Bijlage XI Verwerkersovereenkomst

DE ONDERGETEKENDEN:

I De Stichting **Calvijn College,** statutair gevestigd te Middelburg en kantoorhoudende te 4461 ZN Goes aan Klein Frankrijk 19, ingeschreven in het handelsregister onder nummer KvK 20140185, in deze rechtsgeldig vertegenwoordigd door haar statutair bestuurder Jan Bakker, hierna te noemen "***Verwerkingsverantwoordelijke***",

en

II. De besloten vennootschap met beperkte aansprakelijkheid **[…] B.V.**, statutair gevestigd en kantoorhoudende te ([postcode]) [plaats] aan de [adres], ingeschreven in het handelsregister onder nummer [nummer], in deze rechtsgeldig vertegenwoordigd door haar statutair bestuurder [naam], hierna te noemen "***Verwerker***",

OVERWEGINGEN:

A. Verwerker levert diensten aan Verwerkingsverantwoordelijke in het kader van […] en/of zal die diensten gaan leveren;
B. Verwerker zal ten behoeve van de uitvoering van de onder A genoemde diensten persoonsgegevens gaan verwerken van [leerlingen/personeel] van Verwerkingsverantwoordelijke waarvoor Verwerkingsverantwoordelijke verantwoordelijk is in de zin van de Algemene verordening gegevensbescherming (AVG);
C. Verwerkingsverantwoordelijke zal deze persoonsgegevens aan Verwerker verstrekken, althans Verwerker zal deze persoonsgegevens onder verantwoordelijkheid van Verwerkingsverantwoordelijke verkrijgen;
D. Partijen willen, gelet op het bepaalde in artikel 28 lid 3 AVG, de voorwaarden van de verwerking van deze persoonsgegevens vastleggen in deze overeenkomst.

KOMEN OVEREEN ALS VOLGT:

Artikel 1. Definities

1.1. In deze overeenkomst betekenen de volgende begrippen hetgeen daarbij hieronder is vermeld wanneer zij met een hoofdletter worden geschreven:

Artikel: een artikel van de Overeenkomst;

AVG:	de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene verordening gegevensbescherming);
Betrokkene:	degene op wie een persoonsgegeven betrekking heeft;
Beveiligingsincident:	een inbreuk op de beveiliging, waarbij persoonsgegevens zijn blootgesteld aan vernietiging, verlies, wijziging, of ongeoorloofde vertrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens;
Datalek:	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde vertrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens;
Geheimhoudingsverklaring:	de geheimhoudingsverklaring zoals bedoeld in bijlage 3;
Opdracht:	de overeenkomst van opdracht tussen Verantwoordelijk en Verwerker tot het uitvoeren van [diensten];
Overeenkomst:	onderhavige verwerkersovereenkomst inclusief bijlagen;
Partijen:	Verwerkingsverantwoordelijke en Verwerker;
Persoonsgegeven(s):	elk gegeven betreffende een geïdentificeerd of identificeerbare natuurlijke persoon, die Verwerker bij of in verband met het uitvoeren van de Opdracht verkrijgt;
[Subverwerker(s):	de subverwerker(s) als bedoeld in Artikel 3.1.]

Artikel 2. Onderwerp

2.1. Verwerker en Verwerkingsverantwoordelijke zullen handelen conform de Algemene verordening gegevensbescherming (AVG), de Telecommunicatiewet, en alle overige privacyregelgeving.

2.2. Verwerkingsverantwoordelijke heeft en houdt volledige zeggenschap over de Persoonsgegevens.

2.3. Verwerker verwerkt de Persoonsgegevens op behoorlijke en zorgvuldige wijze.

2.4. Verwerker verwerkt de Persoonsgegevens uitsluitend in het kader van de uitvoering van de Opdracht conform de instructies van Verwerkingsverantwoordelijke, in overeenstemming met de door Verwerkingsverantwoordelijke bepaalde doeleinden en middelen, met inachtneming van de door Verwerkingsverantwoordelijke vastgestelde bewaartermijnen en met inachtneming van de door Verwerkingsverantwoordelijke vastgestelde regels met betrekking tot de toegang tot de Persoonsgegevens, zoals beschreven in bijlage 1.

2.5. Verwerker zal onder geen omstandigheid de Persoonsgegevens verder verwerken dan bepaald onder Artikel 2.4. Verwerker zal, bijvoorbeeld, de Persoonsgegevens niet voor eigen doeleinden of die van derden verwerken noch de Persoonsgegevens aan derden verstrekken, behoudens de verstrekking van Persoonsgegevens aan Subverwerkers in het kader van de uitvoering van de Opdracht.

Artikel 3. [Inschakeling derden]

3.1. [Verwerker is gerechtigd bij de verwerking van de Persoonsgegevens [naam] als subverwerker(s) in te schakelen.]

3.2. [Verwerker is niet gerechtigd bij de verwerking van de Persoonsgegevens een andere Subverwerker in te schakelen dan genoemd in Artikel 3.1 zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Toestemming zal niet zonder redelijke grond worden geweigerd. Verwerkingsverantwoordelijke kan aan die toestemming nadere voorwaarden verbinden die door Verwerker aan de Subverwerker moeten worden opgelegd.]

3.3. [Verwerker draagt er zorg voor dat de betreffende Subverwerker(s) tenminste dezelfde verplichtingen op zich nemen als opgenomen voor Verwerker in de Overeenkomst en in het bijzonder op grond van het bepaalde in Artikel 2.4. Een kopie van de subverwerkersovereenkomst met de Subverwerker is aan de Overeenkomst gehecht als bijlage 2.]

3.4. [Indien de Subverwerker die Verwerker wil inschakelen buiten de EER is gevestigd, staat Verwerker er jegens Verwerkingsverantwoordelijke voor in, onverminderd het bepaalde in Artikel 3.2, dat deze Subverwerker een passend niveau van bescherming en veiligheid van Persoonsgegevens waarborgt in de zin van de AVG en overlegt Verwerker daarvan bewijs aan Verwerkingsverantwoordelijke.]

3.5. [Verwerker blijft in de verhouding tussen Partijen altijd aanspreekpunt en volledig verantwoordelijk en aansprakelijk voor de uitvoering en naleving van de bepalingen uit de Overeenkomst voor zover zij verplichtingen scheppen voor Verwerker, inclusief de naleving van de nadere voorwaarden als bedoeld in Artikel 3.2.]

Artikel 4. Beveiligingsmaatregelen

4.1. Verwerker neemt passende technische en organisatorische maatregelen om de Persoonsgegevens adequaat te beveiligen en beveiligd te houden tegen verlies of enige vorm van onrechtmatige gebruik of verwerking, waarbij rekening wordt gehouden met de stand van de techniek, de kosten van tenuitvoerlegging van deze maatregelen en de aard van de te beschermen Persoonsgegevens.

4.2. Verwerker neemt – onder verwijzing naar het bepaalde in bijlage 1 - in ieder geval de volgende maatregelen met betrekking tot de Persoonsgegevens:

a. [encryptie (versleuteling) van digitale bestanden met [AES-128] bits;]
b. [beveiliging van netwerkverbindingen via Transport Layer Security (TLS);]
c. [aanpassen van persoonsgegevens dat zij niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder aanvullende gegevens (pseudonimisering);]
d. […]

4.3. [Verwerker heeft de technische en organisatorische maatregelen in het kader van de uitvoering van de Opdracht ingericht conform de uitgangspunten van ISO 27001/ISO 27002.]

4.4. Verwerker staat er jegens de Verwerkingsverantwoordelijke voor in dat de beveiliging van de Persoonsgegevens doeltreffend zal zijn.

Artikel 5. Meldplicht datalekken

5.1. Verwerker zal Verwerkingsverantwoordelijke onmiddellijk - doch uiterlijk binnen 36 uur na ontdekking – schriftelijk op de hoogte stellen van iedere (mogelijk) Datalek zoals die binnen de organisatie van Verwerker of Subverwerker, dan wel ten aanzien van de middelen onder beheer van Verwerker of Subverwerker, plaatsvindt. Deze melding dient plaats te vinden bij de Functionaris Gegevensbescherming van de Verwerkingsverantwoordelijke, wiens contactgegevens zijn opgenomen in bijlage 4.

5.2. Verwerker draagt zorg voor een intern beleid in het geval zich een beveiligingsincident voordoet zodat hierop adequaat gereageerd kan worden.

5.3. Indien er sprake is van een mogelijk Datalek zal Verwerker in ieder geval schriftelijk de volgende vragen als opgenomen in bijlage 5 aan de Functionaris Gegevensbescherming moeten beantwoorden.

5.4. Verwerker is gerechtigd de antwoorden op de vragen als genoemd in bijlage 5 in Artikel 5.3 gefaseerd te verstrekken aan de Functionaris Gegevensbescherming zolang alle vragen maar uiterlijk binnen 36 uur na de inbreuk zijn beantwoord.

5.5. Verwerker verplicht zich voorts de Functionaris Gegevensbescherming steeds onmiddellijk schriftelijk op de hoogte te houden van eventuele nieuwe ontwikkelingen.

5.6. Op Verwerkingsverantwoordelijke rust de verplichting indien het beveiligingsincident moet worden aangemerkt als een Datalek deze te melden aan de Autoriteit Persoonsgegevens en indien noodzakelijk tevens aan de betrokkenen, tenzij Verwerkingsverantwoordelijke om haar moverende redenen aangeeft dat de melding – overeenkomstig de opgave van Verwerkingsverantwoordelijke en enkel indien de situatie als bedoeld onder Artikel 5.1 zich voordoet – door de Verwerker of (eventuele) Subverwerker dient te worden gedaan.

5.7. Verwerkingsverantwoordelijke bepaalt voorts wanneer en op welke wijze het beveiligingsincident zal worden gecommuniceerd aan derden (waaronder in ieder geval begrepen: personeel, Subverwerkers, media, verzekeraar, brancheorganisatie en/of ketenpartners). Verwerkingsverantwoordelijke kan in overleg met Verwerker en (eventuele) Subverwerker(s) ook besluiten dat een andere partij dan Verwerkingsverantwoordelijke communiceert aan derden.

5.8. Verwerker documenteert alle beveiligingsincidenten, met inbegrip van de feiten omtrent het incident, de gevolgen daarvan en de genomen corrigerende maatregelen. Verwerker stelt deze administratie op eerste [schriftelijke] verzoek van Verwerkingsverantwoordelijke ter beschikking aan Verwerkingsverantwoordelijke.

Artikel 6. Locatie van data en doorgifte buiten EER

6.1. De Persoonsgegevens zullen door Verwerker worden opgeslagen op servers die zijn geplaatst in [Nederland].

6.2. Verwerker zal de Persoonsgegevens niet doorgeven naar een land buiten de EER zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijke voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

6.3. Toestemming zal niet zonder redelijke grond worden geweigerd door Verwerkingsverantwoordelijke. In ieder geval zal bij doorgifte van Persoonsgegevens aan een Subverwerker/derde buiten de EER sprake moeten zijn van een passend niveau van bescherming en veiligheid in de zin van de AVG, dan wel – indien er geen waarborgen zijn voor een passend beschermingsniveau - van een omstandigheid als genoemd in artikel 49 AVG. Verwerker overlegt daarvan bewijs aan Verwerkingsverantwoordelijke.

6.4. Partijen stellen nadrukkelijk vast dat de mogelijkheid voor een derde om Persoonsgegevens buiten de EER te kunnen raadplegen door in te loggen op de servers waarvan Verwerker gebruik maakt ten behoeve van de uitvoering van de Opdracht, is aan te merken als doorgifte van Persoonsgegevens buiten de EER.

6.5. Partijen stellen verder nadrukkelijk vast dat in ieder geval het verzenden van Persoonsgegevens met gebruikmaking van Gmail, Hotmail, Dropbox, Whatsapp en WeTransfer leidt, dan wel kan leiden, tot doorgifte van Persoonsgegevens buiten de EER.

Artikel 7. Geheimhoudingsplicht

7.1. Verwerker houdt de Persoonsgegevens geheim. Verwerker draagt ervoor zorg dat de Persoonsgegevens niet direct of indirect ter beschikking komen van derden. Onder derden wordt ook het personeel van Verwerker begrepen voor zover het niet noodzakelijk is dat zij bij de Opdracht en/of de Overeenkomst kennis hoeft te nemen van de Persoonsgegevens.

7.2. Verwerker zorgt ervoor dat het personeel dat betrokken is bij de verwerking van Persoonsgegevens, de in de Overeenkomst opgenomen verplichtingen van Verwerker kent en verplicht is die na te komen. Hiertoe heeft, of zal, Verwerker het betreffende personeel de Geheimhoudingsverklaring laten ondertekenen.

7.3. De geheimhoudingsplicht voor de Verwerker is niet van toepassing voor zover Verwerkingsverantwoordelijke uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen, indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de Opdracht en de uitvoering van deze Verwerkersovereenkomst, of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

Artikel 8. Bewaartermijnen, vernietiging en back-up

8.1. Verwerker zal Persoonsgegevens die hem in het kader van de Overeenkomst ter beschikking zijn gesteld niet langer bewaren dan noodzakelijk is (i) voor de uitvoering van de Opdracht; of (ii) om een op hem rustende wettelijke verplichting na te komen. [In bijlage 1 staat gespecificeerd hoe lang welke Persoonsgegevens worden bewaard.]

8.2. Verwerker stelt alle Persoonsgegevens met betrekking tot het/de door Verwerkingsverantwoordelijke aangegeven Project(en) op eerste schriftelijke verzoek van Verwerkingsverantwoordelijke ter beschikking aan Verwerkingsverantwoordelijke.

8.3. Verwerker stelt voorts alle Persoonsgegevens die in het kader van de Opdracht worden verwerkt uiterlijk binnen tien (10) werkdagen na het einde van de Opdracht en/of de Overeenkomst ter beschikking aan Verwerkingsverantwoordelijke, tenzij Partijen schriftelijk uitdrukkelijk anders overeenkomen.

8.4. Verwerker zal alle Persoonsgegevens waarvan Verwerkingsverantwoordelijke aangeeft dat deze moeten worden verwijderd op eerste schriftelijke verzoek van Verwerkingsverantwoordelijke volledig en onherroepelijk verwijderen van haar systemen, dan wel verwijderen uit haar administratie en deze op geen enkele andere wijze nog verwerken.

8.5. Indien na het einde van de Opdracht de Verwerkingsverantwoordelijke bevestigt dat hij alle Persoonsgegevens in een door hem schriftelijk geaccepteerd technisch formaat bezit, verwijdert Verwerker alle Persoonsgegevens volledig en onherroepelijk binnen veertien (14) dagen van haar systemen, dan wel uit haar administratie, nadat is bevestigd dat Verwerkingsverantwoordelijke de Persoonsgegevens bezit.

8.6. Verwerker kan afwijken van het in Artikel 8.4 en 8.5 bepaalde, voor zover ten aanzien van Persoonsgegevens een wettelijke bewaartermijn zou gelden of voor zover dat noodzakelijk is om tegenover Verwerkingsverantwoordelijke nakoming van zijn verbintenissen te bewijzen.

8.7. Verwerker maakt minimaal dagelijks, volgens een door Partijen overeengekomen procedure die tenminste voldoet aan de eisen van professionele toewijding, [twee reservekopieën] (back-ups) van de Persoonsgegevens. Eén van de back-ups zal worden bewaard op een andere plaats en in een ander gebouw dan waar de server staat waar Verwerker gebruik van maakt aangaande de uitvoering van de Opdracht.

Artikel 9. Register van verwerkingsactiviteiten

9.1. Verwerker houdt een register bij zoals bedoeld in artikel 30 lid 2 AVG van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van de Verwerkingsverantwoordelijke heeft verricht en is ervoor verantwoordelijk dat dit register volledig en juist is.

9.2. Dit register bevat de volgende gegevens:

a. de naam en contactgegevens van de Verwerker en Verwerkingsverantwoordelijke(n), diens vertegenwoordigers en indien van toepassing diens functionarissen voor gegevensbescherming.

b. de categorieën van verwerkingen die voor rekening van de Verwerkingsverantwoordelijke zijn uitgevoerd.

c. indien van toepassing aan welk derde land buiten de EER of welke internationale organisatie Persoonsgegevens worden doorgegeven.

d. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Artikel 10. Inlichtingen en medewerkingsplicht bij uitoefening rechten door Betrokkene

10.1. Verwerker draagt ervoor zorg dat Betrokkene al zijn rechten uit de in Artikel 2.1 opgenomen regelgeving kan uitoefenen.

10.2. Verwerker zal verder op eerste schriftelijke verzoek van Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen vijf (5) werkdagen nadat daartoe een verzoek is gedaan, overgaan tot:

a. het schriftelijk verstrekken van alle benodigde informatie die Verwerkingsverantwoordelijke nodig mocht hebben;

b. het verbeteren, aanvullen, verwijderen of afschermen van Persoonsgegevens.

10.3. Indien Betrokkene zich direct richt tot Verwerker ter uitoefening van een recht als bedoeld in Artikel 9.1, dan zal Verwerker onverwijld de Betrokkene doorverwijzen naar de Verwerkingsverantwoordelijke, dan wel op uitdrukkelijk schriftelijk verzoek van de Verwerkingsverantwoordelijke het verzoek van Betrokkene afhandelen.

Artikel 11. Toezicht op de naleving

11.1. Verwerker zal (halfjaarlijks – in april en september van een kalenderjaar) – Verwerkingsverantwoordelijke schriftelijk rapporteren in het kader van de uitvoering van de Overeenkomst en specifiek ten aanzien van de feiten en ontwikkelingen met betrekking tot de technische en organisatorische beveiligingsmaatregelen.

11.2. Verwerkingsverantwoordelijke heeft het recht de naleving van de bepalingen van de Overeenkomst te controleren bij Verwerker. Verwerkingsverantwoordelijke kan dat na toestemming van Verwerker daartoe zelf doen of hij kan dat laten doen door een onafhankelijke registeraccountant, registerinformaticus of andere daartoe gecertificeerde auditor.

11.3. Verwerkingsverantwoordelijke draagt de kosten van de audit met uitzondering van de kosten van het personeel van Verwerker en (eventuele) Subverwerker(s) dat de controle begeleidt. Deze laatste kosten zijn voor Verwerker, respectievelijk Subverwerker(s). Indien uit de audit volgt dat de Verwerker tekortschiet in de uitvoering van de Overeenkomst, zal Verwerker die tekortkomingen per direct herstellen/ongedaan maken.

11.4. Verwerkingsverantwoordelijke zal de audit [minimaal tien (10) dagen] voor aanvang schriftelijk aankondigen aan Verwerker, voorzien van een omschrijving op welke onderdelen de audit ziet en het auditproces.

Artikel 12. Aansprakelijkheid en vrijwaring

12.1. [Verwerker is aansprakelijk voor alle schade veroorzaakt door Verwerker en/of (eventuele) Subverwerker voortvloeiende uit het niet nakomen van de Overeenkomst, alsmede verband houdende met de overtreding door Verwerker en/of (eventuele) Subverwerker van de Algemene verordening gegevensbescherming (AVG).]

12.2. Verwerker vrijwaart Verwerkingsverantwoordelijke tegen elke (rechts)vordering van een derde jegens Verwerkingsverantwoordelijke welke voortvloeit uit het feit dat Verwerker en/of (eventuele) Subverwerker tekort is geschoten in de nakoming van zijn verplichtingen uit hoofde van de Overeenkomst.

Artikel 13. Duur en beëindiging

13.1. De Overeenkomst vangt aan bij ondertekening hiervan door Partijen.

13.2. De Overeenkomst eindigt van rechtswege op het moment dat de Opdracht eindigt.

13.3. De Overeenkomst is niet tussentijds opzegbaar.

13.4. Beëindiging van de Overeenkomst laat de toepasselijkheid van de bepalingen die bedoeld zijn het einde van de Overeenkomst te overleven onverlet. Het betreft in dit kader in ieder geval de bepalingen uit Artikelen 7,8,10,12, en 15.

Artikel 14. Evaluatie

Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van (verouderde) beveiligingsmaatregelen vereist. Partijen zullen dan ook jaarlijks gezamenlijk – doch zoveel vaker als noodzakelijk blijkt - de uitvoering van de Overeenkomst, waaronder in ieder geval begrepen de maatregelen zoals geïmplementeerd op basis van de Overeenkomst – evalueren. Op basis van de evaluatie zal Verwerker in overleg met Verwerkingsverantwoordelijke waar nodig de beveiligingsmaatregelen verscherpen, aanvullen of verbeteren om te blijven voldoen aan zijn verplichtingen onder de Overeenkomst.

Artikel 15. Toepasselijk recht en geschillen

15.1. Op de Overeenkomst is uitsluitend Nederlands recht van toepassing.
15.2. Alle geschillen, welke tussen Partijen mochten ontstaan in verband met de Overeenkomst, zullen bij uitsluiting worden voorgelegd aan de bevoegde rechter van de rechtbank […].

Artikel 16. Overige bepalingen

16.1. Algemene leverings- en betalingsvoorwaarden of andere algemene voorwaarden van Partijen zijn niet van toepassing op de Overeenkomst.
16.2. Wijzigingen van de Overeenkomst worden slechts geacht te zijn overeengekomen, indien deze door Partijen schriftelijk zijn overeengekomen.
16.3. Indien en voor zover tegenstrijdigheden voorkomen tussen de Overeenkomst en een nadere overeenkomst, geldt het gestelde in deze Overeenkomst.
16.4. Het nalaten door één van de Partijen om binnen een in de Overeenkomst genoemde termijn nakoming van enige bepaling te verlangen, tast het recht om alsnog nakoming te eisen niet aan, tenzij de betreffende Partij uitdrukkelijk en schriftelijk met de niet nakoming akkoord is gegaan.
16.5. Indien een bepaling uit de Overeenkomst of een nadere Overeenkomst ongeldig blijkt of door een rechter buiten werking wordt gesteld, dan heeft dat geen invloed op de overige bepalingen van de Overeenkomst. Partijen zullen vervolgens in overleg treden om een nieuwe bepaling overeen te komen die qua inhoud zo dicht mogelijk ligt bij de oorspronkelijke.

Aldus overeengekomen en in tweevoud opgemaakt te [plaats] op [datum].

Verwerkingsverantwoordelijke	Verwerker
_____	_____
[…]	[…]
voor deze: [de heer/mevrouw] […]	voor deze: [de heer/mevrouw] […]

Bijlage XI.a bij Verwerkersovereenkomst

Bijlage 1 Doel en middelen

I. INLEIDING

Verwerkingsverantwoordelijke dient op grond van de Algemene verordening gegevensbescherming (AVG) doel en middelen voor de verwerking van persoonsgegevens vast te stellen. Op basis van de AVG dient Verwerker de persoonsgegevens slechts te verwerken ten behoeve en in opdracht van Verwerkingsverantwoordelijke. Door middel van deze Bijlage stelt Verwerkingsverantwoordelijke - overeenkomstig de doeleinden zoals Verwerkingsverantwoordelijke in zijn register van verwerkingsactiviteiten heeft opgenomen - vast voor welke doelen en met welke middelen Verwerker de persoonsgegevens in het kader van uitvoering van de Opdracht verwerkt.

II. DOELEN

Ten behoeve van de onderstaande doelen die zijn aangevinkt worden Persoonsgegevens door Verwerker verwerkt:

☐ A. […]

☐ B. […]

☒ C. het geleverd krijgen/in gebruik kunnen nemen van de dienst(en) door Verwerkingsverantwoordelijke en haar onderaannemers.

☒ D. het verkrijgen van toegang tot de dienst(en), waaronder identificatie, authenticatie en autorisatie.

☒ E. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik, en het voorkomen van inconsistentie en onbetrouwbaarheid, van de Persoonsgegevens binnen de dienst(en).

☒ F. de continuïteit en goede werking van de dienst(en) conform de afspraken die Verantwoordelijke en Verwerker, waaronder onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden door Verwerker en het verschaffen van ondersteuning en/of training aan Verwerkingsverantwoordelijke en/of andere geautoriseerde gebruikers door Verwerker.

☒ G. het aan de Verwerkingsverantwoordelijke voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van de uitvoering van een Project te kunnen verbeteren.

☒ H. het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die gesteld worden aan Verwerkingsverantwoordelijke.

III. MIDDELEN

III.1 Categorieën van Persoonsgegevens

Per doel als hierboven beschreven worden de volgende Persoonsgegevens verwerkt:

A B C D E F G H	

III.2 Bijzondere/gevoelige Persoonsgegevens

Ten aanzien van de volgende bijzondere /gevoelige Persoonsgegevens worden de volgende specifieke beveiligingsmaatregelen genomen:

1. […]

2. […]

3. […]

III.3 Toegang tot en beveiliging van de Persoonsgegevens

Toegang tot Persoonsgegevens
Binnen de organisatie van Verwerker (en door haar ingeschakelde Subverwerkers) hebben alleen toegang tot de Persoonsgegevens: de personen werkzaam op afdeling […]. De personen werkzaam op deze afdelingen hebben allen een geheimhoudingsverklaring ondertekend.

Buiten de organisatie van de Verwerker (en door haar ingeschakelde Subverwerkers) hebben alleen toegang tot de Persoonsgegevens […].

[Inloggen gaat door middel van minimaal een beveiligde en versleutelde verbinding op basis van een moderne Cipher Suite. De netwerkverbinding is gecodeerd en geverifieerd met (minimaal) AES_128_GCM en gebruikt ECDHE_RSA als mechanisme voor sleutelwisseling.]

Beveiliging server Verwerker
De servers met daarop het netwerk van Verwerker is gesitueerd in een datacenter van […] (subsubverwerker). De wijze waarop […] de servers geplaatst in haar datacenter beveiligd is opgenomen in **Annex A**.

III.4 Bewaartermijnen Persoonsgegevens

Verwerker zal de Persoonsgegevens die zij in het kader van de Opdracht verwerkt niet langer bewaren dan overeenkomstig het bepaalde in artikel 8 van de Verwerkersovereenkomst. [Op het vorenstaande

bestaan de volgende uitzonderingen/Ten aanzien van het bepaalde in artikel 8 gelden de volgende aanvullende bepalingen:]

a) […]

III.5 Hard- en Software

Bij het vaststellen van de doel en middelen wordt niet van (wezenlijk) belang geacht dat Verwerkingsverantwoordelijke ook vaststelt met welke technische en organisatorische middelen (hard- en software) Verwerker de Opdracht uitvoert en de Persoonsgegevens verwerkt indien de doelen van de verwerking goed zijn omschreven. Wel wordt verlangd dat de Verwerkingsverantwoordelijke door Verwerker volledig wordt geïnformeerd welke hard- en software wordt gebruikt. Een opsomming van welke hard- en software Verwerker gebruikt bij de verwerking van de Persoonsgegevens is aan deze Bijlage gehecht als **Annex B**.

Bijlage 2 Subverwerkersovereenkomst(en)

Klopt het dat er hier niets staat?

Bijlage 3 Geheimhoudingsverklaring

[De heer/mevrouw] [naam], hierna ‘medewerker’, werkzaam bij Verwerker,

verklaart zich akkoord met het volgende:

1. Medewerker heeft uit hoofde van zijn functie toegang tot persoonsgegevens.

2. Het is de medewerker zowel gedurende als na afloop van zijn arbeidsovereenkomst met Verwerker verboden om - ongeacht de wijze waarop en de redenen waarom de arbeidsovereenkomst tot een einde is gekomen - op enigerlei wijze aan derden, direct of indirect, in welke vorm en op welke wijze dan ook enige mededeling te doen van of aangaande persoonsgegevens, waarvan de medewerker in het kader van de uitoefening van zijn werkzaamheden voor de Stichting kennis heeft genomen.

3. Deze persoonsgegevens zijn privacygevoelig en mogen uitsluitend worden verwerkt voor het doel waarvoor ze zijn verkregen.

4. De geheimhoudingsplicht mag worden doorbroken indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de opdracht en de uitvoering van de functie van medewerker of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

5. Indien medewerker een (mogelijke) inbreuk op de beveiliging signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de medewerker dit per omgaande aan Verwerker ongeacht het tijdstip van de dag.

[Plaats] [datum]:

_____

[naam]

Bijlage 4 Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming is de heer Verwijs, te bereiken onder telefoonnummers (0113) 22 41 70 en (0113) 21 10 20 en onder e-mail functionarisgegevensbescherming@calvjincollege.nl.

Bijlage 5 Formulier gegevens datalek

Deze bijlage bevat een aantal onderdelen van de gegevens die Verwerkingsverantwoordelijke moet opgeven als zij een (mogelijk) datalek meldt aan de AP. Bij het formulier zijn de vragen uit bijlage 1 bij de Europese Verordening 611/2013 als uitgangspunt gehanteerd. Het IRT van Verwerkingsverantwoordelijke gebruikt deze vragen om de benodigde informatie zo volledig en juist mogelijk te krijgen met betrekking tot het mogelijke datalek.

Gegevens over het datalek

1) Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
2) Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
   a) Minimaal: [vul aantal in]
   b) Maximaal: [vul aantal in]
3) Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
4) Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan)
   a) Op [datum]
   b) Tussen [begindatum periode] en [einddatum periode]
   c) Nog niet bekend
5) Wat is de aard van de inbreuk? (De School kan meerdere mogelijkheden aankruisen)
   a) Lezen (vertrouwelijkheid)
   b) Kopiëren
   c) Veranderen (integriteit)
   d) Verwijderen of vernietigen (beschikbaarheid)
   e) Diefstal
   f) Nog niet bekend
6) Om welk type persoonsgegevens gaat het? (De School kan meerdere mogelijkheden aankruisen)
   a) Naam-, adres- en woonplaatsgegevens
   b) Telefoonnummers
   c) E-mailadressen of andere adressen voor elektronische communicatie
   d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
   e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
   f) Burgerservicenummer (BSN) of sofinummer
   g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
   h) Geslacht, geboortedatum en/of leeftijd
   i) Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
   j) Overige gegevens, namelijk [vul aan]
7) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (Meerdere antwoorden mogelijk)

a) Stigmatisering of uitsluiting
b) Schade aan de gezondheid
c) Blootstelling aan (identiteits)fraude
d) Blootstelling aan spam of phishing
e) Anders, namelijk (vul aan)

Vervolgacties naar aanleiding van het datalek

8) Welke technische en organisatorische maatregelen heeft de School getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Technische beschermingsmaatregelen

9) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan)
a) Ja
b) Nee
c) Deels, namelijk: [vul aan]

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als de School bij vraag 9 gekozen heeft voor optie a of optie c. Als de School gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen t