Rijndijk 235
2394 CD Hazerswoude
Nederland

Telefoon +31 (0)71 3416911
Email noordbeek@noordbeek.com

Privacyscan Intergrip

Rapport van bevindingen inzake een Privacyscan van

De toepassing Intergrip binnen de keten vo-mbo

Definitieve versie: 1.00

Opdrachtgever	J. Bartling	saMBO-ICT
	E. Hooijer	Intergrip B.V.
Auteur	R. Paans	Noordbeek B.V.
	L.A.T. Benschop	
	A.J. Stroo	
Rapportnummer	MBOPIA6-1	
Classificatie	Openbaar	
Status	Definitief	
Datum	18 april 2016	
Bestandsnaam	Rapport MBOPIA6 Intergrip 2016	
KvK nummer	Rijnland 33265070	
BTW nummer	NL8203.45.180.B01	

Colofon

Opdrachtgever	J. Bartling, saMBO-ICT E. Hooijer, Intergrip
Contactpersoon	prof.dr.ir. R. Paans RE Directeur Telefoon 06 21 58 15 50 Email ronald.paans@noordbeek.com
Afzendergegevens	Noordbeek B.V. Rijndijk 235 2394 CD Hazerswoude http://www.noordbeek.com/
Auteurs	R. Paans L.A.T. Benschop A.J. Stroo
Kwaliteitscontrole	K.C. Schoon

Inhoud

1. Inleiding

Noordbeek heeft op 24 januari 2016 van de Stichting Kennisnet, namens saMBO-ict en Intergrip B.V., de opdracht gekregen om een onderzoek uit te voeren naar de privacyaspecten van het systeem Intergrip, in de vorm van een Privacy Impact Assessment (PIA). Hiermee wordt getoetst of het verzamelen en verwerken van persoonsgegevens voldoet aan het gestelde in de Wet bescherming persoonsgegevens (Wbp).

Het systeem Intergrip wordt in regionaal verband gebruikt voor de overdracht van gegevens over vo-leerlingen tussen het vo en mbo, over het algemeen binnen een Regionale Meld- en Coördinatiefunctie (RMC).

Het systeem speelt een belangrijke rol bij een soepele overstap van leerlingen vanuit het vo naar de mbo-instellingen en wordt door meer dan driekwart van de onderwijsinstellingen in Nederland gebruikt.

Noordbeek heeft het onderzoek naar de privacyaspecten uitgevoerd aan de hand van het normenkader opgenomen in de uitvraag van Stichting Kennisnet. Het normenkader is gebaseerd op de vereisten uit het certificeringsschema 1.1 van Edustandaard en gericht op de risico's voor de overdracht van persoonsgegevens tussen vo- en mbo-instellingen.

1.1. Toelichting op de overstap vo-mbo

Bij de overstap van het vo naar het mbo is het risico op Voortijdig Schoolverlaten (VSV) aanwezig. Om dit tegen te gaan legt de Overstap VO-MBO de verantwoordelijkheid voor de doorstroom van de leerlingen neer bij zowel het vo als het mbo. De vervolgkeuzes van de leerlingen worden geregistreerd in Intergrip. Met behulp van de Mbo-Check van de mbo-instellingen worden de statussen van de leerlingen teruggekoppeld aan het vo. Het is vervolgens aan het vo om ervoor te zorgen dat alle leerlingen bij vervolgonderwijs worden geplaatst.

Deze combinatie zorgt ervoor dat mogelijke risicoleerlingen vroegtijdig worden gesignaleerd. Bovendien kunnen zij via het systeem worden overgedragen aan Leerplicht of aan een van de trajectbureaus. De leerplichtmonitor bevat niet de inhoudelijke leerlingdossiers.

1.2. Toelichting op de applicaties VO-MBO en DDD

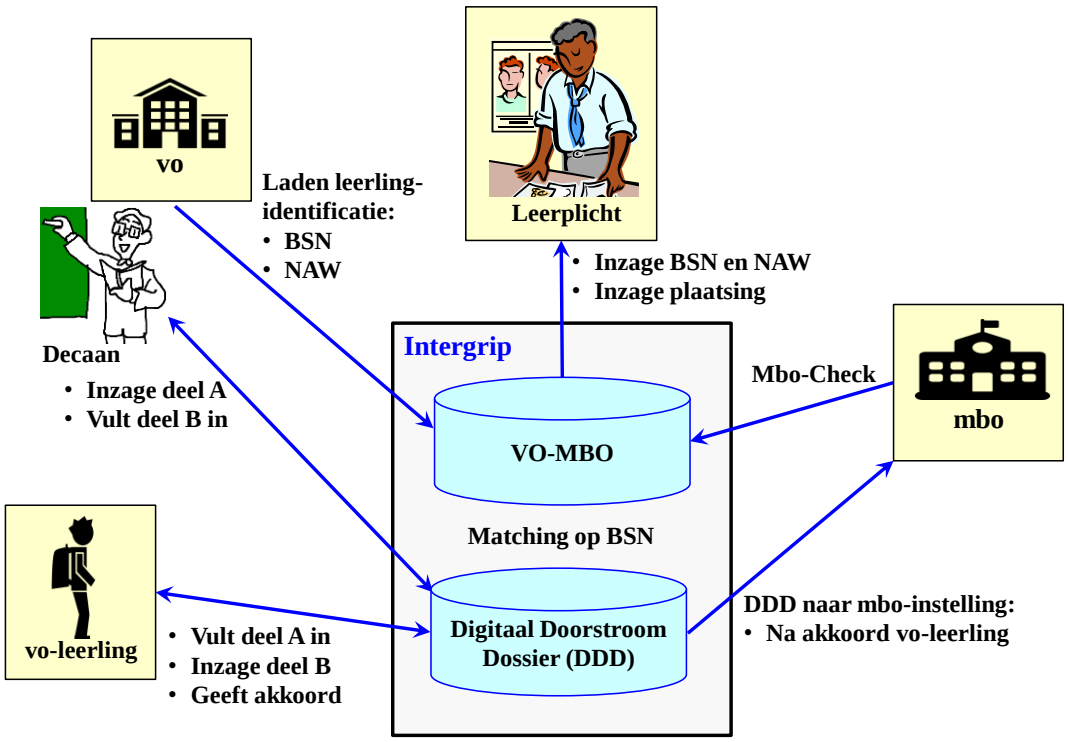
De vo-instelling start het proces door de leerlinggegevens te laden in de applicatie VO-MBO (zie Figuur 1). Dit zijn onder andere het Burgerservicenummer (BSN) als unieke identificatie en naam, adres en woonplaats (NAW). Op deze wijze wordt de leerling bekend gemaakt aan Intergrip.

Als de vo-leerling zich wil inschrijven bij een mbo-instelling wordt gebruik gemaakt van een separate applicatie, namelijk het inhoudelijk Digitaal Doorstroom Dossier (DDD). Dit bevat drie gedeelten:

- Deel A is het leerlinggedeelte. Dit wordt door de leerling zelf ingevuld en moet worden goedgekeurd door de ouder(s) of de wettelijke vertegenwoordiger(s);
- Deel B is het mentorgedeelte (deel B). De decaan of mentor controleert de inhoud van het leerlinggedeelte (Deel A) en vult daarna Deel B in;

- De leerling leest Deel B en ziet wat de mentor of decaan heeft vermeld. Vervolgens kan de leerling akkoord geven om het DDD naar de mbo-instelling te versturen. Zonder een expliciet akkoord van de leerling wordt het DDD niet verstuurd.

De mbo-instelling geeft een terugkoppeling via de Mbo-Check naar de applicatie VO-MBO. Hierin staat de status van de aanmelding.



Figuur 1

De inhoud van het DDD wordt vastgesteld in het landelijk halfjaarlijks overleg met de projectleiders in de regio's. Deze inhoud bestaat onder andere uit persoonsgegevens, aangevuld met informatie over de studieloopbaan en eventuele werkervaring.

Er is een DDD per aan te melden mbo-instelling. Als een leerling zich bij meerdere instellingen inschrijft zijn er meerdere DDD's.

2. Conclusie en adviezen

Noordbeek heeft de applicaties VO-MBO en DDD beoordeeld, inclusief het onderliggende platform en de procedures bij Intergrip, en de keten ‘vo – Intergrip – mbo’ bij twee Regionale Meld- en Coördinatiefuncties (RMC’s).

2.1. Conclusies

Met betrekking tot het stelsel van maatregelen voor de informatiebeveiliging en privacybescherming bij Intergrip zijn wij van mening:

> *Het platform voor VO-MBO en DDD, zoals dat door Intergrip wordt geboden, voldoet in hoofdlijnen aan de gestelde normen en standaarden voor informatiebeveiliging en privacybescherming.*

Onze detailbevindingen en adviezen zijn uitgewerkt in de hoofdstukken 3 en 4.

Met betrekking tot de onderwijsinstellingen die participeren in de keten ‘vo – Intergrip – mbo’ zijn wij van mening:

> *De privacybescherming voor de betreffende vo-leerlingen is in toereikende mate geborgd, zolang de applicaties VO-MBO en DDD door een onderwijsinstelling worden gebruikt zoals dat in opzet is bedoeld door Intergrip.*

2.2. Adviezen

Intergrip besteedt veel aandacht aan het inrichten van een gedegen stelsel van maatregelen voor het borgen van de privacy en het veilig leveren van haar diensten. Niettemin zijn tijdens ons onderzoek enkele verbeterpunten naar voren gekomen.

Dit resulteert in de volgende adviezen:

- Gebruik een model voor de bewerkersovereenkomst;
- Hanteer een classificatieschema voor de gegevens;
- Publiceer een privacystatement, bijvoorbeeld op de internetsite;
- Voer periodiek een gestructureerde risicoanalyse uit conform het actuele dreigingsbeeld;
- Voer periodiek security-audits uit;
- Test periodiek, of na majeure wijzigingen, de webapplicatiesoftware op mogelijke kwetsbaarheden voor cyberdreigingen;
- Voer periodiek een reconciliatie uit voor intern autorisatiebeheer;
- Maak afspraken over het periodiek beschikbaar stellen van de rapportages over de beschikbaarheid aan de afnemers.

3. Bevindingen en aandachtspunten

Het normenkader is gebaseerd op het certificeringsschema 1.1 van Edustandaard[1] en is opgesteld naar de risico's voor de overdracht van persoonsgegevens tussen vo- en mbo-instellingen. Het normenkader is omgezet naar een vragenlijst. Onze waarnemingen zijn per vraag in Hoofdstuk 4 in detail uitgewerkt.

De vragenlijst is opgedeeld in twee delen, namelijk de vragen gericht op privacybescherming en de vragen gericht op informatiebeveiliging.

In dit hoofdstuk bespreken wij alleen de vragen waarvoor wij bevindingen of aandachtspunten hebben geconstateerd.

Voor alle vragen die in dit hoofdstuk niet zijn genoemd voldoet het systeem Intergrip aan de norm.

[1] https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema-rosa-1/1.1/

3.1. Algemeen oordeel over Privacybescherming, Privacyvraag 7

Vraag 7

Wat is – in het licht van de hiervoor genoemde risico's - het algemeen oordeel van de auditor over de omgang met persoonsgegevens en privacy van studenten door Intergrip?

Antwoord 7

Het algemene oordeel van Noordbeek betreffende de privacybescherming is als volgt:

> *Het platform voor VO-MBO en DDD, zoals dat door Intergrip wordt geboden, voldoet in hoofdlijnen aan de gestelde normen en standaarden voor informatiebeveiliging en privacybescherming.*

De toereikenheid van de privacywaarborgen hangt mede af van de gebruikersorganisaties binnen de RMC's. Onze conclusie is als volgt:

> *De privacybescherming voor de betreffende vo-leerlingen is in toereikende mate geborgd, zolang de applicaties VO-MBO en DDD door een onderwijsinstelling worden gebruikt zoals dat in opzet is bedoeld door Intergrip.*

Tijdens het onderzoek is echter wel een aantal bevindingen en aandachtspunten naar voren gekomen. Deze leiden tot de volgende adviezen:

- Gebruik een model voor de bewerkersovereenkomst;
- Hanteer een classificatieschema voor de gegevens;
- Publiceer een privacystatement, bijvoorbeeld op de internetsite;
- Voer periodiek een gestructureerde risicoanalyse uit conform het actuele dreigingsbeeld;
- Voer periodiek security-audits uit;
- Test periodiek, of na majeure wijzigingen, de webapplicatiesoftware op mogelijke kwetsbaarheden voor cyberdreigingen;
- Voer periodiek een reconciliatie uit voor intern autorisatiebeheer;
- Maak afspraken over het periodiek beschikbaar stellen van de rapportages over de beschikbaarheid aan de afnemers.

Een deel van deze adviezen heeft betrekking op de gehele Intergrip-keten en zal als zodanig moeten worden opgepakt.

> *Advies: Overweeg een privacy statement op te nemen waarin de betrokkene helder en in begrijpelijke taal wordt geïnformeerd over de verwerking van de persoonsgegevens.*

> *Advies: Stel verbeterplannen op voor de geconstateerde aandachtspunten binnen de Intergrip-keten.*

> *Advies: Stel op basis van een gestructureerde risicoanalyse het dreigingsbeeld op, bepaal of de reeds getroffen beheersmaatregelen toereikend zijn en voer, waar nodig, aanvullende maatrelen door.*

3.2. Specificatie van de verplichte aanmeldingsgegevens

Vanuit het mbo worden de volgende aanmeldingsgegevens gevraagd:

Gegevensset (*=verplicht):

- BSN*
- Intakedatum
- Naam
- Postcode*
- Geboortedatum*
- Status*
- Opleiding*
- Crebo
- Leerweg
- Sector
- Niveau
- Locatie
- Reden beeindigen
- Deelnemernummer/leerlingnummer

Het BSN is een bijzonder persoonsgegeven dat wordt behandeld conform Wbp Art. 16, aangezien hierbij sprake is van het risico van identiteitsfraude. Het gebruik van het BSN valt onder de wet van 21 juli 2007, houdende algemene bepalingen betreffende de toekenning, het beheer en het gebruik van het burgerservicenummer (Wet algemene bepalingen burgerservicenummer, afgekort tot Wabb).

Het BSN wordt gebruikt conform Wabb Art. 11, lid 1, '*Bij het uitwisselen van persoonsgegevens tussen gebruikers onderling, waarbij een persoonsnummer wordt gebruikt als middel om persoonsgegevens in verband te brengen met een persoon aan wie een burgerservicenummer is toegekend, wordt het burgerservicenummer van die persoon vermeld.*'

De naam en geboortedatum zijn reguliere persoonsgegevens conform Wbp Art. 1, lid a.

De overige verplichte aanmeldingsgegevens zijn administratieve gegevens, die in relatie tot het BSN en de naam als reguliere persoonsgegevens dienen te worden behandeld.

3.3. Bevindingen voor Privacybescherming

3.3.1. Privacyvraag 1C: Intergrip als verantwoordelijke of bewerker

Vraag 1 en 1C

Vraag1: *Hoe is de rol van Intergrip te kwalificeren in de zin van de Wbp: verantwoordelijke of bewerker?*
Vraag 1C: *Heeft Intergrip met alle onderwijsinstellingen bewerkersovereenkomst gesloten?*

Antwoord 1 en 1C

Intergrip verwerkt gegevens na een expliciete schriftelijke opdracht.

> *Conclusie: Intergrip is een bewerker die de gegevens bewerkt namens de verantwoordelijke voor zover dit formeel is overeengekomen.*

Een bewerker mag alleen handelen namens de verantwoordelijke en de verkregen gegevens niet zelfstandig verder verwerken. Uit onze waarnemingen blijkt dat Intergrip zelfstandig geen aanvullende verwerkingen verricht, die niet in lijn zijn met het doel waarvoor de gegevens zijn verkregen.

Wij constateren dat niet voor alle RMC's een bewerkersovereenkomst is opgesteld waarin de aard van de verwerkingen formeel is gedefinieerd. Wij hebben geen uitvoerig onderzoek verricht naar de oorzaken voor het ontbreken van deze bewerkersovereenkomsten. Indicaties voor mogelijke verklaringen zijn:

- Onvoldoende brede kennis van informatiebeveiliging en privacybescherming bij de betrokken deelnemers binnen de RMC;
- Geen eenduidig beeld van de persoonsgegevens die vanuit de relevante wet- en regelgeving mogen worden verwerkt;
- Het ontbreken van een algemeen gedragen, up-to-date en op de branche toegespitste model bewerkersovereenkomst.

> *Conclusie: Intergrip heeft niet met alle regio's (als vertegenwoordiger van de onderwijsinstellingen en gemeenten) een bewerkersovereenkomst gesloten met een specificatie van de aard van de verwerkingen.*

> *Advies: Sluit een bewerkersovereenkomst af met iedere verantwoordelijke*.

3.3.2. Privacyvraag 2: Convenant 'Digitale onderwijsmiddelen en privacy'

Vraag 2

Voldoet Intergrip aan (de uitgangspunten van) het convenant[2] 'Digitale onderwijsmiddelen en privacy'? Wordt er gebruik gemaakt van de bij het convenant behorende model bewerkersovereenkomst?

Antwoord 2

Wij constateren dat niet alle bewerkersovereenkomsten met de RMC's op een gelijke wijze zijn uitgewerkt. Ondanks dat de uitgangspunten op hoofdlijnen overeenkomen zijn er verschillen in de afspraken.

Er is een branche specifieke bewerkersovereenkomst, die nader is toegespitst op de branche specifieke aandachtspunten. Deze wordt aangepast naar recente ontwikkelingen, zoals de meldplicht datalekken.

> *Conclusie: De uitgangspunten komen op hoofdlijnen overeen. De branche specifieke bewerkersovereenkomst is nader toegespitst op de branche specifieke aandachtspunten en wordt aangepast naar recentelijke ontwikkelingen zoals de meldplicht datalekken.*
>
> *Advies: Stel nieuwe bewerkersovereenkomsten op. Gebruik waar mogelijk standaard sjablonen conform het model zoals opgesteld door Kennisnet. Neem relevante wetgeving op in de op te stellen bewerkersovereenkomst.*
>
> *Advies: Overweeg aansluiting te zoeken bij de voor de branche specifiek ontwikkelde model bewerkersovereenkomst en de ketenpartners als Kennisnet en de MBO Raad te betrekken.*

Wij hebben waargenomen dat Intergrip hiertoe reeds contact heeft gezocht met Stichting Kennisnet voor inventariseren van de mogelijkheden voor gebruik van de modelovereenkomsten en de opname van recente wetgeving.

[2] www.privacyconevnant.nl

3.3.3. Privacyvraag 4: Gevoeligheid van persoonsgegevens

Vraag 4

Wordt er (bijvoorbeeld ten aanzien van beveiliging) onderscheid gemaakt in de gevoeligheid van de verzamelde persoonsgegevens?

Antwoord 4

In opzet ontbreekt het aan een classificatie naar de gevoeligheid van de gegevens. Er is geen gestructureerde expliciete risicoanalyse uitgevoerd, met als doel om de gegevens naar gevoeligheid in te delen en per klasse passende maatregelen te definiëren.

In bestaan hebben wij geconstateerd dat Intergrip wel rekening heeft gehouden met de gevoeligheid van privacygegevens. Hiertoe heeft Intergrip een stelsel van technische en organisatorische maatregelen ingericht. Dit omvat onder andere:

- De gegevens worden ontsloten op basis van noodzaak. Via de applicatie VO-MBO is de privacygevoelige informatie slechts zeer beperkt inzichtelijk. Deze applicatie is met name gericht op het inzichtelijk maken van de status en voortgang van het inschrijfproces bij de mbo-instelling. Alleen de applicatie DDD bevat de inhoudelijke dossiers van de leerlingen;
- De toegang tot de gegevens is gebaseerd op een rechtenstructuur waarbij, met juiste toepassing door de RMC's, het inzicht in privacygevoelige gegevens kan worden beperkt tot de vanuit de taak bepaalde noodzaak;
- De toegang tot de data en ontsluiting van gegevens verloopt via een versleutelde verbinding.
- Telefonisch (vanuit zowel Helpdesk activiteiten alsmede beheeractiviteiten) wordt er door Intergrip geen BSN gevraagd vanwege privacygevoeligheid. Wij hebben dit expliciet geverifieerd tijdens ons locatiebezoek.

Conclusie: In opzet ontbreekt het aan een indeling van gegevens naar gevoeligheid.

Advies: Stel een classificatieschema op dat aansluit bij de uitgangspunten vanuit de Wbp, inclusief de meldplicht datalekken.

Advies: Bepaal op basis van het ontwikkelde classificatieschema de indeling van de gegevens en via een gestructureerde risicoanalysemethodiek of aanvullende beschermingsmaatregelen noodzakelijk zijn.

3.4. Algemeen oordeel over Informatiebeveiliging

Wij constateren dat bij Intergrip beheerprocedures bestaan die zijn gericht op de eigen interne procedures, maar dat die in opzet niet altijd in voldoende mate zijn geformaliseerd en gedocumenteerd. Dit kan ertoe leiden dat interne procedures niet altijd duidelijk zijn voor medewerkers, met als gevolg dat een deel van de handelingen afwijkend zou kunnen worden uitgevoerd.

Daarnaast voert Intergrip geen regelmatig terugkerende risicoanalyses uit. Zo een risicoanalyse is van belang om de systemen en procedures van Intergrip te beschermen tegen huidige en toekomstige dreigingen. Het is aan te bevelen om, bezien vanuit de geconstateerde risico's, de relevante beheersprocedures te formaliseren.

Wij constateren dat Intergrip op dit moment werkt aan een procedure betreffende de Meldplicht Datalekken. Datalekken kunnen worden gezien als een risico voor de gehele keten van samenwerkende organisaties. Een integraal beleid is nodig om datalekken op een effectieve wijze te onderkennen en de gevolgen zo beperkt mogelijk te houden.

Advies: Stel op basis van een gestructureerde risicoanalyse het dreigingsbeeld op, bepaal of de reeds getroffen beheersmaatregelen toereikend zijn en daar waar nodig voer aanvullende maatrelen door.

Advies: Formaliseer de benodigde interne beheersprocedures en stel deze voor de relevante betrokkene beschikbaar.

3.5. Aandachtspunten voor Informatiebeveiliging

3.5.1. IB-vraag 1: Informatiebeveiligingsbeleid

Vraag 1

Is er een beveiligingsbeleid, en voorziet dat ook in incidentenbeheer (datalekken)?

Antwoord 1

Wij constateren dat het informatiebeveiligingsbeleid van Intergrip nog in concept is. Als basis hiervoor is de ISO/IEC 27001 norm genomen. Deze moet echter voor Intergrip op maat worden ingevuld.

Het informatiebeveiligingsbeleid voorziet op dit moment niet in incidentenbeheer (datalekken). Uit onze review van de incidentrapportages blijkt dat Intergrip een goede informele procedure kent met betrekking tot incidentbeheer. Deze is echter niet geformaliseerd in gedocumenteerd beleid.

Intergrip heeft geen ingevuld classificatiestelsel om informatie in te delen naar gevoeligheid.

Conclusie: Intergrip heeft een concept informatiebeveiligingsbeleid, waarin incidenten-beheer is opgenomen, maar nog geen expliciete verwijziging naar de afhandeling van datalekken.

Conclusie: Het beveiligingsbeleid ontbreekt een ingevuld classificatiestelsel voor ge-voeligheid van gegevens.

Conclusie: Het beveiligingsbeleid is nog niet formeel goedgekeurd.

Advies: Ontwikkel een informatiebeveiligingsbeleid waarin de uitgangspunten voor in-formatiebeveiliging en privacy worden beschreven.

Advies: Zoek samenwerking met ketenpartners om organisatie-overschrijdende risico's als datalekken aan te pakken. Voer jaarlijks een risicoanalyse uit en stel beheersmaat-regelen vast om de grootste risico's te behandelen.

3.5.2. IB-vraag 3: Security audits

Vraag 3

Vinden er reguliere (security)audits plaats? Zo ja, kan de school de rapporten inzien?

Antwoord 3

Uit onze documentreview blijkt dat Intergrip zich in artikel 7.1 van de standaard bewerkersovereenkomsten heeft verplicht tot het opleveren van een jaarlijkse TPM. Wij concluderen dat er op dit moment geen terugkerende procedure is ingericht voor het uitvoeren van een (security) audit of het opleveren van een TPM. Een (security) audit staat bij Intergrip wel op de planning.

De hostingleverancier TripleIT is ISO/IEC 27001 gecertificeerd. Hieruit volgt dat de onderdelen van het systeem van Intergrip die door TripleIT worden beheerd zijn onderworpen aan reguliere audits.

Conclusie: Er vinden geen regelmatige (security)audits plaats.

Advies: Overweeg periodiek security audits (mede op basis van de aandachtspunten uit een risicoanalyse) te laten uitvoeren naar de opzet en werking van het stelsel van beheersmaatregelen en stel deze ter inzage beschikbaar aan de deelnemende schoolinstellingen.

3.5.3. IB-vraag 4: Beveiligingsscans

Vraag 4

Laat de school of leverancier op reguliere basis beveiligingsscans uitvoeren op het hostingplatform en de software?

Antwoord 4

Er vinden geen reguliere scans plaats op de software. De servers van Intergrip worden up-to-date gehouden door hostingleverancier TripleIT.

Wij hebben tijdens de interviews geconstateerd dat er geen scans plaatsvinden naar mogelijke kwetsbaarheden in de webapplicatiesoftware.

Conclusie: Er vinden geen beveiligingsscans plaats op de webapplicatiesoftware.

Advies: Laat periodiek (minimaal elk kwartaal) of na majeure wijzigingen de webapplicatiesoftware testen op mogelijke kwetsbaarheden (tenminste de OWASP Top 10).

3.5.4. IB-vraag 7: Afspraken dossieroverdracht

Vraag 7

Zijn er duidelijke afspraken over de dossieroverdracht?

Antwoord 7

Er zijn duidelijke afspraken over veilige gegevensuitwisseling. Er worden afspraken gemaakt tussen de deelnemende mbo-instellingen en Intergrip over de afstemming van de technische koppeling voor de uitvoer van de Mbo-Check en de uitwisseling van de benodigde gegevens. Wij hebben vastgesteld dat Intergrip een overzicht bijhoudt van de technische koppelingen en (geautomatiseerde) processen voor bestandsuitwisseling.

Wij constateren dat een beperkt aantal schoolinstellingen informatie over leerlingen uitwisselt per e-mail. Intergrip heeft aangegeven dat dit een ongewenste situatie is.

Conclusie: Er zijn duidelijke afspraken over veilige gegevensuitwisseling.

Conclusie: Informatie-uitwisseling van leerlinggegevens per email is ongewenst.

Advies: Onderzoek gezamenlijk met de betreffende schoolinstelling naar mogelijkheden voor verdere beveiliging van de uitwisselingen via email.

3.5.5. IB-vraag 10: Bewustzijn

Vraag 10

Zijn de gebruikers van het systeem bij zowel de school als de leverancier zich voldoende bewust van ict-veiligheid en de daarbij horende gedragsregels?

Antwoord 10

De gebruikers alsook de leverancier zijn op de hoogte van de privacyaspecten en de noodzaak tot beschermen van de privacygevoelige gegevens.

Het continu op niveau houden van het bewustzijn voor de diverse dreigingen en kwetsbaarheden gerelateerd aan het verwerken van privacygevoelige gegevens in de keten blijft noodzakelijk.

Conclusie: Er is aandacht voor ict-veiligheid.

Advies: Maak in samenwerking met de ketenpartners het bewustzijn van ict-veiligheid en awareness een blijvend terugkerend punt als onderdeel van een awareness campagne gericht op de beveiliging van de vo-mbo-keten. Gebruik de uitkomsten van een risicoanalyse bij het vaststellen van het communicatiemateriaal binnen de keten.

3.5.6. IB-vraag 17: Bewaartermijnen

Vraag 17

Zijn er tussen de school en leverancier afspraken over de bewaartermijn van leerlinggegevens?

Antwoord 17

Er zijn afspraken gemaakt tussen de school en leverancier voor de bewaartermijnen. De databases worden per jaargang ontsloten.

Wij constateren dat in de productieomgeving de RMC's alleen toegang hebben tot de jaargangen 2014, 2015 en het lopend jaargang 2016.

Intergrip heeft nog historisch materiaal. Wij constateren dat voor Intergrip de (archief)databases nog inzichtelijk zijn tot 2012. Er is geen gestructureerd proces voor schonen.

> *Conclusie: Er is nog geen schoningsprocedure opgesteld voor het verwijderen van de gegevens uit de (archief) databases.*
>
> *Advies: Stel een schoningsprocedure op voor het verwijderen van de tot een persoon herleidbare informatie nadat de bewaartermijn is overschreden.*

3.5.7. IB-vraag 20: Gebruikersautorisatieprocedure

Vraag 20

Hebben de school en de leverancier een duidelijke gebruikersautorisatie procedure ingebouwd in de applicatie?

Antwoord 20

Er is een duidelijke autorisatieprocedure. De Helpdesk van Intergrip handelt de autorisatieverzoeken af en toetst daarbij of een autorisatieverzoek afkomstig is van een binnen de RMC gemandateerd persoon.

Binnen de RMC's gelden specifieke afspraken over de verdere invulling van het autorisatiebeheer. Het autorisatiebeheer is een ketenverantwoordelijkheid.

Intergrip biedt het platform, maar is inhoudelijk niet verantwoordelijk voor de toegekende autorisaties binnen de RMC's, tenzij dat specifiek is overeengekomen.

Conclusie: De procedure voor het beheer van autorisaties is adequaat, met uitzondering van de reconciliatie.

Advies: Omdat autorisatiebeheer een ketenverantwoordelijkheid is het wenselijk om periodiek een validatie van de uitgegeven gebruikersautorisaties bij de RMC's, inclusief de autorisaties van Intergrip medewerkers, uit te voeren.

Advies: Maak de accountscontrole onderdeel van de uitdienstprocedure.

3.5.8. IB-vraag 23: Beschikbaarheidsafspraken

Vraag 23

Zijn er afspraken tussen school en leverancier over beschikbaarheid van de dienst?

Antwoord 23

Uit de waarnemingen blijkt dat de RMC's en Intergrip meetbare Key Performance Indicatoren (KPI's) voor de beschikbaarheid hebben vastgelegd in de SLA 2016. De meetresultaten over beschikbaarheid worden niet gerapporteerd aan de afnemers van de dienstverlening.

Conclusie: Er zijn afspraken tussen de school en de leverancier over beschikbaarheid en er zijn maatregelen getroffen.

Conclusie: Er is geen rapportage aan de school over beschikbaarheid.

Advies: Overweeg een externe beschikbaarheidsrapportageprocedure te formaliseren en te documenteren als onderdeel van standaard service level rapportages.

Deze pagina is blanco vanwege dubbelzijdig printen.

4. Detailrapport (Analyse van de Evaluatieresultaten)

Noordbeek heeft de in de bijlage B genoemde documenten bestudeerd en diverse interviews uitgevoerd met in totaal 6 medewerkers van Intergrip. Onze waarnemingen en conclusies zijn hieronder per norm uitgewerkt. De toetsingen en waarnemingen bij de normen zijn gebaseerd op de deelvragen bij de desbetreffende normen.

Het oordeel bij een norm is voorzien van een gele of rode markering indien naar onze mening onvoldoende invulling wordt gegeven aan de intentie en doelstelling van de norm.

4.1. Toetsvragen Privacybescherming

Nr.	Privacyvraag	Waarneming	Oordeel
1 1A	Hoe is de rol van Intergrip te kwalificeren in de zin van de Wbp: verantwoordelijke of bewerker? Verwerkt Intergrip persoonsgegevens alleen na een expliciete schriftelijke opdracht van de onderwijsinstellingen?	In de rol van bewerker biedt Intergrip een platform voor het faciliteren van de doorstroom van leerlingen van een vo-instelling naar mbo-instellingen. Wij hebben waargenomen dat Intergrip met de aangesloten regio's contracten heeft afgesloten waarin de dienstverlening is omschreven.	OK Intergrip verwerkt gegevens na een expliciete schriftelijke opdracht.
1B	Zijn de onderwijsinstellingen voldoende geïnformeerd over de werking van en verwerkingen door Intergrip?	Voor de verschillende gebruikersgroepen zijn handleidingen beschikbaar waarin staat toegelicht hoe de applicaties werken. De applicatie is intuïtief en eenvoudig. De gebruikers van de applicatie (de leerling en mentoren) geven zelf de persoonsgegevens op. Intergrip verzamelt geen aanvullende gegevens anders dan de betrokkene zelf heeft opgegeven. De onderwijsinstellingen worden ingelicht over de verwerkingen van de persoonsgegevens en het functioneren van de Intergripapplicaties bij initiële aansluiting en gedurende half jaarlijkse landelijke overleggen. Tijdens de landelijke overleggen wordt de geboden functionaliteit doorgenomen.	OK De instellingen worden in voldoende mate geïnformeerd.

Nr.	Privacyvraag	Waarneming	Oordeel
		Tevens wordt bij initiële aansluiting een toelichting gegeven over het gebruik van de applicaties.	
1C	Heeft Intergrip met alle onderwijsinstellingen bewerkersovereenkomst gesloten?	In de rol van bewerker biedt Intergrip een platform voor het faciliteren van de doorstroom van leerlingen van een vo-instelling naar mbo-instellingen. Wij constateren dat er binnen de gestelde scope voor Intergrip sprake is van: ♦ Werkzaamheden die worden uitgevoerd volgens de uitdrukkelijke instructies van de verantwoordelijke vo-instellingen en mbo-instellingen; ♦ Dienstverlening die betrekking heeft op het verwerken van persoonsgegevens noodzakelijk en relevant voor de scope; ♦ Geen zeggenschap over de verwerking van persoonsgegevens. Intergrip bepaalt niet zelf hoe met de gegevens wordt omgegaan; ♦ Geen beslissingen nemen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens. Het bewerkersbegrip is in principe van toepassing op alle verschillende vormen van dienstverlening binnen de gestelde scope van VO-MBO en DDD. Wij hebben waargenomen dat niet voor alle regio's een bewerkersovereenkomst is opgesteld, terwijl daar vanuit de wetgeving (Wbp) een noodzaak toe is. De initiële verantwoordelijkheid hiervoor ligt bij de RMC's als vertegenwoordiger van de vo-instellingen en mbo-instellingen.	Deels OK Intergrip heeft niet met alle regio's (als vertegenwoordiger van de onderwijsinstellingen en gemeenten) een bewerkersovereenkomst gesloten met een specificatie van de aard van de verwerkingen. Advies: Sluit een bewerkersovereenkomst af met iedere verantwoordelijke.
1D	Maakt Intergrip gebruik van persoonsgegevens, voor eigen zoals analyse en productverbetering?	Intergrip gebruikt testdata voor het verbeteren van de applicatie. Daarvoor is initieel productiedata gebruikt, waarbij de BSN's zijn vervangen door gegenereerde dummy BSN's en alle persoonlijk identificeerbare informatie random is gemaakt.	OK Intergrip gebruikt geen BSN's voor andere activiteiten.

Nr.	Privacyvraag	Waarneming	Oordeel
	Zo ja, is daarvoor voorafgaande toestemming geregeld met de MBO-instellingen en/of geschiedt deze verwerking geanonimiseerd/gepseudonimiseerd?	Wij hebben gevalideerd dat de gebruikte BSN's in de testomgeving geen daadwerkelijke BSN's zijn, door een test BSN op te zoeken in de productieomgeving. Wij hebben waargenomen dat het BSN niet in de productieomgeving voorkwam.	
1E	Worden de gegevens van een mbo-instelling in Intergrip, nog door derden (andere partijen dan de mbo-instellingen) verwerkt? Bijvoorbeeld een verzuimloket of DUO?	De gegevens van mbo-instellingen wordt alleen door de hosting leverancier TripleIT verwerkt. TripleIT levert de servers waarop de gegevens zijn opgeslagen en voert daarop technisch onderhoud uit, waaronder patchen en het verzorgen van de backups. Voor het uitvoeren van de technische werkzaamheden is een contract afgesloten tussen Intergrip en TripleIT. Wij constateren dat Intergrip verder geen andere partijen toegang geeft tot de gegevens. Wij hebben tijdens de interviews bij een tweetal RMC's bevestigd gekregen dat er geen technische koppeling bestaat tussen het systeem Intergrip en bijvoorbeeld het verzuimloket of DUO.	OK Geen andere partijen hebben toegang tot de gegevens.
2	Voldoet Intergrip aan (de uitgangspunten van) het convenant 'Digitale onderwijsmiddelen en privacy' [3]? Wordt er gebruik gemaakt van de bij het convenant behorende model bewerkersovereenkomst?	Uitgangspunt van de bewerkersovereenkomst is dat Intergrip de bewerker is en de schoolinstelling de verantwoordelijke. De standaard convenanten van Intergrip wijken af van de model bewerkersovereenkomsten behorende bij het 'Convenant Digitale Onderwijsmiddelen en Privacy'. In de Intergrip-bewerkersovereenkomst zijn de uitgangspunten vanuit de Wbp overgenomen: ♦ De bewerker mag alleen uit naam van de verantwoordelijke acties uitvoeren; ♦ De bewerker mag, behalve met voorafgaande schriftelijke toestemming van de Verantwoordelijke, geen persoonsgegevens doorgeven aan enige derde partij; ♦ De bewerker wordt elk gebruik van persoonsgegevens verboden, anders dan in verband met het verrichten van diensten voor de verantwoordelijke;	OK met advies De uitgangspunten komen op hoofdlijnen overeen. De branche specifieke bewerkersovereenkomst is nader toegespitst op de branche specifieke aandachtspunten en wordt aangepast naar recentelijke ontwikkelingen zoals de meldplicht datalekken.

[3] www.privacyconevnant.nl

Nr.	Privacyvraag	Waarneming	Oordeel
		♦ De verplichtingen blijven van kracht ook na beëindiging van de werkzaamheden, gedurende een periode gelijk aan de bewaartermijn van de persoonsgegevens. De Intergrip-bewerkersovereenkomst is meer generiek van aard dan de model bewerkersovereenkomst opgesteld voor de branche. De model bewerkersovereenkomst 'digitale onderwijsmiddelen en privacy' bevat tevens bijlagen waarin de persoonsgegevens moeten worden omschreven en de daarvoor getroffen maatregelen. Deze onderdelen ontbreken in de bewerkersovereenkomst van Intergrip, maar zijn wel opgenomen in de verwerkingsspecificatie. Wij constateren dat: ♦ De uitgangspunten in de modellen op hoofdlijnen overeenkomen, en in de opgevraagde bewerkersovereenkomsten en verwerkingsspecificaties de uitwerking van de te verwerken gegevens zijn opgenomen; ♦ De door Intergrip gehanteerde model bewerkersovereenkomst en verwerkingsspecificatie zijn gedateerd en vergen aanpassing naar de laatste ontwikkelingen in de wetgeving; ♦ De beschrijving en detaillering zijn nader uitgewerkt in het model van de branche. Tevens wordt de branche specifieke model bewerkersovereenkomst geactualiseerd met de laatste wettelijke ontwikkelingen, zoals de meldplicht datalekken; ♦ Intergrip is voornemens om de model bewerkersovereenkomsten van de branche te adopteren.	Advies: Stel nieuwe bewerkersovereenkomsten op. Gebruik waar mogelijk standaard sjablonen conform het model zoals opgesteld door Kennisnet. Neem relevante wetgeving op in de op te stellen bewerkersovereenkomst. Advies: Overweeg aansluiting te zoeken bij de voor de branche specifiek ontwikkelde model bewerkersovereenkomst en de ketenpartners als Kennisnet en de MBO Raad te betrekken.
3A	Is er geregeld (technisch afgedwongen) dat: ♦ Er een rechtenstructuur is die afdwingt dat onderwijsinstellingen onderling bij elkaar geen persoonsgegevens van elkaar kunnen inzien?	Wij hebben waargenomen dat een rechtenstructuur in de database is opgenomen, waarbij een user_id is een gebruiker, wordt gekoppeld aan een region_id is een regio en de applicatie waartoe men toegang heeft (system_id is een systeem (DDD, VO-MBO, etc.)). Binnen deze applicaties worden rollen toebedeeld: (- role_id is het type rol (VO-rol, MBO-rol, Administrator, Supervisor)). Een rol heeft altijd een user, regio, systeem, type rol (vo, mbo, admin etc.).	OK Er is een adequate rechtenstructuur.

Nr.	Privacyvraag	Waarneming	Oordeel
		In het geval van vo of mbo bijvoorbeeld, zal een database instance worden gevuld (vo- of mbo-school). Wanneer een nieuwe regio aansluit vraagt Intergrip de projectleiding (telefonisch of per e-mail) een lijst te sturen met naam, tel nr en e-mailadres van de beheerders (decanen). Voor deze decanen maakt Intergrip een account aan en stuurt hen de accountgegevens. Wij constateren dat het versturen van de accountgegevens op een gecontroleerde wijze wordt uitgevoerd. Deze decanen mogen vervolgens zelf de accounts voor hun mentoren aanmaken en verstrekken. Intergrip maakt uitsluitend accounts aan op verzoek van projectleiders. Bij aanvragen anders dan van een projectleider verwijst Intergrip de aanvrager door naar de beheerder van de school of instellingen. Wij constateren dat een gebruiker (bijvoorbeeld een mentor) niet meer rechten kan uitdelen dan hij of zij zelf heeft en geen informatie buiten de eigen regio kan inzien (tenzij daarvoor expliciet geautoriseerd).	
3B	Is er geregeld (technisch afgedwongen) dat: ♦ Mbo-instellingen geen inzage hebben in de persoonsgegevens van andere instellingen (op bijvoorbeeld BSN-niveau), tenzij die inzage een wettelijke basis heeft?	Wij constateren dat via de Mbo-Check een mbo-instelling alleen de inhoudelijke dossiers in het DDD opvraagt op basis van de eigen inschrijvingen. Dit gebeurt via veilige verbindingen (zie ook IB-normen 11 en 12). Wij constateren dat er een tabel is opgenomen met de BSN's van de leerlingen om de unieke koppeling te maken en persoonsverwarring te voorkomen. Elke mbo-instelling verkrijgt van Intergrip een uniek nummer. Tevens heeft elke leerling een uniek nummer. Op basis van deze unieke nummers worden leerlingen en mbo-instellingen gekoppeld en verkrijgt de mbo-instelling alleen die DDD-dossiers waarop zij recht heeft op basis van de inschrijving van de leerling. Zo is er sprake van een wettelijke basis. Wij hebben 25 DDD-dossiers gesampled en daarbij geconstateerd dat deze aan de juiste mbo-instelling beschikbaar zijn gesteld.	OK Instellingen hebben geen inzage in elkaars gegevens.

Nr.	Privacyvraag	Waarneming	Oordeel
3C	Is er geregeld (technisch afgedwongen) dat: ♦ Voor de uitwisseling van een overstap- of doorstroomdossier gecontroleerd wordt of de toestemming van wettelijke vertegenwoordiger(s) is gegevens voordat een uitwisseling kan plaatsvinden? Vgl. art. 2.3.6a Wet educatie en beroepsonderwijs. En dat bij gebreke van akkoord deze uitwisseling niet kan plaatsvinden?	Wij hebben geobserveerd dat een student jonger dan 18 jaar een akkoordverklaring moet laten invullen door de ouder van de student. Dit gebeurt door naam, datum en plaats in te vullen van de ouder. Het is niet mogelijk dit procesdeel technisch af te laten dwingen omdat de persoonsgegevens van de ouders/verzorgers niet mogen worden verwerkt door Intergrip. Bij het invullen van een DDD in de demo omgeving blijkt dat bij het ontbreken van de akkoordverklaring het DDD niet wordt verstuurd naar de mbo-instelling.	OK Er wordt gecontroleerd op toestemming van de wettelijke vertgenwoordiger(s).
4	Wordt er (bijvoorbeeld ten aanzien van beveiliging) onderscheid gemaakt in de gevoeligheid van de verzamelde persoonsgegevens?	In het informatiebeveiligingsbeleid is een passage opgenomen voor het classificeren van de informatie en informatiesystemen. Intergrip hanteert als uitgangspunt '*Het beveiligingsniveau van een informatiesysteem is afhankelijk van de informatie die het systeem verwerkt en hoe de informatie is geclassificeerd. Classificatie dient door de eigenaar of de verantwoordelijke van het informatiesysteem te worden bepaald.*' Wij constateren dat het classificatieschema in opzet nog moet worden ingevuld. In de praktijk heeft Intergrip invulling gegeven aan de bescherming van persoonsgegevens. Zo is het inhoudelijk dossier met de privacygevoelige gegevens van de leerlingen (het DDD) gescheiden van de status van de doorstroom naar een mbo-instelling in de applicatie VO-MBO. Op basis van de noodzaak voor toegang tot de privacygevoelige gegevens zijn de autorisaties uitgegeven.	Deels OK In opzet ontbreekt het aan een indeling van gegevens naar gevoeligheid. Advies: Stel een classificatieschema op dat aansluit bij de uitgangspunten vanuit de Wbp inclusief de meldplicht datalekken. Advies: Bepaal op basis van het ontwikkelde classificatieschema de indeling van de gegevens en via een gestructureerde risicoanalysemethodiek of aanvullende

Nr.	Privacyvraag	Waarneming	Oordeel
		De wachtwoorden van gebruikers zijn gehashed opgeslagen. Er zijn geen andere gegevens in de database encrypt of gehashed.	beschermingsmaatregelen noodzakelijk zijn.
5	Wordt er, en zo ja in hoeverre, gebruik gemaakt van de 'Gegevensstandaard VO-MBO-overstapdossier' [4] zoals deze in beheer is gegeven bij Edustandaard?	Wij hebben in de testomgeving een volledige dossierdoorloop opnieuw uitgevoerd om vast te stellen dat de uitvraag voor het inhoudelijk dossier op een intuïtieve en gestructureerde manier wordt gedaan en verloopt conform de datamodellen. Een deel van de vragen zijn gesloten, of bevatten een beperkt aantal keuzemogelijkheden. Intergrip heeft getracht het aantal vrije tekstvelden te minimaliseren. Wij constateren dat de inhoudelijke dossiers pas kunnen worden verstuurd na expliciete toestemming van de betrokkene en, indien jonger dan 18 jaar, na goedkeuring van de ouder(s) of wettelijk vertegenwoordiger(s). De functionaliteit en de samenstelling van het dossier wordt besproken in een halfjaarlijks landelijk overleg. Wij hebben uit de notulen geconstateerd dat de inhoud van de vragen voor de samenstelling van het dossier worden geëvalueerd en afspraken worden gemaakt over de verbeteracties. Wij hebben samples genomen van de inhoudelijke dossiers in de productieomgeving en geconstateerd dat deze worden gevuld via de uitvraag van de betrokkene. In de productieomgeving hebben wij via observatie waargenomen dat de inhoud van het overdrachtdossier voor veel vo-instellingen generiek is. Wij constateren dat afwijkingen expliciet contractueel worden overeengekomen. Wij constateren dat in de verwerkingsspecificatie de tabellen met de te verwerken gegevens zijn opgenomen in de bijlagen. Deze formele afspraken zijn door de deelnemende partijen ondertekend.	OK De 'Gegevensstandaard VO-MBO-overstapdossier' wordt gevolgd.

[4] https://www.edustandaard.nl/standaarden/afspraken/afspraak/vo-mbo-overstapdossier/

Nr.	Privacyvraag	Waarneming	Oordeel
6	Zijn er koppelingen met andere databases of bronnen waarmee Intergrip wordt gevoed? Kunnen deze bronnen/partijen data van Intergrip muteren, en zo ja, wat is de invloed van een mbo-instelling daarop?	De invoer vanuit de vo-instellingen gaat via een daartoe beschikbaar gesteld portaal. De upload vanuit de vo-instellingen wordt door Intergrip op invoerfouten gecontroleerd en vervolgens in VO-MBO ingevoerd. Wij constateren dat de Intergrip-systemen DDD en VO-MBO geautomatiseerde koppelingen hebben met de mbo-instellingen. Deze leveren via de Mbo-Check de gegevens van leerlingen die zich bij die mbo-instelling hebben aangemeld, inclusief de bijbehorende status van inschrijving. Intergrip vraagt de mbo-instelling de leerlinggegevens te delen van alle leerlingen die zich aanmelden voor een opleiding die start in augustus/september van het aankomende schooljaar. Mocht een leerling niet in een Mbo-Check voor komen, dan krijgt de leerling een status ‘onbekend bij mbo’. Wij constateren dat Intergrip een overzicht bijhoudt van de koppelingen: ♦ Een overzicht van koppelingen per mbo-instelling wordt apart bijgehouden; ♦ Een overzicht van de DDD-koppeling. Type koppelingen: ♦ Handmatig inladen via uploadpagina https://vombo.intergrip.nl/mbocheck ♦ Automatische koppeling via FTP(s), XML (voor Magister), Webservices (GUP voor ROC MN), ELD1 (EduArte) – Real-time. Wij hebben waargenomen dat de bestandsuitwisseling versleuteld plaatsvindt. Uit de waarnemingen blijkt niet dat er koppelingen zijn met andere partijen. Uit diverse interviews die gehouden zijn in een tweetal casus RMC’s blijkt eveneens niet dat er koppelingen zijn met andere databases of bronnen zoals DUO-systemen of gemeentesystemen. Vanuit de mbo-instelling worden de gegevens in VO-MBO aangepast op de status van de inschrijving. Er zijn vanuit de gekoppelde systemen geen aanvullende mutaties op de inhoudelijke privacygevoelige dossiergegevens in het DDD.	OK Er zijn geen koppelingen met andere partijen.

Nr.	Privacyvraag	Waarneming	Oordeel
7	Wat is – in het licht van de hiervoor genoemde risico's - het algemeen oordeel van de auditor over de omgang met persoonsgegevens en privacy van studenten door Intergrip?	Uit de waarnemingen blijkt dat het stelsel van procesmatige en technische maatregelen voor de beveiliging van de persoonsgegevens voldoet aan de hieraan in redelijkheid te stellen eisen. Aandachtspunten zijn: ♦ Hernieuwen van de model bewerkersovereenkomst en formeel deze laten bekrachtigen per regio; ♦ Formaliseren van de Intergrip interne beheersprocedures en de vastlegging daarvan welke relevant voor informatiebeveiliging & privacy; ♦ Periodieke validatie van de uitgegeven gebruikersautorisaties bij de regio's; ♦ Periodieke scans laten uitvoeren naar eventuele technische kwetsbaarheden in de webapplicaties (zoals de OWASP-kwetsbaarheden); ♦ Formaliseren van het informatiebeveiligingsbeleid inclusief classificatietabel en procedure voor meldplicht datalekken; ♦ Opnemen van de meetresultaten voor de beschikbaarheid in de service lever rapportages. De betrokkene (dus: de leerling en/of zijn ouders) moet vooraf worden geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is, in voor de betrokkene begrijpelijke taal. Dit kan bijvoorbeeld in de schoolgids of via de website zijn of via een privacy protocol. Wij constateren dat op de website van Intergrip voor VO-MBO, of bij het Digitaal Doorstroom Dossier geen privacy statement is opgenomen en geen informatie wordt gegeven over het doel en de aard van de verwerking. Het is aannemelijk dat de toelichting mondeling wordt gegeven door de mentor van de leerlingen.	OK met advies Advies: Overweeg een statement op te nemen waarin de betrokkene helder en in begrijpelijke taal wordt geïnformeerd over de verwerking van de persoonsgegevens. Advies: Stel verbeterplannen op voor de Intergripketen voor de geconstateerde aandachtspunten. Advies: Stel op basis van een gestructureerde risicoanalyse het dreigingsbeeld op, bepaal of de reeds getroffen beheersmaatregelen toereikend zijn en daar waar nodig voer aanvullende maatrelen door. Advies: Formaliseer de benodigde interne beheersprocedures en stel deze voor de relevante betrokkene beschikbaar.

4.2. Toetsvragen Informatiebeveiliging

Nr.	IB-vraag	Waarneming	Oordeel
1	Is er een beveiligingsbeleid, en voorziet dat ook in incidentenbeheer (datalekken)?	Intergrip heeft een concept informatiebeveiligingsbeleid, dat is gebaseerd op de internationale standaard ISO/IEC 27001. Het informatiebeveiligingsbeleid bevat op hoofdlijnen een beschrijving van het afhandelen van beveiligingsincidenten, de verantwoordelijkheden van de medewerkers en de meldpunten voor incidenten. Het informatiebeveiligingsbeleid is nog niet geheel ingevuld en nog niet formeel goedgekeurd. Het bevat geen expliciete beschrijving van verantwoordelijkheden in het kader van datalekken. Uit onze analyse van de afhandeling van een incident blijkt dat een feitenonderzoek, analyse van de gebeurtenissen, acties voor vaststellen van de benodigde mitigerende maatregelen en een risicoanalyse heeft plaatsgevonden voor het bepalen van de vervolgschade. De afhandeling is gestructureerd vastgelegd. Uit deze analyse blijkt dat de verantwoordelijken genoemd in het informatiebeveiligingsbeleid waren betrokken bij de analyse.	Deels OK Intergrip heeft een concept informatiebeveiligingsbeleid, waarin incidentenbeheer is opgenomen, maar nog geen expliciete verwijziging naar de afhandeling van datalekken. Het beveiligingsbeleid ontbreekt een ingevuld classificatiestelsel voor gevoeligheid van gegevens. Het beveiligingsbeleid is nog niet formeel goedgekeurd. Advies: Ontwikkel een informatiebeveiligingsbeleid waarin de uitgangspunten voor informatiebeveiliging en privacy worden beschreven. Advies: Zoek samenwerking met ketenpartners om organisatie-overschrijdende risico’s als datalekken aan te pakken. Voer jaarlijks een risicoanalyse uit en stel beheersmaatregelen vast om de grootste risico’s te behandelen.

Nr.	IB-vraag	Waarneming	Oordeel
2	Heeft de leverancier of de onderwijsinstelling officieel erkende ISO- en/of NEN-beveiligingscertificeringen?	Intergrip beschikt niet over een ISO- of NEN-certificering. De medewerkers van Intergrip hebben een geheimhoudingsverklaring ondertekend. Dit is een standaard onderdeel van het contract. Tijdens onze waarnemingen en de interviews ter plaatse hebben wij geconstateerd dat informatiebeveiliging en privacybescherming voldoende aandacht hebben van de medewerkers van Intergrip. Zij acteren naar de uitgangspunten om de informatie passend te beschermen. De hostingleverancier TripleIT is gecertificeerd voor ISO/IEC 27001.	OK Informatiebeveiliging en privacybescherming hebben voldoende aandacht.
3	Vinden er reguliere (security)audits plaats? Zo ja, kan de school de rapporten inzien?	Wij constateren dat bij Intergrip geen periodiek (jaarlijks) proces is ingeregeld om invulling te geven aan Artikel 7.1 van de standaard bewerkersovereenkomst. De hostingleverancier TripleIT voert het technische beheer uit op de servers waarop de Intergrip-applicaties draaien. TripleIT is gecertificeerd voor ISO/IEC 27001.	Niet OK Er vinden geen regelmatige (security) audits plaats. Advies: Overweeg periodiek security audits (mede op basis van de aandachtspunten uit een risicoanalyse) te laten uitvoeren naar de opzet en werking van het stelsel van beheersmaatregelen en stel deze ter inzage beschikbaar aan de deelnemende schoolinstellingen.
4	Laat de school of leverancier op reguliere basis beveiligingsscans uitvoeren op het hostingplatform en de software?	**Hostingplatform** De hostingleverancier TripleIT voert het technische beheer uit op de servers waarop de Intergrip-applicaties draaien. TripleIT voert de patching centraal uit, zodat de servers van Intergrip up-to-date zijn met de nieuwste beschikbare patches en updates.	Niet OK Er vinden geen beveiligingsscans plaats op de webapplicatiesoftware. Advies: Laat periodiek (minimaal elk kwartaal) of na majeure wijzigingen de webapplicatiesoftware testen op

Nr.	IB-vraag	Waarneming	Oordeel
		Wij constateren dat de vulnerabilityscan op de productieserver alleen bestaat uit het inventariseren naar open poorten via dagelijkse NMAP-scans. Uit de scan blijkt dat poorten in beperkte mate open staan. Er is een IP-whitelisting. De servers draaien noodzakelijke modules c.q. programmatuur uit standaard repos. Voor deze standaard repos houdt TripleIT bij of er security issues zijn en voert ad hoc updates uit, indien dat noodzakelijk blijkt te zijn. De servers worden maandelijks gepatched. Wij constateren dat een recente versie van het CentOS OS en kernel release is geïnstalleerd. **Software** Wij constateren dat er geen scans plaatsvinden naar mogelijke kwetsbaarheden in de webapplicatiesoftware.	mogelijke kwetsbaarheden (tenminste de OWASP Top 10).
5	Is het duidelijk hoe de school of leverancier omgaat met back-updata?	Wij constateren dat de backup werkzaamheden als onderdeel van het beheer van het platform plaatsvinden. Een full backup wordt wekelijks uitgevoerd met een retentieperiode van drie weken en een incremental backup (dus alleen de wijzigingen) op zondag, dinsdag, woensdag, donderdag, vrijdag en zaterdag met een retentieperiode van twee weken. De backups worden dagelijks gemaakt en opgeslagen op lokale disk en remote. De backup op disk heeft als doel om zonder tussenkomst van Triple IT een herstel te kunnen uitvoeren. Alle andere restore's worden remote gedaan door Triple IT. De leverancier Triple IT is gecertificeerd voor ISO/IEC 27001voor de hosting dienstverlening, inclusief de fysieke toegangsbeveiliging.	OK Het backup-proces is adequaat.

Nr.	IB-vraag	Waarneming	Oordeel
6	Er zijn duidelijke afspraken over de inhoud van het overdrachtsdossier.	Wij hebben in de testomgeving een volledige dossierdoorloop opnieuw uitgevoerd om vast te stellen dat de uitvraag voor het inhoudelijk dossier op een intuïtieve en gestructureerde manier wordt gedaan. Een deel van de vragen zijn gesloten, of bevatten een beperkt aantal keuzemogelijkheden. Intergrip heeft getracht het aantal vrije tekstvelden te minimaliseren. Wij constateren dat de inhoudelijke dossiers pas kunnen worden verstuurd na expliciete toestemming van de betrokkene en, indien jonger dan 18 jaar, na goedkeuring van de ouder(s) of wettelijk vertegenwoordiger(s). De functionaliteit en de samenstelling van het dossier wordt besproken in een halfjaarlijks landelijk overleg. Wij hebben uit de notulen geconstateerd dat de inhoud van de vragen voor de samenstelling van het dossier worden geëvalueerd en afspraken worden gemaakt over de verbeteracties. Wij hebben samples genomen van de inhoudelijke dossiers in de productieomgeving en geconstateerd dat deze dossiers zijn gebaseerd op de uitvraag van de betrokkene. In de productieomgeving hebben wij via observatie waargenomen dat de inhoud van het overdrachtdossier voor veel vo-instellingen generiek is. Wij constateren dat afwijkingen expliciet contractureel worden overeengekomen. Wij constateren dat in de verwerkingsspecificatie de tabellen met de te verwerken gegevens zijn opgenomen in de bijlagen. Deze formele afspraken zijn door de deelnemende partijen ondertekend.	OK Er zijn duidelijke afspraken over de inhoud van het overdrachtsdossier.
7	Zijn er duidelijke afspraken over de dossieroverdracht?	Wij hebben de beheerder van de technische koppelingen geïnterviewd en de systeeminstellingen geobserveerd. Er zijn afspraken gemaakt tussen de deelnemende mbo-instellingen en Intergrip over de afstemming van de technische koppeling voor de uitvoer van de Mbo-Check en de uitwisseling van de benodigde gegevens. Intergrip stemt met de betrokken IT-medewerker(s) af over de benodigde maatregelen zoals een veilige (versleutelde) technische verbinding, IP-whitelisting, poortinstellingen etc.	OK met advies Er zijn duidelijke afspraken over veilige gegevensuitwisseling. Informatie-uitwisseling van leerlinggegevens per email is ongewenst.

Nr.	IB-vraag	Waarneming	Oordeel
		Wij hebben vastgesteld dat Intergrip een overzicht bijhoudt van de technische koppelingen en (geautomatiseerde) processen voor bestandsuitwisseling. De effectieve werking van de geautomatiseerde koppelingen worden gemonitord als onderdeel van de dagelijkse taken. Wij constateren dat de medewerker over voldoende kennis beschikte van de technische koppelingen. Intergrip matcht de uniek toegekende student(/leerling)nummers met het toegekende mbo-instelling nummer. Een match vindt eveneens plaats op het BSN, zodat automatisch wordt gewaarborgd dat de gegevens aan de juiste mbo-instelling worden gegeven. Wij hebben een sample van 25 dossiers genomen. Uit de sample bleek dat geen enkel dossier bij een verkeerde mbo-instelling terecht is gekomen. Wij constateren dat een klein aantal mbo-instellingen de gegevensuitwisseling via email verstuurt. Intergrip heeft aangegeven dat dit een ongewenste situatie is.	Advies: Onderzoek gezamenlijk met de betreffende schoolinstelling naar mogelijkheden voor verdere beveiliging van de uitwisselingen via email.
8	Wordt de toegang tot het systeem strikt via https ontsloten?	Er wordt gebruikt gemaakt van TLS-versie 1.2 wat de meest recente versie is qua beveiligingsprotocol. De veiligheid van de cipher suite is goed conform de richtlijnen van het Nationaal Cyber Security Centrum (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256). De subdomeinen en de onderliggende mappen zijn voorzien van een beveiligde verbinding middels een ‘wildcard’ SSL-certificaat geïnstalleerd. Wij constateren dat de toegang tot het systeem strikt via https wordt ontsloten. Wij hebben geobserveerd dat http-verzoeken worden omgezet in (redirect to) https.	OK De toegang tot het systeem is strikt via https ontsloten.
9	Zijn de gebruikers van het systeem voldoende opgeleid voor het gebruik ervan?	Voor de verschillende gebruikersgroepen zijn handleidingen beschikbaar waarin staat toegelicht hoe de applicaties werken. De applicatie is intuïtief en eenvoudig. De gebruikers van de applicatie (de leerling en decanen of mentoren) geven zelf de persoonsgegevens op. Intergrip verzamelt geen aanvullende gegevens anders dan die door de betrokkene zelf zijn opgegeven.	OK De gebruikers van het systeem zijn in voldoende mate opgeleid.

Nr.	IB-vraag	Waarneming	Oordeel
		Wij hebben het intuïtief gebruik van de applicatie getoetst door middel van het doorlopen van de applicatie (in de testomgeving) zonder training vooraf. Wij hebben zonder training de gehele aanmelding en opbouw van een DDD-dossier kunnen uitvoeren. De onderwijsinstellingen worden ingelicht over de verwerkingen van de persoonsgegevens en het functioneren van de Intergrip-applicaties bij initiële aansluiting en gedurende half-jaarlijkse landelijke overleggen. Tijdens de landelijke overleggen wordt de geboden functionaliteit doorgenomen. Tevens wordt bij initiële aansluiting een toelichting gegeven over het gebruik van de applicaties.	
10	Zijn de gebruikers van het systeem bij zowel de school als de leverancier zich voldoende bewust van ict-veiligheid en de daarbij horende gedragsregels?	Wij hebben tijdens onze waarnemingen ter plaatse en gedurende de interviews bij Intergrip waargenomen dat er voldoende aandacht en bewustzijn is voor ict-veiligheid en daarbij horende gedragsregels. Tijdens interviews binnen een tweetal casusregio's is eveneens geconstateerd dat er aandacht is voor ict-veiligheid. De schoolinstellingen zijn zich bewust van de risico's van gegevensuitwisseling en zijn terughoudend in het verschaffen van (onnodige) informatie. In generieke zin geldt dat het bewustzijn van ict-veiligheid en awareness een blijvend punt van aandacht is ter verdere verbetering van de algehele bescherming van de privacygevoelige gegevens. Wij constateren dat vanuit Intergrip de deelnemende RMC's zijn gewezen op de noodzaak tot bescherming van de privacygevoelige gegevens. De Intergrip-systemen zijn voor alle gebruikers en bezoekers te benaderen. Vanuit veiligheidsoogpunt zijn de poorten op de server geblokkeerd die niet voor iedereen toegankelijk moeten zijn. Voor de dienstverlening wordt toegang verschaft op basis van een IP-adres welke is opgenomen in een 'whitelist':	OK met advies Er is aandacht voor ict-veiligheid. Advies: Maak in samenwerking met de ketenpartners het bewustzijn van ict-veiligheid en awareness een blijvend terugkerend punt als onderdeel van een awareness campagne gericht op de beveiliging van de vo-mbo-keten. Gebruik de uitkomsten van een risicoanalyse bij het vaststellen van het communicatiemateriaal binnen de keten.

Nr.	IB-vraag	Waarneming	Oordeel
		FTP whitelist ♦ IP-adres kantoor Veenendaal; ♦ IP-adressen klanten die Mbo-Check aanleveren via FTP(s). **SSH whitelist** ♦ IP-adres kantoor Veenendaal. **MySQL whitelist** ♦ IP-adres kantoor Veenendaal; ♦ Thuis IP-adres programmeurs in verband met thuiswerk of calamiteiten.	
11	Wordt het overdrachts-dossier versleuteld tussen scholen overgedragen? Zo ja, zijn er afspraken over de versleuteling van het dossier?	Wij constateren dat alle subdomeinen bereikbaar zijn via een beveiligde verbinding (https-verbinding), voorzien van een sterke versleuteling. **Koppelingen:** ♦ Handmatig inladen via uploadpagina https://vombo.intergrip.nl/mbocheck ♦ Automatische koppeling via: FTP(s), XML (voor Magister), Webservices (GUP voor ROC MN), ELD1 (EduArte) – Real-time, E-mail – mbocheck@intergrip.nl Wij constateren dat de verbindingen zijn versleuteld met een sterke encryptie. Wij constateren dat Intergrip de methode en opzet van de technische koppeling vooraf afstemt met de schoolinstellingen. Dit is noodzakelijk om de koppeling tot stand te brengen.	OK De verbindingen zijn versleuteld met een sterke encryptie.
12	Als de dossieroverdracht plaatsvindt over het internet, worden hiervoor dan beveiligingsvoorzieningen getroffen?	Wij constateren dat alle subdomeinen bereikbaar zijn via een beveiligde verbinding (https-verbinding), voorzien van een sterke versleuteling. Intergrip stemt met de betrokken IT-medewerker(s) af over de benodigde maatregelen zoals een veilige (versleutelde) technische verbinding, IP-whitelisting, poortinstellingen etc. Wij hebben vastgesteld dat Intergrip een overzicht bijhoudt van de technische koppelingen en (geautomatiseerde) processen voor bestandsuitwisseling. De effectieve werking van de geautomatiseerde koppelingen worden gemonitord als onderdeel van de dagelijkse taken.	OK De beveiligingsvoorzieningen zijn adequaat. Zie ook informatiebeveiliging norm 7.

Nr.	IB-vraag	Waarneming	Oordeel
		Wij constateren dat de betreffende medewerker over voldoende kennis beschikt van de technische koppelingen. **Koppelingen:** ♦ Handmatig inladen via uploadpagina https://vombo.intergrip.nl/mbocheck ♦ Automatische koppeling via: FTP(s), XML (voor Magister), Webservices (GUP voor ROC MN), ELD1 (EduArte) – Real-time, E-mail – mbocheck@intergrip.nl Wij constateren dat de verbindingen zijn versleuteld met een sterke encryptie. Wij constateren dat Intergrip de methode en opzet van de technische koppeling vooraf afstemt met de schoolinstellingen. Dit is noodzakelijk om de koppeling tot stand te brengen.	
13	Is in het proces geborgd dat een overdrachtsdossier alleen terecht kan komen bij de ontvanger die de latende school heeft aangegeven?	Zie Hoofdstuk 1 voor de procedurebeschrijving en IB-vraag 14. Voor een match van een relevant DDD-dossier voor de mbo-instelling wordt gebruik gemaakt van de zogenaamde Mbo-Check. Studenten worden via een combinatie van het BSN en het intergrip-id gekoppeld aan de juiste mbo-instelling. Tevens wordt een koppeling gemaakt met de opleidingsgegevens en het deelnemernummer (zie ook Hoofdstuk 1). Alleen die DDD-dossiers voor de studenten die door de vo-instelling worden aangeleverd aan Intergrip worden beschikbaar gesteld aan de mbo-instelling. Wij hebben eveneens geconstateerd dat een gebruiker geen gegevens kan raadplegen buiten de regio. Wij hebben via een sample van 25 DDD-dossiers waargenomen dat de dossiers aan de juiste instelling waren gekoppeld.	OK Het overdrachtsdossier kan alleen terecht komen bij de ontvanger die de latende school heeft aangegeven.
14	Is het duidelijk hoe de leverancier garandeert dat gegevens op zijn gedeelde systeem niet met elkaar vermengd raken? (data	De database-omgevingen zijn logisch gescheiden. Er is een VO-MBO-database met daarin de statusinformatie over de voortgang van het inschrijfproces van een leerling bij een mbo-instelling. Daarnaast is er een separate database met de inhoudelijke DDD-dossiers.	OK Gegevens kunnen niet met elkaar vermengd raken.

Nr.	IB-vraag	Waarneming	Oordeel
	school 1 komt ongevraagd bij school 2 terecht)	Wij constateren dat de applicaties van Intergrip rollen zijn aangemaakt met rechten op basis van 'need to know' en 'need to have' principes. Dit geldt dus ook voor de toegang tot de Intergrip-systemen en gegevens: ♦ Wij constateren dat een gebruiker-id wordt toegekend aan een regio (RMC) en een systeem (VO-MBO, DDD), en dat deze een type rol (VO, MBO, Admin) krijgt; ♦ Voor een vo- of mbo-gebruiker, zal altijd een vo- of mbo-instelling moeten worden ingevuld; ♦ Wij constateren dat de beheerders van Intergrip allen beschikken over Supervisor rechten en toegang hebben tot alle omgevingen; ♦ Wij hebben geobserveerd dat voor de gebruikers (leerlingen) een duidelijk proces en portaal is ingericht voor het aanvragen van een account (zie IB-vraag 20). Voor een match van een relevant DDD-dossier voor de mbo-instelling, wordt gebruik gemaakt van de Mbo-Check. Studenten worden via een combinatie van het BSN en het Intergrip-id gekoppeld aan de juiste mbo-instelling. Tevens wordt een koppeling gemaakt met de opleidingsgegevens en deelnemernummer (zie ook Hoofdstuk 1). Alleen die DDD-dossiers voor de studenten die door de vo-instelling worden aangeleverd aan Intergrip worden beschikbaar gesteld aan de mbo-instelling. Wij hebben eveneens geconstateerd dat een gebruiker geen gegevens kan raadplegen buiten de regio. Wij hebben via een sample van 25 dossiers waargenomen dat de dossiers aan de juiste instelling waren toegekend.	
15	Heeft de school inzage in de informatiestromen bij de dossieroverdracht? Vindt er tijdens of na de overdacht van een dossier nog verrijking plaats van	Wij constateren dat het dossier (DDD) zelf niet wordt verrijkt binnen Intergrip. Nadat de leerling goedkeuring heeft gegeven, wordt het dossier 'bevroren' en uitgewisseld als PDF. Indien het wenselijk is om aanvullende informatie uit te wisselen over de leerling, dan biedt het systeem DDD de mogelijkheid om 'warme overdracht' aan te vinken (alleen met een akkoord van de leerling). Dit is het signaal voor een mbo-instelling om contact te zoeken met de vo-instelling voor nadere informatie. Deze informatie wordt echter niet in het DDD of VO-MBO vastgelegd. Wij hebben 25 samples genomen van DDD-dossiers en	OK De school heeft inzage in de informatiestromen bij de dossieroverdracht. Er vindt geen verrijking plaats.

Nr.	IB-vraag	Waarneming	Oordeel
	het dossier met bijvoorbeeld medische gegevens?	daarin visueel waargenomen dat de informatie in de PDF's van de DDD's overeenkomt met de vragenlijst zoals de leerling die heeft ingevuld. Wij hebben bij een tweetal casus RMC's gevalideerd dat verdere verwerking plaatsvindt in de systemen van de mbo-instellingen. Er vinden dus geen verrijkingen plaats in het DDD nadat de leerling het DDD heeft 'goedgekeurd' voor versturen.	
16	Is er voldoende duidelijk aan welke systemen het systeem van de leverancier gekoppeld is?	Wij constateren dat een overzicht wordt bijgehouden van de koppelingen met de andere instellingen. Intergrip houdt dit overzicht bij om te borgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de interfaces zijn geborgd. De servers van Intergrip worden gemonitord door de hosting partij TripleIT. Deze monitoring services zijn niet gekoppeld aan de Intergrip-database zelf, maar bewaken de server waarop deze draait. Uit onze waarnemingen, samples, observaties en interviews is niet gebleken dat gebruik wordt gemaakt van andere analyse- of rapportagetools gericht op de inhoudelijke informatie in de DDD-database.	OK De koppelingen zijn beschreven.
17	Zijn er tussen de school en leverancier afspraken over de bewaartermijn van leerlinggegevens?	In de model Bewerkersovereenkomst van Intergrip is een bewaartermijn opgenomen. Deze bewaartermijn is eveneens opgenomen in de procedurebeschrijving. De bewaartermijnen zijn: ♦ Bewaartermijn aangeleverde (ge-uploade) bestanden 1 jaar ♦ Bewaartermijn persoonsgegevens in database 2 jaar Nadat is vastgesteld dat de upload succesvol is geweest, wordt het bestand na maximaal 1 jaar vernietigd. De gegevens in de database worden maximaal 2 jaar bewaard. Wij constateren dat in de productieomgeving de RMC's alleen toegang hebben tot de jaargangen 2014, 2015 en de lopend jaargang 2016. Dit is conform de overeengekomen bewaartermijn van 2 jaar voor het inhoudelijk dossier.	Niet OK Er is nog geen schoningsprocedure opgesteld voor het verwijderen van de gegevens uit de (archief) databases. Advies: Stel een schoningsprocedure op voor het verwijderen van de tot een persoon herleidbare informatie nadat de bewaartermijn is overschreden.

Nr.	IB-vraag	Waarneming	Oordeel
		De databases worden handmatig verwijderd, meestal bij het klaarzetten van een nieuw schooljaar. Wij constateren dat voor Intergrip de (archief)databases nog inzichtelijk zijn tot 2012. Er is nog geen schoningsprocedure opgesteld voor het verwijderen van de gegevens. Vanuit beveiligingsperspectief is het niet wenselijk om persoonsgegevens oneindig te bewaren.	
18	Zijn er met de leverancier afspraken over de inzet van data uit het systeem?	Voor de ontwikkel- en testomgevingen zijn productiegegevens geanonimiseerd. Hiertoe zijn de identificerende leerlinggegevens uit de portals verwijderd en is gebruik gemaakt van random nummers en dergelijke. De nieuwe set is vervolgens beschikbaar gesteld voor de ontwikkel- en testomgeving. Wij hebben waargenomen dat bij het invullen van testgegevens er geen 'hit' was op de gegevens in de productieomgeving. Uit onze waarnemingen blijkt dat niet met productiegegevens wordt getest.	OK De inzet van data is adequaat.
19	Heeft de leverancier de productie- en testomgevingen van het systeem voldoende van elkaar gescheiden?	De productieomgeving is compleet gescheiden van de testomgeving. De productieomgeving heeft een ander IP-adres. De database en data op productie is niet te benaderen vanuit een andere omgeving. De testomgeving is binnen Intergrip de verzamelnaam voor de volgende omgevingen: ♦ Test omgeving: http://portal.intergriptest.nl ♦ Demo omgeving: http://portal.intergripdemo.nl ♦ Beta omgeving: http://portal.intergripbeta.nl Wij hebben waargenomen dat er een separate productieomgeving is naast de testomgevingen. Wij constateren dat ook uit de Url blijkt dat het om een testomgeving gaat. Uit de waarnemingen blijkt dat de gegevens in de testomgeving geen productiegegevens bevatten. Wij hebben dit gevalideerd door raadpleging van de productieomgeving met testgegevens en geconstateerd dat dit niet leidt tot een 'hit' in de productieomgeving.	OK De productie- en testomgevingen zijn in voldoende mate van elkaar gescheiden.

Nr.	IB-vraag	Waarneming	Oordeel
20	Hebben de school en de leverancier een duidelijke gebruikersautorisatie procedure ingebouwd in de applicatie?	Wij hebben geobserveerd dat voor de gebruikers (leerlingen) een duidelijk proces en portaal zijn ingericht voor het aanvragen van een account. Wij hebben het aanmaken van accounts opnieuw uitgevoerd in de testomgeving. Wij constateren dat accounts worden aangemaakt en vervolgens een activatielink en code wordt gestuurd naar een opgegeven emailadres. Wij constateren dat duidelijke afspraken zijn gemaakt met de RMC's over wie de aanspreekpunten zijn voor het aanvragen van accounts. De Helpdesk van Intergrip handelt de autorisatieverzoeken af en toetst daarbij of een autorisatieverzoek komt van een binnen de RMC gemandateerd persoon. Binnen de RMC's gelden specifieke afspraken over de verdere invulling van het autorisatiebeheer. Intergrip biedt het platform, maar is niet inhoudelijk verantwoordelijk voor de toegekende autorisaties binnen de RMC's, tenzij specifiek overeengekomen. De contactpersonen die gerechtigd zijn voor het aanmaken van accounts, worden op voorhand tezamen met de deelnemende RMC's vastgelegd. Wij constateren dat in de applicaties van Intergrip rollen zijn aangemaakt met rechten op basis van 'need to know' en 'need to have' principes. Wij constateren dat de supervisorrol over alle rechten beschikt. Deze kan andere gebruikers aanmaken. De rollen kennen een hierarchische structuur. Rollen kunnen alleen gebruikers met een gelijke of lagere autorisaties aanmaken en koppelen aan rollen die gelijke of minder rechten hebben. Tevens hebben wij waargenomen dat een gebruiker-id wordt toegekend aan een regio (RMC) en een systeem (VO-MBO, DDD), en dat deze een type rol (VO, MBO, Admin) krijgt. De door het RMC aangewezen projectleider krijgt de admin-rol en is onder andere verantwoordelijk voor: ♦ Het aanmaken van de juiste instanties voor een regio; ♦ Het instellen van de 'beheerders' van instanties; ♦ Het regelmatig aansporen van beheerders tot het bijwerken van gebruikersgegevens; ♦ Het beheren van de administrator-rollen in de eigen regio.	OK met advies De procedure voor het beheer van autorisaties is adequaat, met uitzondering van de reconciliatie. Advies: Omdat autorisatiebeheer een ketenverantwoordelijkheid is het wenselijk om periodiek een validatie van de uitgegeven gebruikersautorisaties bij de RMC's, inclusief de autorisaties van Intergrip-medewerkers, uit te voeren. Advies: Maak de accountscontrole onderdeel van de uitdienstprocedure.

Nr.	IB-vraag	Waarneming	Oordeel
		Per instantie (vo, mbo of Gemeente) kan een beheerder worden aangesteld. Deze persoon is verantwoordelijk voor: ♦ Het aanmaken van rollen binnen de eigen instantie; ♦ Het verwijderen van rollen binnen de eigen instantie. Voor een vo- of mbo-gebruiker zal altijd een vo- of mbo-instelling moeten worden ingevuld. Wij constateren dat in de productieomgeving de RMC's alleen toegang hebben tot de jaargangen 2014, 2015 en de lopend jaargang 2016. Dit is conform de overeengekomen bewaartermijn van 2 jaar voor het inhoudelijk dossier. De databases worden handmatig verwijderd, meestal bij het klaarzetten van een nieuw schooljaar. Wij constateren dat voor Intergrip de (archief)databases nog inzichtelijk zijn tot 2012. Wij constateren dat de beheerders van Intergrip allen beschikken over Supervisor rechten. Dit is vanuit beheeroogpunt een bewuste keuze. Wij constateren dat in de gebruikerslijst nog oud-medewerkers stonden. Het intrekken van de autorisaties voor eigen personeel vormde nog geen vast onderdeel van de uitdienstprocedure.	
21	Ondertekenen personeel, externen en andere partijen die toegang hebben tot de gegevens in het systeem van de leverancier een geheimhoudingsverklaring?	Het personeel, externen en andere partijen die toegang hebben tot de gegevens in het systeem van de leverancier tekenen een geheimhoudingsverklaring. Wij constateren dat de recentelijk aangenomen medewerkers een geheimhoudingsverklaring hebben ondertekend. De geheimhoudingsverklaring vormt een standaard onderdeel van de medewerkerscontracten.	OK Het proces rondom de geheimhoudingsverklaring is adequaat.

Nr.	IB-vraag	Waarneming	Oordeel
22	Wordt er genoeg logging bijgehouden in het systeem? En wordt deze ook veilig bewaard?	Wij constateren dat er reguliere auditlogging plaatsvindt op de systemen van Intergrip. Deze logging registreert het inloggen van gebruikers en beheerders en systeemmeldingen. Wij constateren dat er transactielogging plaatsvindt op de systemen van Intergrip. Deze logging wordt drie dagen bewaard. Een langere bewaartermijn wordt nu niet gedaan door de grote aantallen wijzigingen in de gegevens in de systemen. De gebruikersraadplegingen (CRUD-queries) worden eveneens gelogd. Deze bewaartermijn van drie dagen is gekozen omdat dit voldoende wordt geacht voor het verhelpen van gebruikersproblemen. De logs worden op de productieserver aangehouden.	OK Het proces rondom de logging is adequaat.
23	Zijn er afspraken tussen school en leverancier over beschikbaarheid van de dienst?	Er zijn afspraken tussen onderwijsinstelling en de leverancier over de beschikbaarheid van de dienstverlening. De Intergrip-systemen zijn web-based en gehost op de server van Intergrip. In de generieke SLA en het gesampled contract staat vermeld: ♦ Gecontroleerde downtime in verband met updates en onderhoud wordt ’s nachts uitgevoerd en zal daarmee het gebruik van het systeem niet in de weg staan; ♦ De servers worden dag en nacht gemonitord waarmee de performance, maar ook de snelheid van de server wordt bewaakt; ♦ De ervaring van uptime vanuit de praktijk is 99,5%. De uptime wordt niet gegarandeerd. Wij constateren dat Intergrip gebruik maakt van verschillende contractsjablonen en daarnaast een model SLA hanteert. In de SLA 2016 zijn het beschikbaarheidspercentage en de meetmomenten voor onbeschikbaarheid gedefinieerd en eenduidige Key Performance Indicatoren (KPI’s). Intergrip levert geen service level rapportages aan onderwijsinstellingen.	OK met advies Er zijn afspraken tussen de school en de leverancier over beschikbaarheid en er zijn maatregelen getroffen. Er is geen rapportage aan de school over beschikbaarheid. Advies: Overweeg een externe beschikbaarheidsrapportageprocedure te formaliseren en te documenteren als onderdeel van standaard service level rapportages.
24	Zijn er afspraken tussen school en leverancier over hersteltijden van storingen?	Er zijn afspraken (in een SLA) tussen onderwijsinstelling en de leverancier over hersteltijden van storingen. De Intergrip-systemen zijn web-based en gehost op de server van Intergrip. In de generieke SLA en het gesampled contract staat vermeld:	OK Er zijn afspraken tussen de school en de leverancier over hersteltijden en er zijn maatregelen getroffen.

Nr.	IB-vraag	Waarneming	Oordeel
		♦ Gecontroleerde down time in verband met updates en onderhoud wordt ’s nachts uitgevoerd en zal daarmee het systeem niet in de weg staan; ♦ De servers worden dag en nacht gemonitord waarmee de performance, maar ook de snelheid van de server wordt bewaakt; ♦ De ervaring van uptime is 99,5%, deze wordt niet gegarandeerd; ♦ In het geval van worst case scenario is het systeem binnen 72 uur weer online op een ander domein. Intergrip plaatst de laatste back-up dan op dit nieuwe domein; ♦ Intergrip is tijdens kantooruren beschikbaar van 8:30 tot 17:00 uur; ♦ De reactietijd is binnen 24 uur op werkdagen. Dit betreft de tijd tussen het aanmelden van een incident en een schriftelijke of mondelinge reactie daarop; ♦ De hersteltijd voor showstoppers is 24 uur, mits dit mogelijk is gezien de aard van het incident. Mocht de aard van het issue meer hersteltijd nodig hebben, zal Intergrip doorgaan met de inspanningen die nodig zijn voor herstellen, tot het issue is opgelost. Er wordt geen garantie gegeven over response- of hersteltijden. Wij constateren dat Intergrip gebruik maakt van verschillende contractsjablonen en daarnaast een model SLA hanteert.	
25	Zijn er afspraken tussen school en leverancier over procedures voor het melden van incidenten?	De contracten zijn per RMC niet geheel gelijk. Wij constateren dat Intergrip gebruik maakt van verschillende contractsjablonen en daarnaast een model SLA hanteert. In de contracten is een verwijzing opgenomen naar hersteltijden en reactietijden van de service desk. De service desk vormt het eerste aanspreekpunt voor incidenten. Uit interviews en documentreview blijkt dat Intergrip op dit moment werkt aan nieuwe bewerkersovereenkomsten. In deze overeenkomten zal de Meldplicht Datalekken worden opgenomen. Hiermee wordt de procedure voor het melden van incidenten een onderdeel van de afspraken tussen onderwijsinstellingen en Intergrip. De Helpdesk van Intergrip is bereikbaar en wordt ook gevonden in geval van beveiligings- of functionele problemen. Intergrip zegt in haar SLA toe binnen 72 uur online te kunnen zijn in een ‘worst case scenario’.	OK De incidentenprocedure is adequaat.

Nr.	IB-vraag	Waarneming	Oordeel
		Wij constateren dat incidenten worden geregistreerd in het Zendesk ticketingsysteem van Intergrip. Indien de software moet worden aangepast, wordt de informatie aan JIRA tickets toegevoegd om te worden meegenomen in de software ontwikkeling.	
26	Zijn er afspraken tussen school en leverancier over incidentrapportages?	De contracten zijn per RMC niet geheel gelijk. Wij constateren dat Intergrip gebruik maakt van verschillende contractsjablonen en daarnaast een model SLA hanteert. In de contracten is een verwijzing opgenomen naar hersteltijden en reactietijden van de service desk. De service desk vormt het eerste aanspreekpunt voor incidenten. Er zijn geen contracturele afspraken tussen school en leverancier over incidentrapportages. Uit interviews en documentreview blijkt dat Intergrip op dit moment werkt aan nieuwe bewerkersovereenkomsten. In deze overeenkomsten zal de Meldplicht Datalekken worden opgenomen. Hiermee wordt incidentrapportage een onderdeel van de afspraken tussen onderwijsinstellingen en Intergrip. Wij constateren dat incidenten worden geregistreerd in het Zendesk ticketingsysteem van Intergrip. Indien de software moet worden aangepast, wordt de informatie aan JIRA-tickets toegevoegd om te worden meegenomen bij de ontwikkeling van de software.	OK Incidentrapportage wordt een onderdeel van de afspraken tussen onderwijsinstellingen en Intergrip.

Deze pagina is blanco vanwege dubbelzijdig printen.

5. Opdrachtomschrijving

Noordbeek heeft op 24 januari 2016 van de Stichting Kennisnet, namens saMBO-ict en Intergrip B.V., de opdracht gekregen om een onderzoek uit te voeren naar de privacyaspecten van het systeem Intergrip, in de vorm van een Privacy Impact Assessment (PIA). Hiermee wordt getoetst of het verzamelen en verwerken van persoonsgegevens voldoet aan het gestelde in de Wet bescherming persoonsgegevens (Wbp).

De Stichting Kennisnet vertegenwoordigt de onderwijsinstellingen die gebruik maken van Intergrip en ondersteunt de MBO Raad en saMBO-ICT.

Noordbeek heeft het onderzoek uitgevoerd aan de hand van het normenkader opgenomen in de uitvraag van Stichting Kennisnet. Het normenkader is gebaseerd op de vereisten uit het certificeringsschema 1.1 van Edustandaard en ingevuld naar de risico's voor de overdracht van persoonsgegevens tussen vo- en mbo-instellingen.

5.1. De onderzoeksvraag

De onderzoeksvragen hierbij zijn:

- Wordt in dit voortbrengingsproces op basis van de actuele wet- en regelgeving rondom privacy gewerkt, zoals de Wbp en specifieke onderwijswetgeving?
- Zijn, op basis van deze wet- en regelgeving, voldoende maatregelen voor informatiebeveiliging en privacybescherming getroffen?
- Kan de correcte werking van deze maatregelen, eventueel steekproefsgewijs, worden aangetoond in Intergrip?
- Wat zijn, voor de implementatie en het gebruik van Intergrip, aanbevelingen voor Intergrip B.V. (als opdrachtnemer) en de onderwijsinstellingen (als opdrachtgever) om indien nodig de informatiebeveiliging en privacybescherming te verbeteren?

5.2. Scope

De privacyscan is primair gericht op de bedrijfsvoering, de ondersteunende IT-middelen benodigd voor de verwerking van de privacygevoelige persoonsgegevens en de relevante getroffen beheersmaatregelen voor de IT-middelen.

Van de scope is uitgesloten de toetsing van de technische infrastructuur (technical audit), het operationeel informatiesysteem (system audit) en de procesinrichting (ITIL-audits).

Er is geen onderzoek uitgevoerd naar de werking van de beheersingsmaatregelen in continuïteit.

5.3. De onderzoeksaanpak

Noordbeek is in week vijf en zes gestart met de voorbereidingsfase, welke bestaat uit twee verkennende interviews, het opvragen van documentatie en het opstellen van vragenlijsten. Via deskresearch en gebruikmakend van het normenkaders zoals opgenomen in de uitvraag vanuit Kennisnet zijn vragenlijsten geconcipieerd voor het evaluatieonderzoek. Deze vragenlijsten zijn met de opdrachtgever afgestemd.

In overleg met de opdrachtgever is de lijst van de te interviewen medewerkers opgesteld. Wij hebben diverse inhoudelijke onderzoeksinterviews uitgevoerd tussen 11 en 25 februari 2016. Van ieder interview zijn de hoofdpunten uitgewerkt in gespreksverslagen. Daarnaast hebben wij waarnemingen van de systeeminstellingen uitgevoerd en de documentatie bestudeerd.

Onze waarnemingen via de deskresearch en de interviews vormen de IST-positie. Uit de vergelijking van de SOLL met de IST volgen de GAP's, oftewel de bevindingen. Wij hebben deze gemotiveerd omschreven en, waar mogelijk, volgend uit onze natuurlijke adviesfunctie als auditors, aangevuld met een pragmatisch voorstel voor mogelijke mitigerende maatregelen per bevinding.

Wij hebben deze opdracht voor overeengekomen werkzaamheden uitgevoerd en hierover gerapporteerd conform de richtlijnen van de Nederlandse Orde van Register IT Auditors (NOREA).

5.4. Het onderzoeksteam

De uitvoering van de werkzaamheden is verzorgd door:

- Prof.dr.ir. R. Paans RE (Ronald), hoogleraar aan de Postgraduate Opleiding IT Audit, Compliance & Advisory van de Vrije Universiteit en directeur van Noordbeek;
- L. Benschop MSc RE CISA (Leo), IT Audit Manager;
- A.J. Stroo MSc (Arjen), IT Auditor.

De eindverantwoordelijkheid voor de uitvoering van de opdracht berust bij ondergetekende, directeur van Noordbeek.

5.5. Ondertekening

Dit rapport is alleen bedoeld voor het informeren van de opdrachtgevers en voor het verder verbeteren van het informatiesysteem Intergrip en de bijbehorende procedures, en is niet bedoeld voor verdere verspreiding.

Wij eindigen met een woord van dank voor de geïnterviewden, die naar onze mening op een open en transparante wijze alle door ons gevraagde informatie hebben verstrekt.

Hazerswoude, 18 april 2016

Prof.dr.ir. R. Paans RE
Directeur van Noordbeek B.V.

Documentbeheer

Doelgroep: saMBO-ICT, Intergrip B.V. en Stichting Kennisnet

Versie	Datum	Naam	Verandering
0.01	08-02-2016	R. Paans	Initiële opzet
0.09	29-02-2016	L.A.T. Benschop A.J. Stroo	Verwerken bewijs
0.16	13-03-2016	L.A.T. Benschop A.J. Stroo	Verwerken bewijs en bevindingen
0.17	14-03-2016	R. Paans	Oordeelsvorming
0.70	27-03-2016	R. Paans	Verwerken ontvangen feedback
0.90	03-04-2016	K.C. Schoon	Kwaliteitscontrole
0.92	09-04-2014	R. Paans	Verwerken detail feedback
1.00	18-04-2016	R. Paans	Finaliseren

Accordering

Versie	Datum	Reviewer	Status en doel
0.17	21-03-2016	J. Bartling	Feedback
0.17	21-03-2016	E. Hooijer A. Dankelman	Feedback en nieuwe input (SLA)
0.70	01-04-2016	J. Bartling	OK
0.90	08-04-2016	E. Hooijer A. Dankelman	OK met detail feedback
0.92	13-04-2016	E. Hooijer A. Dankelman	OK
	18-04-2016	J. Bartling	OK