaraan een leverancier binnen Edukoppeling moet voldoen (“aan welke eisen moet een leverancier voldoen”). Maar dit schema is niet geschikt om zonder meer te gebruiken door een onderwijsinstelling. Daarom is deze checklist een vertaling van dat certificeringsschema voor onderwijsinstellingen (“waar moet ik als onderwijsinstelling op letten wat geregeld moet zijn”). De essentie van het schema is daarop vertaald naar een lijst van eisen die voor de onderwijsinstelling geschikt en begrijpelijk is.

✓ ✗	**Beveiliging van organisatie, proces en techniek geldend voor de leverancier**
	Heeft de leverancier of de onderwijsinstelling officieel erkende ISO- en/of NEN-beveiligingscertificeringen? • *Is niet verplicht, maar dekt wel al een groot aantal basale beveiligingsthema’s af. Met name ISO 27001 of ISO 27002 vormen een goede start voor een beveiligingsbewuste organisatie.* • *Is er bewustwording binnen de eigen organisatie?*
	Vinden er reguliere (security)audits plaats? Zo ja, kan de school de rapporten inzien? • *Een audit geeft inzicht in procesbeschrijvingen, status van de ict-infrastructuur, opvolging van de beschreven processen en procedures in de praktijk.* • *De school kan als afnemer de leverancier hiertoe verplichten.* • *De school kan als afnemer van de leverancier een TPM-verklaring (Third Party Mededeling) eisen.* • *Bij een redelijk vermoeden dat de leverancier zijn afspraken niet nakomt kan de school een eigen onderzoek starten naar het handelen van de leverancier.*
	Laat de school of leverancier op reguliere basis beveiligingsscans uitvoeren op het hostingplatform en de software? • *Reguliere scans vormen een goed middel om bekende veiligheidsgaten te vinden. Door minimaal elk kwartaal een up-to-date gehouden scan zijn werk te laten doen worden de softwarelekken snel gevonden.*
	Is het duidelijk hoe de school of leverancier omgaat met back-updata? • *Worden er regelmatig back-ups gemaakt?* • *Worden deze data veilig opgeslagen?*
	Zijn er duidelijke afspraken over de inhoud van het overdrachtsdossier? • *Een goed gestructureerd dossier waarvan de inhoud volledig vaststaat, voorkomt dat gegevens (onbedoeld) getransporteerd kunnen worden. Tevens zorgt dit ervoor dat dossiers goed verwerkt kunnen worden tussen de systemen.* • *Wordt de gegevensstandaard VO-MBO-overstapdossier gebruikt?*
	Zijn er duidelijke afspraken over de dossieroverdracht? • *Een veilige overdracht van dossiers valt of staat met het duidelijk vastleggen hoe dossiers getransporteerd moeten worden en welke functionele, technische en functionele eisen hierbij komen kijken. Als hier geen goede afspraken over bestaan, is er een risico dat dossiers in verkeerde handen vallen of dat het transport onverwachts uitvalt.*
	Wordt de toegang tot het systeem strikt via https ontsloten? • *Het gebruik van https in de URL zorgt ervoor dat derden de communicatie tussen gebruiker en systeem niet kunnen meelezen. Denk aan wachtwoorden en leerlinginformatie die via het systeem geraadpleegd kunnen worden.*
	Zijn de gebruikers van het systeem voldoende opgeleid voor het gebruik ervan? • *Gedegen kennis van het systeem en de procedures zorgt ervoor gebruikers minder fouten maken*

[5] NB: Dit kan dus ook de instelling zelf zijn, indien het systeem ontwikkeld en onderhouden wordt door de onderwijsinstelling.

	en beperkt dus de kans op het lekken van gegevens uit het systeem. Tevens voorkomt voldoende opleiding vragen van gebruikers en verbetert dit de kwaliteit van de informatie in het systeem.
	Zijn de gebruikers van het systeem bij zowel de school als de leverancier zich voldoende bewust van ict-veiligheid en de daarbij horende gedragsregels? • *Een gedegen bewustzijn van een aantal basisregels voor ict-veiligheid is cruciaal bij het gebruik van webdiensten. Hiermee wordt een groot deel van de veelvoorkomende beveiligingsproblemen voorkomen.* • *Kies veilige wachtwoorden en gebruik liefst twofactor-authenticatie (bijv. wachtwoord + sms)* • *Log uit als het systeem niet wordt gebruikt* • *Gebruik alleen vertrouwde wifi-netwerken (zoals eduroam) en apparaten om mee in te loggen*
	Wordt het overdrachtsdossier versleuteld tussen scholen overgedragen? Zo ja, zijn er afspraken over de versleuteling van het dossier? • *Versleutelde overdracht van dossiers beperkt het risico dat derden kunnen meelezen. Afspraken met de leverancier hierover zijn belangrijk.*
	Als de dossieroverdracht plaatsvindt over het internet, worden hiervoor dan beveiligingsvoorzieningen getroffen? *Bijvoorbeeld:* • *Beveiligde tunnel tussen leveranciers onderling* • *Versleutelde webservices met verificatie van zowel latende als ontvangende leverancier/school* • *Versleuteld e-mailverkeer (PGP/GPG)* • *Versleuteld FTP-verkeer met verificatie van zowel latende als ontvangende leverancier/school*
	Is in het proces geborgd dat een overdrachtsdossier alleen terecht kan komen bij de ontvanger die de latende school heeft aangegeven? • *Het mag in geen geval zo zijn dat een dossier bij de verkeerde school belandt. Hiervoor moeten zowel in het proces als in de techniek bij de leverancier waarborgen zijn ingebouwd.*
	Is het duidelijk hoe de leverancier garandeert dat gegevens op zijn gedeelde systeem niet met elkaar vermengd raken? (data school 1 komt ongevraagd bij school 2 terecht) • *Data van verschillende scholen mogen nooit bij een leverancier vermengd raken. De leverancier moet dit in processen en techniek geborgd hebben.* • *Zijn er gescheiden omgevingen bij de leverancier voor de verschillende scholen? (niet één grote database)*
	Heeft de school inzage in de informatiestromen bij de dossieroverdracht? Vindt er tijdens of na de overdacht van een dossier nog verrijking plaats van het dossier met bijvoorbeeld medische gegevens? • *Het is belangrijk om te weten of er naast de latende en ontvangende school nog andere partijen zijn die inzage hebben in over te dragen dossiers of zelfs de mogelijkheid hebben om de dossiers te bewerken. Dat is namelijk verboden.* • *Het is verstandig dat de school hier inzage in heeft en weet wat er met haar gegevens gebeurt.*
	Is er voldoende duidelijk aan welke systemen het systeem van de leverancier gekoppeld is? • *Bijvoorbeeld: met Google Analytics. Maar daarbij kan het gebeuren dat je privacygevoelige gegevens deelt met Google.* • *Of meer algemeen: er worden rapportages gedraaid met een externe webdienst, maar op die manier worden (incomplete) dossiers naar een derde gestuurd.* *Dit zijn niet per definitie 'illegale' handelingen, maar het is wel noodzakelijk dat school en leverancier hierover afspraken maken.*
	Zijn er tussen de school en leverancier afspraken over de bewaartermijn van leerlinggegevens? • *Het is juridisch niet toegestaan om persoonsgegevens oneindig te bewaren. Ook uit beveiligingsoogpunt is lang bewaren niet wenselijk. Mochten er – om wat voor reden ook – toch gegevens lekken, dan blijven de gevolgen beperkt als de set aan gegevens beperkt was.*
	Zijn er met de leverancier afspraken over de inzet van data uit het systeem? • *De leverancier mag geen productiedata gebruiken voor testdoeleinden. Testsystemen worden vaak*

	met minder beveiligingseisen ingezet. Dat opent de achterdeur naar productiegegevens. • *Testdata kunnen bestaan uit gepseudonimiseerde of geanonimiseerde productiedata. Hierdoor lijkt de gegevensset nog wel op productie, maar is deze niet meer terug te herleiden tot echte personen.*
	Heeft de leverancier de productie- en testomgevingen van het systeem voldoende van elkaar gescheiden? • *Het mag nooit gebeuren dat een gebruiker vanaf de testomgeving per ongeluk toch productiegegevens kan aanpassen of andersom. Deze omgevingen mogen niet met elkaar in contact komen. Als gebruikers van omgeving wisselen moeten ze daarvan een duidelijke melding krijgen, en data moeten gescheiden van elkaar opgeslagen worden.*

	Hebben de school en de leverancier een duidelijke gebruikersautorisatie-procedure ingebouwd in de applicatie?
	• *Wie mag accounts (laten) aanmaken?*
	• *Welke procedure wordt gevolgd voor het intrekken van accounts?*
	• *Wie bepaalt welke rechten er worden verleend?*
	  ○ *Hier geldt het principe van het zo laag mogelijke privilegeniveau.*
	• *Vindt er reguliere accountcontrole plaats?*
	• *Op welke wijze worden accountgegevens verstrekt?*
	  ○ *Die moet veilig gebeuren (persoonlijke post, telefoon, sms), zodat derden niet de beschikking kunnen krijgen over een gebruikersaccount.*
	• *De juiste autorisatieprocedure voorkomt dat de verkeerde gebruikers en rechten worden ingesteld, of dat gebruikers die geen toegang meer mogen hebben toch nog toegang houden.*

	Ondertekenen personeel, externen en andere partijen die toegang hebben tot de gegevens in het systeem van de leverancier een geheimhoudingsverklaring? • *Een geheimhoudingsverklaring zorgt ervoor dat boven het reeds wettelijk bepaalde, partijen ervan doordrongen worden dat zij te maken hebben met gevoelige gegevens en dat het lekken ervan op sancties kan komen te staan.*
	Wordt er genoeg logging bijgehouden in het systeem? En wordt deze ook veilig bewaard? • *Logging bestaat uit o.a. gebruikersacties, dossiertransacties, loginpogingen, systeemmeldingen, etc.* • *Logging is essentieel om incidenten te kunnen oplossen. Daarnaast is logging in het geval van een forensisch onderzoek noodzakelijk om bewijslast te kunnen verzamelen.* • *Om logging betrouwbaar te maken moet de logging vanuit het systeem veilig weggeschreven te worden, zodat kwaadwillenden deze niet kunnen aanpassen.*
	Zijn er afspraken tussen school en leverancier over beschikbaarheid van de dienst? • *Een van de pilaren van een beveiligingsbeleid is beschikbaarheid. Een dienst die offline is, is schadelijk voor de continuïteit dus er dienen strakke afspraken tussen school en leverancier te zijn over beschikbaarheid van de dienst. Beschikbaarheid kun je uitdrukken in een percentage per maand. Bijvoorbeeld: tenminste 99,98% van de tijdsperiode is de dienst beschikbaar.* • *School en leverancier hebben gedefinieerd hoe beschikbaarheid wordt gemeten en wat beschikbaarheid van de dienst is. Hierbij spreken de partijen af welk moment als begin en als eindtijd van een verstoring van de dienstverlening wordt genomen. Deze tijden hebben invloed op het beschikbaarheidspercentage.* • *School en leverancier hebben gedefinieerd wat er gebeurt als het beschikbaarheidspercentage structureel te laag is. Hierbij kan een malusregeling van toepassing zijn, waaruit schadevergoeding kan volgen of bijvoorbeeld ontbinding van het contract.*
	Zijn er afspraken tussen school en leverancier over hersteltijden van storingen? • *Als de dienst plat ligt, dan is het goed om te weten binnen hoeveel tijd de dienst normaliter weer functioneert. Als de leverancier dit niet haalt, is het vervolgens mogelijk het incident hogerop te spelen. Hierdoor is het mogelijk de druk bij de leverancier erop te houden.*
	Zijn er afspraken tussen school en leverancier over procedures voor het melden van incidenten? • *Mochten er problemen ontstaan – of het nu gaat om beveiligingsissues of om functionele problemen – er moet een centrale plek zijn waar deze gemeld kunnen worden. Ook zijn er duidelijke afspraken*

	nodig over reactie- en oplostijden. • *De leverancier is verplicht om beveiligingsincidenten onmiddellijk te melden bij de school.*
	Zijn er afspraken tussen school en leverancier over incidentrapportages? • *Ontstane incidenten die betrekking hebben gehad op de dienstverlening moeten aan de school verantwoord worden. De leverancier moet dan ook periodiek incidentrapportages opleveren met daarin oorzaak, gevolg, oplossing en doorlooptijd.*

Bijlage – Voorbeeld bewerkersovereenkomst

Dit is een modelovereenkomst die dient als voorbeeld.

Onderwijsinstellingen en leveranciers kunnen met dit model zelf nadere afspraken maken naar aanleiding van iedere specifieke dienst. Aan de inhoud van dit model kunnen geen garanties of rechten worden ontleend.

In dit model is niet ingegaan op de concept Europese "Algemene Verordening Gegevensbescherming".

Ondergetekenden:

[**Onderwijsinstelling**], gevestigd en kantoorhoudende @ADRES@, hierbij vertegenwoordigd door @vertegenwoordigingsbevoegde@, @functie@, hierna te noemen: "**Onderwijsinstelling**",

en

[**leverancier**], gevestigd en kantoorhoudende aan de @ADRES@, hierbij rechtsgeldig vertegenwoordigd door @vertegenwoordigingsbevoegde@, @functie@, hierna te noemen: "**Leverancier**",

hierna gezamenlijk te noemen: "Partijen",

overwegende dat:

a) Onderwijsinstelling gebruik wenst te maken van de Software-as-a-Service--dienstverlening van Leverancier *[OPTIONEEL:]* en daartoe een Overeenkomst van [datum] (hierna: Overeenkomst) met Leverancier heeft afgesloten;
b) Onderwijsinstelling in het kader van de uitvoering van de Overeenkomst (persoons)gegevens van de leerlingen, diens ouders en/of relaties van Onderwijsinstelling plaatst in de SaaS-oplossing van Leverancier;
c) Partijen afspraken rondom uitwisseling van (persoons)gegevens in deze Bewerkersovereenkomst willen vastleggen;

verklaren te zijn overeengekomen als volgt:

Artikel 1. DEFINITIES

1.1 Persoonsgegevens: elk gegeven betreffende of herleidbaar tot een geïdentificeerde of identificeerbare natuurlijke persoon;
1.2 Gegevens: alle andere gegevens (data) niet zijnde persoonsgegevens;
1.3 Betrokkene: degene op wie de Persoonsgegevens betrekking hebben. In geval van een kind jonger dan 16 jaar wordt met Betrokkene diens wettelijk vertegenwoordiger(s) bedoeld.
1.4 SaaS-oplossing: Software-as-a-Service-oplossing; de door Leverancier geboden dienst;
1.5 [naam SaaS-oplossing]: [omschrijving dienst van Leverancier].
1.6 Bewerkersovereenkomst: deze overeenkomst tussen Onderwijsinstelling en Leverancier;

1.7 Overeenkomst: Overeenkomst tussen Leverancier en Onderwijsinstelling betrekking hebbend op de door Leverancier aan Onderwijsinstelling geleverde dienst(en).
1.8 Verwerken: elk soort handeling (of deel daarvan) met betrekking tot Persoonsgegevens.
1.9 Europese Economische Ruimte: alle landen van de Europese Unie, Liechtenstein, Noorwegen en IJsland.
1.10 Wbp: wet bescherming persoonsgegevens.

Artikel 2. Voorwerp van deze Bewerkersovereenkomst

2.1 Leverancier levert [naam SaaS-oplossing] aan Onderwijsinstelling.
2.2 Onderwijsinstelling is verantwoordelijke ten aanzien van de aan Leverancier verstrekte en te verstrekken (persoons)gegevens. Leverancier handelt als bewerker in opdracht van Onderwijsinstelling en verwerkt de (persoons)gegevens slechts in opdracht van Onderwijsinstelling.
2.3 De door Onderwijsinstelling aan Leverancier geleverde (persoons)gegevens worden geleverd ten behoeve van [naam SaaS-oplossing]. Voor zover Partijen reeds een Overeenkomst hebben gesloten ten aanzien van de SaaS-dienst, gelden de bepalingen van deze Bewerkersovereenkomst als aanvulling daarop.
2.4 [OPTIONEEL:]De in het kader van deze overeenkomst uitgewisselde (persoons)gegevens zijn beperkt tot [OMSCHRIJVING of OPSOMMING IN APARTE BIJLAGE].
2.5 Leverancier zal de ontvangen (persoons)gegevens uitsluitend verwerken ten behoeve van de levering van [naam SaaS-oplossing] aan Onderwijsinstelling en alleen voor zover het verwerken van die gegevens strikt noodzakelijk is ten behoeve van de dienstverlening van Leverancier.
2.6 Alle (intellectuele) eigendomsrechten, auteursrecht en databankenrecht inbegrepen, op de geleverde (persoons)gegevens, blijven te allen tijde berusten bij de Onderwijsinstelling (dan wel de docent of Betrokkene).
2.7 Partijen komen de Wet bescherming persoonsgegevens na. Voor zover de afspraken tussen Partijen niet voorzien in wettelijk vereiste regelingen, komen Partijen overeen te handelen in overeenstemming met de toepasselijke wet- en regelgeving op het gebied van de bescherming van (persoons)gegevens.

Artikel 3. Looptijd Bewerkersovereenkomst

3.1 De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen partijen gesloten Overeenkomst. In het geval dat de dienstverlening van Leverancier aan Onderwijsinstelling (nog) voortduurt, loopt deze Bewerkersovereenkomst door.
3.2 Na (tussentijdse) beëindiging van deze Bewerkersovereenkomst, blijven de bepalingen van artikelen 2, 3.3, 4 en 5 onverkort van toepassing.
3.3 Na beëindiging van de Overeenkomst, en/of na beëindiging van de dienstverlening aan Onderwijsinstelling, is Leverancier gehouden om binnen 30 dagen na beëindiging de door Leverancier verstrekte (persoons)gegevens terug te geven (dan wel om Onderwijsinstelling in de gelegenheid te stellen deze gegevens digitaal te verkrijgen). Eventuele resterende (kopieën van) (persoons)gegevens en/of back-ups dienen daarop door Leverancier te worden vernietigd.

Artikel 4. Beveiligingseisen

4.1 Leverancier zal zorgdragen voor passende technische en organisatorische maatregelen om (persoons)gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De te nemen maatregelen sluiten aan bij de stand van de techniek en de kosten van de tenuitvoerlegging.
4.2 De veiligheidsmaatregelen bieden een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

4.3 De veiligheidsmaatregelen zijn adequaat en voldoen aan de relevante standaarden en kwaliteitseisen.
4.4 [OPTIONEEL:]Leverancier heeft de volgende beveiligingsmaatregelen geïmplementeerd: [opsomming].
4.5 Leverancier is verantwoordelijk voor het regelen van adequaat beveiligde toegang tot de (persoons)gegevens door Onderwijsinstelling.
4.6 Onderwijsinstelling heeft het recht om in overleg met Leverancier de door Leverancier genomen technische en organisatorische (beveiligings)maatregelen - op kosten van Onderwijsinstelling - te (laten) toetsen door een daartoe gecertificeerd en onafhankelijk auditor. Leverancier heeft alsdan het recht om deze audit – al dan niet op eigen initiatief – uit te laten voeren door een door Leverancier in te schakelen onafhankelijk gecertificeerd auditor die een derdenverklaring afgeeft. Onderwijsinstelling wordt – al dan niet op hoofdlijnen – geïnformeerd over de uitkomsten.
4.7 Leverancier stelt Onderwijsinstelling omgaand op de hoogte over ieder veiligheidsincident.

Artikel 5. Geheimhouding en vertrouwelijkheid

5.1 Op Leverancier rust ingevolge artikel 12 van de Wbp een wettelijke geheimhoudingsverplichting. Leverancier is gehouden de ontvangen gegevens als vertrouwelijk te behandelen.
5.2 Leverancier verplicht zijn (oud) werknemers en/of onderaannemers tot geheimhouding met betrekking tot alle (persoons)gegevens waarvan zij met betrekking tot de levering van [naam SaaS-oplossing] kennisnemen.
5.3 Ingeval Leverancier een derde inschakelt bij de dienstverlening, dan dient de Onderwijsinstelling hier uitdrukkelijk mee in te stemmen, voorafgaand aan het sluiten van een overeenkomst met de derde.
5.4 De verstrekte (persoons)gegevens worden door Leverancier niet zonder voorafgaande toestemming van Onderwijsinstelling aan derden ter beschikking gesteld, tenzij Leverancier daartoe krachtens enige wetsbepaling, voorschrift of andere regelgeving verplicht is, of indien de bekendmaking en/of verstrekking in het kader van dienstverlening noodzakelijk is.
5.5 Indien Leverancier een verzoek of een bevel van een Nederlandse of buitenlandse toezichthouder of een opsporings-, strafvorderings- of nationale veiligheidsinstantie ontvangt om (inzage in) (persoons)gegevens te verschaffen, waaronder maar niet beperkt tot een verzoek op grond van de USA Patriot Act, dan zal Leverancier de Onderwijsinstelling onverwijld informeren. Bij de behandeling van het verzoek of bevel zal de Leverancier alle instructies van de Onderwijsinstelling 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.
5.6 Voor zover Leverancier (persoons)gegevens aan anderen dan Onderwijsinstelling levert, zal Leverancier met deze derde gelijksoortige bepalingen als in deze bewerkersovereenkomst omtrent de verwerking van (persoons)gegevens overeenkomen, tenzij sprake is van een omstandigheid als genoemd in artikel 5.4.
5.7 Leverancier zal zijn volledige medewerking verlenen in geval dat een Betrokkene zijn rechten uitoefent op grond van de Wbp of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens. Indien deze Betrokkene met betrekking tot de uitvoering van zijn rechten onder de Wbp direct contact opneemt met Leverancier, dan verwijst Leverancier Betrokkene in eerste instantie door naar Onderwijsinstelling.
5.8 Leverancier draagt er zorg voor dat de ontvangen (persoons)gegevens worden verwerkt (opgeslagen) binnen de Europese Economische Ruimte. Indien dit niet het geval is, mogen de (persoons)gegevens slechts worden verwerkt in een veilig derde land voor zover de wet dit toestaat (een land dat een passend beschermingsniveau biedt). Leverancier zal Onderwijsinstelling (vooraf) actief informeren indien de gegevens buiten de Europese Economische Ruimte worden verwerkt.
5.9 Bij elke schending van de geheimhoudingsverplichting van Leverancier, is deze aan Onderwijsinstelling een direct opeisbare boete van (maximaal) € 50.000,= per overtreding verschuldigd, onverlet de overige rechten op schadevergoeding.
5.10 Leverancier zal Onderwijsinstelling terstond op de hoogte stellen van iedere kennisneming, verstrekking of andere vorm van verwerken van de gegevens, die plaatsvindt in strijd met dit artikel.

Artikel 6. Aansprakelijkheid

6.1 Leverancier is aansprakelijk voor schade of nadeel, voortvloeiende uit het niet nakomen van deze Bewerkersovereenkomst, voorschriften bij of krachtens wet- en regelgeving aangaande de bescherming van (persoons)gegevens, voor zover de schade of het nadeel is ontstaan door de werkzaamheid als Leverancier voor Onderwijsinstelling.

6.2 Leverancier is gehouden tot het (onmiddellijk) beperken van schade en/of voorkomen van verder nadeel van Betrokkene en/of Onderwijsinstelling.

6.3 [OPTIONEEL:]De totale aansprakelijkheid van Opdrachtgever is beperkt tot het bedrag dat in het respectievelijke geval door de aansprakelijkheidsverzekeraar van Leverancier wordt vergoed.

Artikel 7. Algemeen

7.1 Bepalingen in de algemene voorwaarden, overeenkomsten of (mondelinge) afspraken tussen Partijen, met betrekking tot de bescherming van de verstrekte (persoons)gegevens, die afwijken van hetgeen in deze Bewerkersovereenkomst is geregeld, zijn niet van toepassing.

7.2 Op deze overeenkomst is Nederlands recht van toepassing. Bij een dispuut over de toepasselijkheid van Nederlands recht, zijn de bepalingen van de Dataprotectierichtlijn 95/46/EG (aanvullend) van toepassing.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling.	Leverancier.
Naam:	Naam:
Functie:	Functie:
Datum:	Datum: