TOETSFORMULIER VERWERKERSOVEREENKOMSTEN - PRIVACY CONVENANT MODEL 4.0	<LEVERANCIER>	<PRODUCT/DIENST>	THEORETISCHE TOETS	DATUM	PRAKTISCHE TOETS	DATUM	REACTIE LEVERANCIER	<datum>	REACTIE SIVON	<datum>
Toets - Verwerkersovereenkomst	initiële toets door <expert>	<datum>	controle door SIVON	<datum>	met bijdrage <onderwijsinstelling>	<datum>	reactie Leverancier	<datum>	reactie SIVON	<datum>
Toets - Bijlage 1: Privacybijsluiter	initiële toets door <expert>	<datum>	controle door SIVON	<datum>	met bijdrage <onderwijsinstelling>	<datum>	reactie Leverancier	<datum>	reactie SIVON	<datum>
Toets - Bijlage 2: Beveiligingsbijlage	initiële toets door <expert>	<datum>	controle door SIVON	<datum>	met bijdrage <onderwijsinstelling>	<datum>	reactie Leverancier	<datum>	reactie SIVON	<datum>
Toets - Bijlage 3: Wijzigingenbijlage (indien van toepassing)	initiële toets door <expert>	<datum>	controle door SIVON	<datum>	met bijdrage <onderwijsinstelling>	<datum>	reactie Leverancier	<datum>	reactie SIVON	<datum>
Toets - Verwerkersovereenkomst	**Opgenomen (volledig en juist)? [Ja/Nee]**	**Toelichting**	**Vraag of opmerking richting Leverancier**	**Risico [L/M/H]**	**Extra vragen/opmerkingen**	**Risico [L/M/H]**	**Reactie Leverancier**	**Risico [L/M/H]**	**Reactie SIVON**	**Risico [L/M/H]**
Verwerkersovereenkomst behorende bij Convenant Digitale Onderwijsmiddelen en Privacy 4.0										
Naam/Versie/Datum aangeboden verwerkersovereenkomst										
Ondergetekende - Verwerker: naam, juridische entiteit, KvK-nummer, tekenbevoegde					Indien dit niet tijdens de Theoretische toets is gecontroleerd: Klopt de naamgeving van de Leverancier en juridische entiteit ook daadwerkelijk met de KvK? En komt deze overeen met de onderliggende overeenkomst (hoofdovereenkomst)?					
Overwegen het volgende: verwijzing onderliggende overeenkomst (naam en datum) en benoeming product/dienst										
Verschillen geconstateerd tov Verwerkersovereenkomst Model 4.0?										
Zo ja, opgenomen in Bijlage 3: Wijzigingenbijlage										
Toets - Bijlage 1: Privacybijsluiter	**Opgenomen (volledig en juist)? [Ja/Nee]**	**Toelichting**	**Vraag of opmerking richting Leverancier**	**Risico [L/M/H]**	**Extra vragen/opmerkingen**	**Risico [L/M/H]**	**Reactie Leverancier**	**Risico [L/M/H]**	**Reactie SIVON**	**Risico [L/M/H]**
A. Contactgegevens Verwerker en Onderwijsinstelling										
• Functie contactpersonen										
• Contactgegevens (e-mailadres, telefoonnummer)										
B. Versienummer en versiedatum										
Het meest recente versienummer van de Privacybijsluiter en de datum daarvan worden hier vastgelegd.										
C. Algemene informatie										
Het gaat hierbij om informatie over:										
• Naam product en/of dienst					Komt de naam van het product/dienst overeen met de naam ervan in de onderliggende overeenkomst, in de 'overwegen het volgende' bij de vwo, in de applicatie zelf, en op de website (zie link naar productpagina) en in handleidingen?					
• Naam Verwerker en vestigingsgegevens										
• Link naar Leverancier (website/URL)										
• Link naar productpagina (website/URL)					Controleer of er een productpagina/productwebsite is en of deze overeenkomt. Deze kan afwijken van de website van de Leverancier. En, hiermee bedoelen we niet de inlogpagina. Deze is vaak afwijkend en komt in Bijlage 2 terug.					
• Beknopte uitleg en werking product en/of dienst					Komt dit overeen met de daadwerkelijke werking van de applicatie? Check hier ook of dit (grotendeels, hoeft niet per se letterlijk) overeenkomt met de beschrijving in de onderliggende overeenkomst en de website (productpagina/handleiding/instructievideo).					
• Doelgroep (po/vo/(v)so/mbo)					Kloppen deze doelgroepen met het daadwerkelijk gebruik van de applicatie of benoeming daarvan op de website (productpagina/handleiding/demo)? Indien er meer doelgroepen zijn, is er dan een aparte VWO voor die doelgroepen?					
• Gebruikers (Onderwijsdeelnemers/ouders/verzorgers/medewerkers)					Komen de Categorieen Gebruikers overeen met de Categorieen Betrokkenen (zie F.1)? Komen de Gebruikers overeen met de gebruikers(groepen) in de applicatie zelf? Strookt dit met de website (productpagina/handleiding/demo)?					
D. Omschrijving specifieke producten en/of diensten Dit onderdeel bestaat uit een: *					Is er een dataflow-diagram dat inzichtelijk maakt hoe de gegevensstroom is tussen de verschillende onderdelen/modules (onlosmakelijke onderdelen en optionele onderdelen) en de koppelingen met derde partijen? Staan optionele onderdelen 'by default' uit, zijn deze niet zichtbaar (privacy by design/by default)? Kan de applicatiebeheerder optionele modules en koppelingen zelf beheren, dus aan- of uitzetten?					
a. omschrijving van producten en/of diensten en bijbehorende Verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product en/of de aangeboden dienst, inclusief de koppelingen en uitwisseling met derde partijen;					Klopt de weergave hiervan met de praktijk? Controleer de beheeromgeving op mogelijke modules (controleer ook de website, brochures, hoofdovereenkomst en evt. SLA/DAP), diensten (bijv. mail vanuit de applicatie), uitwisselingen (bijv. met andere verwerkingsverantwoordelijken) en koppelingen (bijv. met andere onderwijsleveranciers) en kijk naar partners/samenwerkingen.					
b. omschrijving van aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de Verwerker aanbiedt, inclusief de koppelingen en uitwisseling met derde partijen.					Klopt de weergave hiervan met de praktijk? Controleer de beheeromgeving op mogelijke modules (controleer ook de website, brochures, hoofdovereenkomst en evt. SLA/DAP), diensten (bijv. mail vanuit de applicatie), uitwisselingen (bijv. met andere verwerkingsverantwoordelijken) en koppelingen (bijv. met andere onderwijsleveranciers) en kijk naar partners/samenwerkingen.					
E. Doeleinden voor het verwerken van Persoonsgegevens *										
In dit onderdeel wordt vastgelegd welke doeleinden, zoals vastgelegd in artikel 5 van het Convenant, van toepassing zijn op de Verwerking van Persoonsgegevens met behulp van de specifieke producten en/of diensten.					Zijn alle doeleinden die van toepassing zijn aangekruist? Anders mag de verwerking voor die doeleinden niet plaatsvinden. Standaard zijn dat 'Logging' en Daarnaast zijn de doeleinden in Artikel 5 van het Convenant niet limitatief (en vooral gericht op leerlingen en ouders/verzorgers als primaire betrokkenen), dus controleer vooral of er andere doeleinden zijn en zorg dat deze benoemd zijn. Vraag of maak een verbinding met FORA.					
F. Categorieën Persoonsgegevens inclusief bewaartermijnen Dit onderdeel bestaat uit: *										
1. een omschrijving van de categorieën Betrokkenen (o.a. Onderwijsdeelnemers, ouders/verzorgers, medewerkers) over wie Persoonsgegevens worden verwerkt, en de te verwerken categorieën Persoonsgegevens van deze Betrokkenen, en					Komen de aangegeven categorieen overeen met het gebruik van het product/dienst (de applicatie) in de praktijk? Ontbreken er categorieen in de VWO of juist in de applicatie? Let ook op (soms zelf in te richten) optionele/vrije velden of rubrieken.					
2. door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen).					Er is volgens Artikel 12 van de Model VWO een onderscheid te maken tussen bewaartermijnen en afspraken (bijv. teruggave) na afloop van de onderliggende (hoofd)overeenkomst [lid 2] en de bewaartermijnen die gelden in het kader van wet- en regelgeving (bijv. AVG, Archiefwet en/of een eigen selectielijst) [lid 1]. Wordt dit onderscheid gemaakt? En staat in ieder geval benoemd wat de bewaartermijn is inzake lid 2?					
G. Locatie van opslag en Verwerking Persoonsgegevens										
Onder G. wordt vastgelegd wat de plaats(en)/land(en) van opslag en Verwerking van de Persoonsgegevens zijn.					Controleer aan de hand van H of deze gegevens kloppen.					
H. Subverwerkers										
Verwerker legt hier vast van welke Subverwerkers hij ten tijde van het afsluiten van de Verwerkersovereenkomst gebruikmaakt.					Controleer vanuit het gebruik van de applicatie of deze lijst volledig en juist is. Regelmatig worden Subverwerkers over het hoofd gezien, bijv. de hostingpartij(en!) of de partij die de e-maildienst binnen de applicatie levert. Check ook op cookies (via Cookiebot). Doe bijvoorbeeld naast een test op moderne en veilige internetstandaarden ook een WHOIS-lookup op basis van IP-adres. Kijk hiervoor ook naar onderdeel D. Is de model tabel volledig ingevuld? Controleer ook of er sprake is van een holding en waar het moederbedrijf is gevestigd ivm verplichte doorgifte aan autoriteiten.					
** Indien een Verwerker de Variant Model Bijlage 1 gebruikt dienen D t/m H per product/dienst/module bekeken te worden*										

Toets - Bijlage 2: Beveiligingsbijlage	**Opgenomen (volledig en juist)? [Ja/Nee]**	**Toelichting**	**Vraag of opmerking richting Leverancier**	**Risico [L/M/H]**	**Extra vragen/opmerkingen**	**Risico [L/M/H]**	**Reactie Leverancier**	**Risico [L/M/H]**	**Reactie SIVON**	**Risico [L/M/H]**
Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.										
A. Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.										
• Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast.					Leverancier: Is er een beveiligingsbeleid? Zo ja, graag inzicht geven. Zijn er beveiligingscertificaten, DPIA's, pentesten of andere rapportages op basis waarvan waarborgen op het gebied van IB en P worden geleverd? Wordt het ROSA-certificeringsschema gebruikt of zijn er andere relevante beveiligingscertificaten? Is er een verklaring van toepasselijkheid (TPM)? Graag aanleveren.					
• Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.										
• Verwerker heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van Persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.										
• Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.										
• Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.										
• Verwerker sluit met medewerkers geheimhoudingsverklaringen af en maakt informatiebeveiligingsafspraken.										
• Verwerker stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.										
B. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.										
Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Verwerker gebruikt hiervoor in beginsel het 'Certificeringsschema informatiebeveiliging en privacy ROSA' (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.										

Toetsvorm					Indien gekozen is voor een self-assessment vraag of de leverancier van plan is minimaal een assessment door een peer of beter een onafhankelijke audit te laten uitvoeren en op welke termijn?					
Uitvoerder toets										
Inlogpagina					Voldoen alle gebruikte (web-/sub-/mail-)domeinen aan moderne en veilige internetstandaarden, te testen via internet.nl?					
BIV-classificatie					Valt er iets op aan deze BIV-classificatie? Is deze BIV-classificatie overeenkomstig de classificatie die er door de Onderwijsinstelling aan wordt gegeven? Is duidelijk waarom tot deze classificatie is gekomen?					
Categorie | Maatregelen | Compliance | Uitleg										
Beschikbaarheid (alleen opnemen, indien niet voldaan of bij alternatieve maatregel en/of bij vragen/opmerkingen over de uitleg)										
Integriteit (alleen opnemen, indien niet voldaan of bij alternatieve maatregel en/of bij vragen/opmerkingen over de uitleg)										
Vertrouwelijkheid (alleen opnemen, indien niet voldaan of bij alternatieve maatregel en/of bij vragen/opmerkingen over de uitleg)										
C. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken										
Verwerker heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zal Verwerker de Verwerkingsverantwoordelijke de volgende informatie ter hand stellen:					Opvragen					
• de kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens);										
• de oorzaak van de inbreuk;										
• hoe de inbreuk is ontdekt;										
• de maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;										
• of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht etc. waren;										
• de groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen;										
• wat de mogelijke gevolgen zijn van de inbreuk voor Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor groep(en) Betrokkene(n);										
• de hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).										
In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Verwerker, in beginsel per e-mail, contact met elkaar opnemen via onderstaande contactgegevens, dan wel de contactgegevens zoals opgenomen in Bijlage 4.										
Verwerker (naam, functie, e-mail en telefoonnummer)										
Onderwijsinstelling (naam, functie, e-mail en telefoonnummer)										
Toets - Bijlage 3: Wijzigingenbijlage (indien van toepassing)	**Opgenomen (volledig en juist)? (Ja/Nee)**	**Toelichting**	**Vraag of opmerking richting Leverancier**	**Risico [L/M/H]**	**Extra vragen/opmerkingen**	**Risico [L/M/H]**	**Reactie Leverancier**	**Risico [L/M/H]**	**Reactie SIVON**	**Risico [L/M/H]**
Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.										
1. Beschrijving noodzakelijke afwijkingen Model Verwerkersovereenkomst incl. Bijlagen										
Betreft artikel										
Wijziging of aanvulling?										
Huidige tekst artikel										
Nieuwe tekst artikel (onderstreep wijzigingen en aanvullingen)										
Reden van wijziging of aanvulling (noodzaak en motivering)										