0224 - 21 47 45
info@alles-in-1.org
www.alles-in-1.org

Model Verwerkersovereenkomst Versie 3.0

Deze Model Verwerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant).

De nieuwe Model Verwerkersovereenkomst 3.0 komt in de plaats van eerdere Model verwerkersovereenkomsten uit 2015 en 2016. De uitgangspunten van deze Model Verwerkersovereenkomst 3.0 sluiten aan bij de bepalingen in het Convenant, geven invulling aan verplichtingen op grond van de Europese Algemene Verordening Gegevensbescherming (hierna: AVG), en de uitgangspunten zoals onder andere in (inter)nationale beveiligingsnormen, jurisprudentie en richtsnoeren van de toezichthouder zijn aangegeven.

Reeds afgesloten Verwerkersovereenkomsten op basis van de modellen uit 2015 en 2016 blijven hun gelding houden totdat deze verwerkersovereenkomsten door partijen worden beëindigd. Het uitgangspunt is dat met ingang van 25 mei 2018, het moment waarop de AVG van toepassing wordt, Onderwijsinstellingen en Leveranciers bij het aangaan van een verwerkersovereenkomst of bij vernieuwing van een bestaande verwerkersovereenkomst, de Model Verwerkersovereenkomst 3.0. gebruiken.

In het Convenant is afgesproken dat Onderwijsinstellingen en Leveranciers het actuele model gebruiken bij het maken van afspraken. Van de actuele Model Verwerkersovereenkomst kan alleen gemotiveerd en schriftelijk worden afgeweken.

Deze Model Verwerkersovereenkomst 3.0 bevat twee bijlagen:

1. In de Privacybijsluiter (Bijlage 1) wordt met name een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en voor welke doeleinden.
2. In de Beveiligingsbijlage (Bijlage 2) wordt omschreven welke technische en organisatorische beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven

Informatie over het Convenant en de model Verwerkersovereenkomst is te vinden op de website www.privacyconvenant.nl. Meer informatie en antwoorden op vragen over privacy en de wettelijke rechten en verplichtingen voor Onderwijsinstellingen zijn te vinden op de websites van de sectorraden PO-Raad, VO-raad, MBO Raad (saMBO-ICT) en bij Kennisnet.

Maart 2018

Partijen:

1. Het bevoegd gezag van onderwijsinstelling:
   geregistreerd onder BRIN-nummer:

   bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs,
   gevestigd en kantoorhoudende aan (adres):
   te (postcode):
   (plaats):

   te dezen rechtsgeldig vertegenwoordigd door:
   functie:
   Naam:
   hierna te noemen: "**Onderwijsinstelling**".

en

2. De besloten vennootschap De Bloeiende Naboom B.V., gevestigd en kantoorhoudende aan Botterstraat 18 te (2162 LA) Lisse, te dezen rechtsgeldig vertegenwoordigd door de Algemeen Directeur, Carina Wassenaar – van Gelder, hierna te noemen: "**Verwerker**"

hierna gezamenlijk te noemen: **"Partijen"**, of afzonderlijk: **"Partij"**

Overwegen het volgende:

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij de door Verwerker geboden Online diensten, omvattende één integrale online leeromgeving voor leerlingen en een voor de leerkracht ontwikkeld dashboard waarop een volledig overzicht op te vragen is van de leerlinggegevens en de historische leerlingresultaten binnen de Alles-in-1 Online leeromgeving. Ook hebben leerkrachten een compleet overzicht van de huidige oefening waar een leerling mee bezig is. Daarnaast hebben leerlingen en leerkrachten toegang tot het toetsprogramma ALLES TOETSEN en het scholenregistratiesysteem, ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
b. Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Verwerkersovereenkomst wordt verstaan onder:

a. Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
b. Bijlage(n): bijlage(n) bij het Convenant of de Verwerkersovereenkomst;
c. Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy 3.0;
d. Convenantpartij: een tot het Convenant toegetreden Onderwijsinstelling of Leverancier;
e. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
g. Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;

h. Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenovereenkomst. Instructies worden verstrekt door en aan de contactpersonen van partijen zoals die zijn opgenomen in de Bijlage(n);
i. Keten iD: een pseudoniem van een persoonsgebonden nummer van een Onderwijsdeelnemer dat de Onderwijsdeelnemer niet langer direct identificeerbaar maakt. Hierna wordt dat pseudoniem opnieuw versleuteld tot het Keten iD, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen. Het Keten iD wordt ook ECK iD genoemd;
j. Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;
k. Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;
l. Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
m. Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;
n. Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;
o. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Verwerker, zoals omschreven in overweging a met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en Leverancier voor het betreffende product of dienst;
p. Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
q. Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
r. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling-administratiesysteem, kernregistratiesysteem, studentinformatiesysteem, deelnemersadministratie, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, dashboards en kwaliteitsmanagementsystemen voor zover zij Persoonsgegevens van Onderwijsdeelnemers bevatten, een elektronische leeromgeving en een leerling volgsysteem;
s. Standaardattributenset: de door het Platform vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het Keten iD gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen (zoals gepubliceerd op de website van het Platform);
t. Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van de Model Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;
u. AVG: de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG);
v. Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.
3. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen zoals opgenomen in Bijlage 1, die plaatsvinden ter uitvoering van de Product- en Dienstenovereenkomst. Verwerker brengt Onderwijsinstelling onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het (het bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Verwerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Onderwijsinstelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Onderwijsinstelling een keuze kan maken voor eventueel aangeboden optionele diensten.
3. Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker voorafgaand aan het sluiten van deze Verwerkersovereenkomst de Onderwijsinstelling in Bijlage 1 over de in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, en de Verwerkingen die in dat kader plaatsvinden. De in Bijlage 1 opgenomen informatie moet in begrijpelijke taal zijn beschreven, waardoor Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en) en de uitvoering van de bijbehorende Verwerkingen.
4. De Onderwijsinstelling neemt de in lid 2 van dit artikel genoemde Verwerking van de Persoonsgegevens op in een register van de verwerkingsactiviteiten[1] die onder hun verantwoordelijkheid plaatsvinden.
5. Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Onderwijsinstelling verricht.
6. Onderwijsinstelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

Artikel 4: Privacyconvenant

1. Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5: Gebruik Persoonsgegevens

1. Verwerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen, behoudens een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een rechterlijke uitspraak, voor zover daartegen geen beroep meer openstaat. In dat geval stelt Verwerker de Onderwijsinstelling voorafgaand aan de Verwerking van dat wettelijke voorschrift dan wel de rechterlijke uitspraak in kennis, tenzij dergelijke kennisgeving om gewichtige redenen van algemeen belang verboden is.
2. Een overzicht van onder meer de categorieën Persoonsgegevens en het doel waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacybijsluiter bij deze Verwerkersovereenkomst.
3. De Verwerker dient in de Privacybijsluiter aan te geven of de Privacybijsluiter ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiter voor welke, door de VerwerkersVerwerkingsverantwoordelijke vastgestelde, doeleinden persoonsgegevens worden verwerkt bij het gebruik van zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt
4. Indien Verwerker in strijd met de AVG het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.
5. <u>*SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN HET ONDERWIJSKUNDIG RAPPORT*</u>: *In aanvulling op het bepaalde in lid 4, is het Verwerker uitsluitend toegestaan om Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde andere onderwijsinstelling, na een concreet verzoek tot verstrekking van die onderwijsinstelling en op voorwaarde dat deze andere onderwijsinstelling haar administratieve onderwijsidentiteit (bijv. BRIN of OiN) aan Verwerker kenbaar heeft gemaakt. Indien de andere onderwijsinstelling niet beschikt over een administratieve onderwijsidentiteit zal Verwerker Persoonsgegevens alleen aan die andere onderwijsinstelling verstrekken op uitdrukkelijke instructie van Onderwijsinstelling.*

[1] Zie voor een voorbeeld de Aanpak IBP bij https://kn.nu/IBPonderwijs

6. *SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS:*

*a. Convenantspartijen die Leermiddelen en Toetsen ontwikkelen en aanbieden (hierna te noemen: **Leermiddelenleverancier**), zullen jaarlijks ten behoeve van het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, (welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld) de Privacy Bijsluiter voor die Leermiddelen en Toetsen aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt (met betrekking tot de Leermiddelen en Toetsen die op de desbetreffende leermiddelenlijsten worden opgenomen).*

b. Verwerker (de distributeur) wisselt in opdracht van de Onderwijsinstelling gegevens uit met deze Leermiddelenleveranciers.

c. De Onderwijsinstelling is verantwoordelijk voor het maken en vastleggen van afspraken met iedere Leermiddelenleverancier in een Verwerkersovereenkomst.

d. Onderwijsinstelling vrijwaart Verwerker (distributeur) voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Leermiddelenleverancier, en de Onderwijsinstelling vrijwaart de Leermiddelenleverancier voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Verwerker (distributeur).

e. De verantwoordelijkheid van Verwerker (distributeur) voor het beheer van de Persoonsgegevens houdt op, op het moment dat de Leermiddelenleverancier die gegevens heeft ontvangen van Verwerker (distributeur).

Artikel 6: Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt er voor dat een ieder die hij betrekt bij de Verwerking van Persoonsgegevens, waaronder zijn werknemers, vertegenwoordigers en/of Subverwerkers, deze gegevens als vertrouwelijk behandelt. Verwerker waarborgt dat met de tot het Verwerken van de Persoonsgegevens geautoriseerde personen een geheimhoudingsovereenkomst of –beding is gesloten, of dat deze door een wettelijke verplichting tot geheimhouding zijn gebonden.
2. De in lid 1 bedoelde geheimhoudingsplicht geldt niet in de hierna genoemde gevallen:
   a. voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken;
   b. indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan Onderwijsinstelling te verlenen diensten; of
   c. indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling dan wel een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, tot verstrekking verplicht is.
3. Verwerker onthoudt zich van verstrekking of bekendmaking van Persoonsgegeven aan een Derde, tenzij deze verstrekking of bekendmaking plaatsvindt in opdracht van Onderwijsinstelling respectievelijk wanneer dit noodzakelijk is om te voldoen aan een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, of een op de Verwerker rustende wettelijke verplichting. Onder wettelijke verplichtingen zijn begrepen Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker - tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - Onderwijsinstelling onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.
4. Verwerker zorgt er voor dat de onder diens gezag werkende medewerkers uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

Artikel 7: Beveiliging en controle

1. Met inachtneming van het bepaalde in artikel 32 AVG zal Verwerker, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
2. Naast de maatregelen als genoemd in artikel 32 lid 1 AVG, worden onder meer de volgende maatregelen - waar passend - genomen:
   a. een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens;
   b. maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;
   c. het regelen van procedures rondom het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen

(vergelijkbaar met de toepasselijke ISO-normering, en/of vergelijkbaar met het geldende Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren.

3. Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.
4. In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de passende technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud, vorm en de werkwijze van de verklaringen die Verwerker verstrekt over de afgesproken beveiligingsmaatregelen.
5. De Verwerker stelt in goed overleg de Onderwijsinstelling in staat om effectief te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Verwerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken.
6. In aanvulling op de voorgaande leden heeft Onderwijsinstelling te allen tijde het recht om, in overleg met de Verwerker en met inachtneming van een redelijke termijn, de naleving van Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, de Product- en Dienstenovereenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen, te (doen) controleren middels een audit uitgevoerd door een onafhankelijke gecertificeerde externe deskundige:
    a. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een Verwerker, in overleg met Onderwijsinstelling, in te schakelen externe deskundige die een derden-verklaring (TPM) afgeeft.
    b. De auditor verstrekt het auditrapport alleen aan Partijen.
    c. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
    d. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
    e. Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8: Datalekken

1. Partijen hebben een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling of Verwerker een Datalek vaststelt, dan zal deze de andere Partij daarover zonder onredelijke vertraging informeren zodra hij kennis heeft genomen van dat Datalek. Verwerker verstrekt ingeval van een Datalek alle relevante informatie aan Onderwijsinstelling met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen.
3. Verwerker informeert Onderwijsinstelling onverwijld indien een vermoeden bestaat dat een Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen zoals bedoeld in artikel 34,lid 1, AVG.
4. Verwerker stelt bij een Datalek de Onderwijsinstelling in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Verwerker dient hierbij aansluiting te zoeken bij de bestaande processen die Onderwijsinstelling daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking de Persoonsgegevens, en meer in het bijzonder (verdere) schending van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, te voorkomen of te beperken.
5. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. In geval een Datalek bij Verwerker meerdere Onderwijsinstellingen in gelijke mate treft, kan Verwerker, na overleg met een of meerdere Verwerkingsverantwoordelijken, namens de Onderwijsinstellingen een melding doen van het Datalek aan de Autoriteit Persoonsgegevens. Van het voornemen hiervan zal Verwerker Onderwijsinstelling onverwijld (en zo mogelijk voorafgaand aan de melding) in kennis stellen.
6. In geval van het Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Onderwijsinstelling de Betrokkenen informeren over het Datalek.
7. Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.
8. Partijen documenteren alle Datalekken in een (incidenten)register, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

9. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e van deze Verwerkersovereenkomst, informeert de Verwerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9 Bijstand

1. Verwerker verleent Onderwijsinstelling bijstand bij het doen nakomen van de op Onderwijsinstelling rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking - maar niet beperkt - tot:
   a. het - voor zover redelijkerwijs mogelijk - vervullen van de plicht van Onderwijsinstelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
   b. het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;
   c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
   d. het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
   e. het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 8 van deze Verwerkersovereenkomst.
2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

Artikel 10: Doorgifte aan derde landen buiten de Europese Economische Ruimte

1. Verwerker is uitsluitend gerechtigd tot doorgifte van Persoonsgegevens aan een derde land of internationale organisatie indien Onderwijsinstelling daarvoor specifieke Schriftelijke toestemming heeft gegeven, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Onderwijsinstelling voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
2. Indien na toestemming van Onderwijsinstelling Persoonsgegevens worden doorgegeven aan derde landen buiten de Europese Economische Ruimte of aan een internationale organisatie zoals bedoeld in artikel 4 lid 26 AVG, dan zien Partijen er op toe dat dit alleen plaatsvindt conform wettelijke voorschriften en eventuele verplichtingen die in dit verband op Onderwijsinstelling rusten. Indien gegevens worden doorgegeven aan een derde land of een internationale organisatie, dan wordt dit in Bijlage 1 bij deze Verwerkers-overeenkomst aangegeven, inclusief een opgave van de landen waar, of internationale organisaties door wie, de Persoonsgegevens worden verwerkt. Daarbij wordt tevens aangegeven op welke wijze is voldaan aan de voorwaarden op basis van de AVG voor doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.

Artikel 11: Inschakeling Subverwerker

1. Onderwijsinstelling geeft Verwerker door ondertekening van deze Verwerkers-overeenkomst toestemming tot het inschakelen van Subverwerkers, van wie de identiteit en vestigingsgegevens zijn opgenomen in de Privacybijsluiter.
2. Tijdens de duur van de Verwerkersovereenkomst licht Verwerker Onderwijsinstelling in over een voorgenomen toevoeging van een nieuwe Subverwerker of wijziging in de samenstelling van de bestaande Subverwerkers, waarbij Onderwijsinstelling de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
3. Verwerker is verplicht iedere Subverwerker via een overeenkomst of andere rechtshandeling minimaal dezelfde verplichtingen inzake gegevensbescherming op te leggen als in deze Verwerkersovereenkomst aan Verwerker zijn opgelegd. Hieronder vallen onder meer de verplichting om de Persoonsgegevens niet verder te Verwerken anders dan in het kader van deze Verwerkersovereenkomst is overeengekomen, en de verplichting tot het nakomen van de geheimhoudingsverplichtingen, meldingsverplichtingen, medewerkingsverplichtingen en beveiligingsmaatregelen met betrekking tot de Verwerking van Persoonsgegevens zoals in deze Verwerkersovereenkomst vastgelegd. Verwerker zal op verzoek van Onderwijsinstelling afschriften verstrekken van deze Verwerkers-overeenkomsten, of van de relevante passages uit de Verwerkersovereenkomst of een andere overeenkomst of een andere bindende rechtshandeling tussen Verwerker en de door deze overeenkomstig artikel 11, lid 1, van deze overeenkomst ingeschakelde Subverwerker.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Verwerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van de Onderwijsinstelling. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
3. Verwerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
4. Verwerker zal alle Subverwerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Verwerkers-overeenkomst en zal waarborgen dat alle Subverwerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Aansprakelijkheid

1. Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Product- of Dienstenovereenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:
   a. verhaalsactie op grond van artikel 82 AVG; of
   b. schadevergoedingsactie uit hoofde van deze Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthouder betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

   Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken partij op grond van de geldende wet- of regelgeving ter beschikking staat.
2. Het bepaalde in lid 1 sub b geldt onverminderd het bepaalde in artikel 14 lid 2.
3. Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthouder, beiden in verband met deze Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Artikel 14: Tegenstrijdigheid en wijziging Verwerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Verwerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Verwerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.
3. Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens de Onderwijsinstelling de keuze hiertoe aanvaardt, de Onderwijsinstelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens en de doeleinden waaronder de Persoonsgegevens worden Verwerkt. De wijzigingen zullen in Bijlage 1 worden opgenomen.
4. Wijzigingen in de artikelen van de Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
5. In het geval enige bepaling van deze Verwerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Verwerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 15: Duur en beëindiging

1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder in ieder geval artikel 5, lid 1, en de artikelen 6, 9 en 12.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling,		***Leverancier,***	
			
Zo plaatst u een handtekening: *http://www.alles-in-1.org/content/upload/files/handtekening.mov*			
Naam:		Naam:	C. Wassenaar - van Gelder
Functie:		Functie:	Algemeen Directeur
Datum:		Datum:	18-04-2018
Plaats:		Plaats:	Lisse

Bijlage 1: Privacybijsluiter
Bijlage 2: Beveiligingsbijlage

BIJLAGE 1: PRIVACYBIJSLUITER
Online diensten t.b.v. de leermethode Alles-in-1

Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals onderwijsdeelnemers). Onderwijsinstellingen moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft onderwijsinstellingen informatie over de dienstverlening die Verwerker verleent en welke persoonsgegevens de Verwerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen van wie persoonsgegevens worden verwerkt.

Het gebruik van deze Privacybijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. De Privacybijsluiter is een bijlage bij de Modelverwerkersovereenkomst en omvat de Instructies voor de Verwerking van Persoonsgegevens van de Onderwijsinstelling aan de Verwerker.

In het kader van de herkenbaarheid is het wenselijk dat Verwerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacybijsluiter. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 1A", "Bijlage 1B", etc.. Deze Bijlagen worden aan de Verwerkersovereenkomst gehecht.

Voor specifieke branches zoals uitgevers, distributeurs en leveranciers van student- en leerling-administratiesystemen, kunnen specifieke privacybijsluiters worden gemaakt die gebaseerd zijn op dit model. Deze specifieke modellen zijn afgestemd door de Initiatiefnemers van het Convenant. De modellen zijn te vinden op de website van het Platform: www.edu-k.nl/ibp.

A. Algemene informatie

Naam product en/of dienst:	Alles-in-1 Online Diensten
Naam Verwerker en vestigingsgegevens:	De Bloeiende Naboom BV, Botterstraat 18, 2162LA, Lisse
Link naar leverancier en/of productpagina:	www.alles-in-1.org
Beknopte uitleg en werking product en dienst:	Adaptiee en integrale lesomgeving voor onderwijsdeelnemers
Doelgroep (zoals po/vo, onderbouw/bovenbouw):	PO, onderbouw en bovenbouw
Gebruikers:	onderwijsdeelnemers/docenten

B. Omschrijving specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen van Persoonsgegevens:

1. Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.
    a. Alles-in-1 Online biedt één integrale online leeromgeving voor scholieren. Binnen deze omgeving kunnen scholieren relevant materiaal bekijken en oefeningen maken.
    b. Voor de leerkracht biedt Alles-in-1 Online een dashboard waarop een volledig overzicht op te vragen is van de leerlinggegevens en de historische leerlingresultaten binnen de Alles-in-1 Online leeromgeving. Daarnaast hebben leerkrachten een compleet overzicht van de huidige oefening waar een leerling mee bezig is.
        - Voor een goede werking van a en b worden de volgende leerlinggegevens verwerkt: naam, leeftijd (optioneel), school en groep, geboortedatum(optioneel), pasfoto(optioneel). Daarnaast worden de behaalde oefeningresultaten opgeslagen. Tot slot worden opgeslagen: loginnaam, wachtwoord en tijden van inloggen. Optionele velden worden duidelijk gemarkeerd. Scholen dragen zelf zorg voor de selectie van welke persoonsgegevens wel of niet 'essentieel' zijn. Scholen zijn zelf verantwoordelijk is voor de keuze om optionele gegevens vast te leggen.

2. Omschrijving van de optionele Verwerkingen die de Verwerker aanbiedt
    a. [N.V.T.]
    b. [N.V.T.]

MBO

Toelichting: Het gaat hier om aanvullende diensten en bijhorende Verwerkingen die geen onlosmakelijk onderdeel vormen van de aangeboden dienst. Dit zijn bijvoorbeeld optionele diensten voor de Onderwijsinstelling die behulpzaam kunnen zijn voor de Onderwijsinstelling t.b.v. het primaire (leer)proces en administratieve werkzaamheden.

De Onderwijsinstelling dient een keuze te maken en daarbij opdracht te geven om persoonsgegevens te verwerken, voor het afnemen van deze diensten. Dat kan door de keuze schriftelijk aan te geven in deze bijlage (bijvoorbeeld door het aanvinken van een tick-box ☑).

De opdracht kan ook worden verleend doordat de Onderwijsinstelling in de praktijk de dienst activeert, bijvoorbeeld door een product of dienst aan of uit zetten. De Onderwijsinstelling die op deze wijze de keuze maakt, dient dit op basis van eerder verstrekte informatie (zoals bijvoorbeeld opgenomen in deze bijsluiter) te doen.

C. Doeleinden voor het verwerken van gegevens

De Verwerker dient in deze Bijsluiter expliciet aan te geven of deze:

☑ I. leverancier is van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen, of

☐ II. (tevens) leverancier is van een School- en Leerlinginformatiemiddel.

Ad I. Indien de Verwerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

a. het met gebruikmaking van het Digitale Onderwijsmiddel geven en volgen van onderwijs en het begeleiden en volgen van Onderwijsdeelnemers, waaronder:
   - de opslag van leer- en toetsresultaten;
   - het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;
   - de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;
   - analyse en interpretatie van leerresultaten;
   - het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.

b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;

c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

d. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.

e. de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;

f. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;

g. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.

h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.

i. De uitvoering of toepassing van een andere wet

Ad II. (Alleen) indien de Verwerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

a. de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:
   - de indeling en aanpassing van roosters;
   - de analyse en interpretatie van leerresultaten;
   - het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;
   - het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;
   - de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling;
   - financieel beheer;
   - monitoring en verantwoording, ten behoeve van met name: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vorm) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;
   - het behandelen van geschillen.
   - het uitwisselen van Persoonsgegevens met Derden, waaronder:
   - toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
   - samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen;
   - partijen betrokken bij de invulling van stage of leer-/ werkplekken voor zover noodzakelijk en wettelijk toegestaan;
   - Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgonderwijs.
b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
d. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel, Verwerkte Persoonsgegevens.
e. de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
f. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
g. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.
i. De uitvoering of toepassing van een andere wet

D. Categorieën en soorten persoonsgegevens

1. Omschrijving van de categorieën Betrokkenen over wie Persoonsgegevens worden verwerkt, en de categorieën persoonsgegevens van de Betrokkenen:

Van toepassing	**Categorie**	**Toelichting**
X	1. Contactgegevens	Leerlinggegevens: loginnaam, wachtwoord en tijden van inloggen. De leerlingnaam kan optioneel worden vastgelegd.
X	2. Onderwijs-deelnemer-nummer	Een administratienummer dat onderwijsdeelnemers identificeert kan optioneel worden vastgelegd.
	3. Nationaliteit en geboorteplaats	N.V.T.
	4. Ouders, voogd	N.V.T.
	5. Medische gegevens	N.V.T.
	6. Godsdienst	N.V.T.

X	7. Studievoortgang	Behaalde oefenresultaten
X	8. Onderwijsorganisatie	Naam school en groep
	9. Financiën	N.V.T.
X	10. Beeldmateriaal	Een leerlingpasfoto kan optioneel worden vastgelegd. Overig Beeldmateriaal (foto's van bijeenkomsten e.d.) wordt niet standaard vastgelegd. Als dit van toepassing is dan worden deze alleen gebruikt na uitdrukkelijke toestemming van de betrokken ouders van leerlingen en is bekend voor welke specifieke verwerking en specifiek doel dit beeldmateriaal gebruikt wordt.
	11. Docent, zorg-coördinator, intern begeleider, decaan, mentor	N.V.T.
X	12. Overige gegevens, te weten	Leeftijd en geboortedatum van leerlingen kunnen optioneel worden vastgelegd.
	13. BSN/PGN	N.V.T.
	14. Keten-ID (ECK-ID)	unieke iD voor de 'educatieve contentketen'. hiermee kunnen onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.

3. Door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen):
   Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig de (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. De Onderwijsinstelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen Zie artikel 12.

E. Opslag Verwerking Persoonsgegevens:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens: Nederland

F. Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.
Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:

- Maketime, Haarlem, NL: programmeur Alles-in-1 Online
- Eyestone, Haarlem, NL: programmeur Alles-in-1 Online
- Pixelbyte, Alkmaar, NL: (technische) ondersteuning bij gebruik Alles-in-1 Online, systeemarchitect Alles-in-1 Online en CRM
- Yeti, Groningen, NL:ontwikkelaar Alles Toetsen

Opmerking: indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt én op welke wijze is gewaarborgd dat de gegevens rechtmatig kunnen worden doorgegeven.

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiter of de werking van dit product of deze dienst, kunt u terecht bij: B. Broekema, b.broekema@alles-in-1.org, 06-14887207.

G. Versie 1.0, 7 april 2018

Deze Privacybijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.

BIJLAGE 2: BEVEILIGINGSBIJLAGE

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Normen informatiebeveiliging

Verwerker is verplicht om aan Onderwijsinstelling aan te tonen of en op welke wijze passende technische en organisatorische maatregelen zijn genomen om te waarborgen en te kunnen aantonen dat de verwerking plaatsvindt in overeenstemming met de AVG en de Model Verwerkersovereenkomst.
Voor het toepassen en aantonen van de technische maatregelen, kan Verwerker gebruik maken van (zo snel als redelijkerwijs mogelijk de meest recente versie van) het in het onderwijs ontwikkelde *'Certificeringsschema informatiebeveiliging en privacy ROSA'*[2]. Dat schema voorziet in een baseline van (beveiligings)maatregelen waarmee organisaties dit aantoonbaar kunnen maken.

Indien Verwerker voornoemd Certificeringsschema gebruikt, dan mag gebruik worden gemaakt van een standaard beveiligingsbijlage die is afgestemd door de Initiatiefnemers van het Convenant. Deze afgestemde bijlage 2 is te vinden op de website van het Platform en komt in de plaats van deze model bijlage 2: www.edu-k.nl/ibp.

Verwerker kan ook gebruik maken van andere certificeringsmechanismen en/of (inter)nationaal erkende normen en standaarden voor informatiebeveiliging, mits die een gelijkwaardig of hoger niveau van beveiliging bieden en de door Verwerker genomen maatregelen aan de Onderwijsinstelling inzichtelijk worden gemaakt.

Minimale beveiligingsmaatregelen en aantoonbaarheid

Verwerker plaatst op deze plek in de bijlage een verklaring waaruit blijkt dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens. Deze verklaring bevat ten minste:

a. Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid;
b. Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan;
    i. Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
    ii. Verwerker heeft de Persoonsgegevens die worden Verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken;
    iii. 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. Hierbij heeft Verwerker procedures vastgesteld en gedeeld met de Onderwijsinstelling voor de identificatie, autorisatie en authenticatie van medewerkers alsmede rondom de registratie, aanmelding en afmelding van de medewerkers;
    iv. Verwerker zorgt dat de toegang tot het product of de dienst beveiligd is door middel van een passend beleid voor wachtwoorden dat aansluit bij de stand van de techniek;
    v. Verwerker heeft procedures voor het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke ISO-normering en/of vergelijkbaar met het Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren;
    vi. Verwerker heeft maatregelen genomen om de Persoonsgegevens te beschermen tegen verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

[2] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa

vii. Verwerker maakt bij de beveiliging van de Verwerking van Persoonsgegevens gebruik van een (inter) nationale beveiligingsnorm;
viii. Verwerker heeft maatregelen genomen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

c. Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.

Er zijn geen DBN medewerkers die direct toegang hebben tot persoonsgegevens. Sommigen hebben uit hoofde van hun functie via autorisatie een raadpleegfunctie , als zijnde impersonator. Deze toegang gebruiken zij als dat noodzakelijk is n.a.v. een vraag van een Onderwijsinstelling.

De Alles-in-1 Online diensten zijn standaard beschikbaar tijdens schooltijden (ma – vrij: 8:00 – 17:00). Buiten deze schooltijden is de dienst ook zo goed mogelijk beschikbaar, maar beschikbaarheid kan niet worden gegarandeerd. Incidenten die de beschikbaarheid van de dienst op enigerwijze beïnvloeden zullen binnen schooltijden met de allerhoogste prioriteit worden behandeld. Alleen incidenten die de beschikbaarheid van de dienst ernstig beïnvloeden zullen buiten schooltijden met de allerhoogste prioriteit worden behandeld.

Voor alle genoemde softwarepakketten wordt gebruik gemaakt van een versie die in active support zit van de leverancier zoals b.v. CentOS, PHP, Symfony framework en Windows server.

De Alles-in-1 Online code draait op een eigen VPS bij TransIP. Deze server is ingericht met de Open Source pakketten CentOS, PHP, NGINX en MariaDB. De server is beschermd met ConfigServer Security & Firewall en bruteforce beveiliging. Alleen Pixelbyte heeft als ICT leverancier van Verwerker root toegang tot deze server. Toegang tot het gedeelte waar de Alles-in-1 Online code zich bevindt is voorbehouden aan Pixelbyte en Maketime, de ontwikkelaar van de Alles-in-1 applicaties. Toegang tot de server is alleen mogelijk via een beveiligde (HTTPS, SSH, SFTP) verbinding. Alle data blijft daarnaast binnen Nederland.

Updates aan de Alles-in-1 Online code worden eerst uitgebreid getest op een aparte stagingserver waarop niet gewerkt wordt met persoonsgegevens. Deze updates worden na akkoord iedere woensdag tussen 17:00 en 21:00 uitgerold naar de live server en daar aan een laatste test onderworpen.

Grote updates aan het besturingssysteem en de overige besturingssysteem-, en databasesoftware op de Alles-in-1 Online server worden wekelijks geïnstalleerd op zaterdag en/of zondag tussen 10:00 en 11:00. Gedurende dit onderhoudsinterval kan de beschikbaarheid van de Alles-in-1 Online dienst op geen enkele manier worden gegarandeerd en eventuele meldingen hieromtrent zullen niet in behandeling worden genomen.

Een dagelijkse backup van de database van Alles-in-1 Online wordt gemaakt om 12:00. Een dagelijkse backup van de gehele Alles-in-1 Online omgeving wordt gemaakt om 2:00 Deze backups worden via een SFTP verbinding verstuurd naar een eigen VPS bij Leaseweb. De data wordt hier versleuteld opgeslagen. Deze backup-server is een Windows Server, is voorzien van een firewall en ESET-Endpoint beveiligingssoftware.

De code staat op PHP en het Symfony Framework. De PHP code is gebaseerd op de nieuwste PHP versie en het Symfony Framework, dat is een nu geldende LTS versie met security fixes.

Gebruikte libraries en packages worden gemanaged via Composer. Dat om deze libraries en packages up-to-date te houden.

Alle wachtwoorden van medewerkers, leerkrachten en scholen zijn versleuteld middels bcrypt (cost 12). Wachtwoorden worden automatisch gegenereerd en bestaan uit 8 karakters (cijfers, hoofd- en kleine letters). Autorisatie wordt geregeld door de Symfony firewall en ACL.

Lokale werkstations waarop met de code wordt gewerkt zijn voorzien van een up-to-date Windows versie, beveiligd met een wachtwoord. Na twee minuten inactiviteit logt het systeem automatisch uit. Virusscanner ESET-Endpoint is geïnstalleerd, is up-to-date en draait wekelijks scans naast de standaard monitoring.

Minimaal twee keer per maand wordt de Alles-in-1 Online server nagekeken op zijn automatische updates. Eventuele fouten daarin worden op dat moment hersteld en handmatige updates worden geïnstalleerd. Daarnaast stuurt het systeem tussendoor automatische onderhoudsberichten en beveiligsingswaarschuwingen per mail naar Pixelbyte als er bepaalde fouten worden geconstateerd. Tijdens dit onderhoud worden ook de logbestanden nagelopen op eventuele fouten.

Verwerker rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 31-12 aan Verantwoordelijke over de door Verwerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.
Contactgegevens helpdesk/servicedesk voor beveiligingsincidenten: Pixelbyte, Hazenkoog 28b, 1822BT, Alkmaar. Tel: 0224-799870.

Beveiligingsincidenten en/of datalekken:
ZIE BIJLAGE 2A PROCEDURE DATALEK DBN

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: Bram Broekema. Bereikbaar via mail: b.broekema@alles-in-1.org of telefonisch: 06-14887207

De contactpersoon voor Verwerker is:

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging:
ZIE BIJLAGE 2A PROCEDURE DATALEK DBN

Er is een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat ten minste te volgende punten:

- De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
- De wijze waarop informatie wordt gedeeld:
  - Op welke manier (via e-mail, telefoon);
  - Aan wie gericht (contactpersonen en contactgegevens);
  - Met wie kan (bij vervolgacties) contact worden opgenomen.
- Informatie die in ieder geval over een incident gedeeld moet worden
  - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
  - De oorzaak van het beveiligingsincident;
  - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
  - Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
  - De omvang van de groep betrokkenen;
  - Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
- Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie 1.0 7 april 2018

Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.

Bijlage 2a Procedure datalek DBN
Laatst bijgewerkt: 13-04-2018

1. Definities

Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
Werkstation: een elektronisch apparaat waarmee met één van de digitale diensten van DBN gewerkt kan worden. O.a. (maar niet beperkt tot) Windows en Mac pc's en laptops, smartphones en tablets.

Werktijd: 9:00 tot 18:00 op werkdagen (maandag t/m vrijdag, landelijke vrije dagen uitgezonderd).

2. Partijen

DBN IT contactpersoon: Bram Broekema. Bereikbaar via mail: b.broekema@alles-in-1.org of telefonisch: 06-14887207.
AP: Autoriteit Persoonsgegevens (voorheen CBP)

3. Algemeen

3.1. Medewerkersprotocol omgaan met gegevens

3.1.1. RDP

Uitgangspunt is dat medewerkers altijd binnen de beveiligde RDP omgeving van DBN werken. Medewerkers zullen indien niet noodzakelijk niet buiten de RDP met vertrouwelijke DBN bestanden werken.

Indien het absoluut noodzakelijk is dat er buiten de RDP met een vertrouwelijk bestand gewerkt wordt dan zal/zullen alleen dit/deze noodzakelijke bestand(en) naar het lokale werkstation worden gekopieerd en, wanneer lokaal werken niet meer noodzakelijk is, direct worden teruggeplaatst binnen de RDP omgeving en verwijderd worden van het lokale werkstation. Noodzaak tot werken buiten de RDP is er bijvoorbeeld als een bestand nodig is op een locatie waar geen, of niet voldoende snel/stabiel, internet beschikbaar is. Medewerker is zelf verantwoordelijk voor de bepaling of er sprake is van een voorgenoemde noodzakelijke situatie. Bij twijfel kan altijd advies worden ingewonnen bij de DBN ICT contactpersoon.

Medewerkers zullen vertrouwelijk omgaan met gebruikersnamen en wachtwoorden. Dit houdt in dat deze nimmer ter beschikking zullen worden gesteld aan derden en veilig worden bewaard. Medewerker is zelf verantwoordelijk voor deze veilige opslag van het wachtwoord in welke vorm dan ook (digitaal of niet digitaal). Bij twijfel kan altijd advies worden ingewonnen bij de DBN ICT contactpersoon.

Medewerker zal in het geval van onregelmatigheden direct melding doen bij de desbetreffende incident manager

Voorbeelden van onregelmatigheden:
- Diefstal/vermissing van een werkstation waarop gewerkt is met de DBN RDP omgeving of waarop DBN RDP inloggegevens zijn opgeslagen.
- Constatering van een virus/ongeoorloofde toegang tot een werkstation waarop gewerkt is met de DBN RDP omgeving of waarop DBN RDP inloggegevens zijn opgeslagen.
- Constatering van ernstige (beveiligings)foutmeldingen tijdens het gebruik van de DBN RDP omgeving

3.1.2. E-mail

Uitgangpunt is dat medewerkers altijd binnen de beveiligde RDP omgeving van DBN met hun e-mail zullen werken. Geautoriseerde mailadressen zijn daar ingesteld per medewerker account en de wachtwoorden van deze mailadressen zijn niet bekend bij de medewerkers en kunnen zodoende niet op andere externe werkstations worden ingesteld. Indien een medewerker noodzaak ziet om zijn/haar mailadres buiten de RDP op een extern werkstation toegankelijk te hebben kan hiertoe een verzoek worden ingediend bij de DBN IT contactpersoon die dit zal beoordelen. Instellen van het mailadres zal altijd door deze contactpersoon uitgevoerd worden. Wachtwoorden van mailadressen zullen nooit worden gecommuniceerd.

Medewerkers zullen vertrouwelijk omgaan met hun DBN e-mail.

Medewerker zal in het geval van onregelmatigheden direct melding doen bij de desbetreffende incident manager

Voorbeelden van onregelmatigheden:
- Diefstal/vermissing van een werkstation waarop gewerkt is met DBN e-mail.
- Constatering van een virus/ongeoorloofde toegang tot een werkstation waarop gewerkt is met DBN e-mail.

3.1.3. DBN Online Diensten (w.o. CRM systeem en digitale leeromgeving)

Medewerkers zullen vertrouwelijk omgaan met gebruikersnamen en wachtwoorden. Dit houdt in dat deze nimmer ter beschikking zullen worden gesteld aan derden en veilig worden bewaard. Medewerker is zelf verantwoordelijk voor deze veilige opslag van het wachtwoord in welke vorm dan ook (digitaal of niet digitaal).

Medewerkers zullen vertrouwelijk omgaan met alle informatie die zich binnen de DBN Online Diensten bevindt.

Medewerker zal in het geval van onregelmatigheden direct melding doen bij de desbetreffende incident manager

Voorbeelden van onregelmatigheden:
- Diefstal/vermissing van een werkstation waarop gewerkt is met de DBN Online Diensten, of waarop inloggegevens van DBN Online Diensten zijn opgeslagen.
- Constatering van een virus/ongeoorloofde toegang tot een werkstation waarop gewerkt is met de DBN Online Diensten, of waarop inloggegevens van DBN Online Diensten zijn op-geslagen.
- Constatering van ernstige (beveiligings)foutmeldingen tijdens het gebruik van de DBN RDP omgeving

4. Protocol datalek

Incident Manager: Pixelbyte. Bereikbaar via mail: info@pixelbyte.nl of telefonisch: 0224-799870 (intern binnen Alles-in-1 op toestelnummer 004)

Escalatiemanager: DPO (/FG) B. Broekema. Bereikbaar via mail: b.broekema@alles-in-1.org of telefonisch: 06-14887207

4.1. RDP

Checklist na een melding n.a.v. een probleem op een extern apparaat waarmee toegang is verkregen tot de DBN RDP server (dus bijvoorbeeld een medewerker die op zijn/haar werkstation een virus heeft of na diefstal van een werkstation). Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap “incidenten”.

1. Toegang dichtzetten: het wachtwoord van de medewerker wordt aangepast. Deze stap wordt binnen 60 minuten binnen werktijd na de melding uitgevoerd.
2. Bepaling ernst van de melding: er wordt een controle van de toegangslogfiles op de RDP server uitgevoerd om te constateren of er sprake is geweest van ongeoorloofde toegang. Is er geen sprake van ongeoorloofde toegang dan wordt doorgegaan naar stap 5.
3. Controle autorisatieniveau medewerker: als er ongeoorloofde toegang tot de RDP server is geweest dan wordt bekeken of de betreffende medewerker een autorisatie-niveau heeft dat toegang geeft tot mappen en/ of email waarin zich bestanden / in-formatie met beschermde persoonsgegevens bevinden. Het gaat hier om de mappen 6.01 t/m 6.11. Is er geen sprake van een autorisatieniveau dat toegang geeft tot één van die mappen dan wordt doorgegaan naar stap 5.
4. Escalatie probleem: op dit moment kan geconcludeerd worden dat er mogelijk toe-gang is geweest tot beschermde persoonsgegevens door een onbevoegd persoon. De escalatiemanager moet worden ingeseind en deze dient de betrokken partijen in te lichten en melding te doen bij de AP.
5. Externe probleem oplossen (optioneel): het probleem op het externe werkstation van de medewerker wordt opgelost. Dit bijvoorbeeld in het geval van een virusmelding.
6. Communicatie aangepaste wachtwoord: het nieuwe wachtwoord wordt telefonisch aan de medewerker doorgegeven. Hiermee krijgt de medewerker weer toegang tot het systeem.

Checklist na een melding n.a.v. een probleem op de DBN RDP server zelf (bijvoorbeeld een virusmelding geconstateerd door een medewerker of een geautomatiseerde veiligheidswaarschuwing gestuurd door het systeem

zelf). Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap “incidenten”.

1. Toegang dichtzetten: de complete toegang tot de RDP server wordt voor alle mede-werkers afgesloten. Deze stap wordt binnen 30 minuten na de melding uitgevoerd.
2. Bepaling ernst van de melding: er wordt een controle van de (antivirus) logfiles op de RDP server uitgevoerd om te constateren of er sprake is geweest van ongeoorloofde toegang. Is er geen sprake van ongeoorloofde toegang dan wordt doorgegaan naar stap 4.
3. Escalatie probleem: op dit moment kan geconcludeerd worden dat er mogelijk toe-gang is geweest tot beschermde persoonsgegevens door een onbevoegd persoon. De escalatiemanager moet worden ingeseind en deze dient de betrokken partijen in te lichten en melding te doen bij de AP.
4. Interne probleem op de DBN RDP server oplossen: het probleem op de RDP server wordt opgelost.
5. Aanpassen wachtwoorden (optioneel): afhankelijk van de ernst van de melding worden de wachtwoorden van alle medewerkers aangepast en aan de medewerker doorgege-ven.
6. Toegang openzetten: de toegang tot de DBN RDP server wordt weer opengezet.

Checklist na een melding waaruit blijkt dat er ongeoorloofde toegang tot gevoelige bestanden op de DBN RDP is geweest). Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap “incidenten”.

1. Toegang dichtzetten: de complete toegang tot de RDP server wordt voor alle mede-werkers afgesloten. Deze stap wordt binnen 30 minuten na de melding uitgevoerd.
2. Escalatie probleem: het probleem wordt geëscaleerd naar de escalatiemanager.
3. Bepalen oorzaak en omvang incident: d.m.v. controle van de logfiles op de RDP server wordt zo precies mogelijk in kaart gebracht hoe het lek is ontstaan en welke bestan-den hierbij betrokken zijn. Dit wordt constant gecommuniceerd met de escalatiema-nager.
4. Externe partijen inlichten: in overleg met de escalatiemanager worden de benodigde externe partijen ingelicht via de bij de escalatiemanager bekende contactgegevens. Daarnaast wordt melding gedaan bij de AP.
5. Oorzaak datalek oplossen: de oorzaak van het datalek wordt opgelost.
6. Aanpassen wachtwoorden: de wachtwoorden van alle medewerkers worden aange-past en aan de medewerkers doorgegeven.
7. Toegang openzetten: de toegang tot de DBN RDP server wordt weer opengezet.

4.2. E-mail

Checklist na een melding n.a.v. een probleem op een extern werkstation waarmee toegang is verkregen tot een DBN e-mail adres (dus bijvoorbeeld een medewerker die op zijn/haar werkstation een virus heeft of na diefstal van een werkstation). Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap “incidenten”.

1. Toegang dichtzetten: het e-mail wachtwoord van de desbetreffende account wordt aangepast en in het geval van een verloren apparaat wordt vanaf de Exchange server indien mogelijk een “remote wipe” van het desbetreffende apparaat uitgevoerd. Deze stap wordt binnen 30 minuten uitgevoerd.
2. Bepaling ernst van de melding: er wordt een controle van de toegangslogfiles op de Exchange mailserver uitgevoerd om te constateren of er sprake is geweest van onge-oorloofde toegang. Is er geen sprake van ongeoorloofde toegang dan wordt doorge-gaan naar stap 5.
3. Controle autorisatieniveau medewerker: als er ongeoorloofde toegang tot de e-mail is geweest dan wordt bekeken of zich in de desbetreffende e-mailbox informatie met be-schermde persoonsgegevens bevindt. Is er geen sprake van aanwezigheid van be-schermde persoonsgegevens dan wordt doorgegaan naar stap 5.
4. Escalatie probleem: op dit moment kan geconcludeerd worden dat er mogelijk toe-gang is geweest tot beschermde persoonsgegevens door een onbevoegd persoon. De escalatiemanager moet worden ingeseind en deze dient de betrokken partijen in te lichten en melding te doen bij de AP.
5. Externe probleem oplossen (optioneel): het probleem op het externe werkstation van de medewerker wordt opgelost. Dit bijvoorbeeld in het geval van een virusmelding.
6. E-mail opnieuw instellen op extern werkstation (optioneel): het aangepaste wacht-woord wordt opnieuw ingesteld op het externe werkstation van de desbetreffende medewerker.
7. Aanpassen van het mailwachtwoord binnen de RDP accounts die toegang hebben tot het betrokken mailaccount

Checklist na een melding waaruit blijkt dat er ongeoorloofde toegang tot gevoelige DBN e-mails is geweest. Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap "incidenten".

1. Toegang dichtzetten: het e-mail wachtwoord van de desbetreffende mailaccount wordt aangepast. Deze stap wordt binnen 30 minuten na de melding uitgevoerd.
2. Escalatie probleem: het probleem wordt geëscaleerd naar de escalatiemanager.
3. Bepalen oorzaak en omvang incident: d.m.v. controle van de logfiles op de RDP en Ex-change server wordt zo precies mogelijk in kaart gebracht hoe het lek is ontstaan. Dit wordt constant gecommuniceerd met de escalatiemanager. Als hieruit blijkt dat het datalek is ontstaan door ongeoorloofde toegang tot de DBN RDP server dan wordt het desbetreffende RDP datalek protocol vanaf hier ook gestart.
4. Externe partijen inlichten: in overleg met de escalatiemanager worden de benodigde externe partijen ingelicht via de bij de escalatiemanager bekende contactgegevens. Ook wordt er melding gedaan bij de AP.
5. Oorzaak datalek oplossen: de oorzaak van het datalek wordt opgelost.
6. E-mail opnieuw instellen op extern werkstation (optioneel, indien er medewerkers be-trokken zijn met dit mailadres ingesteld op een extern werkstation): het aangepaste wachtwoord wordt opnieuw ingesteld op het externe werkstation van de desbetref-fende medewerker.
7. Aanpassen van het mailwachtwoord binnen de RDP accounts die toegang hebben tot het betrokken mailaccount.

4.3. DBN Online Diensten (w.o. CRM systeem en Alles-in-1 Online)

Checklist na een melding n.a.v. een probleem op een extern apparaat waarmee toegang is verkregen tot de DBN Online Diensten (dus bijvoorbeeld een medewerker die op zijn/haar werkstation een virus heeft of na diefstal van een werkstation). Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap "incidenten".

1. Toegang dichtzetten: het wachtwoord van de medewerker wordt aangepast. Deze stap wordt binnen 30 minuten na de melding uitgevoerd.
2. Bepaling ernst van de melding: er wordt een controle van de toegangslogfiles op de Webserver waarop de DBN Online Diensten draaien uitgevoerd om te constateren of er sprake is geweest van ongeoorloofde toegang. Is er geen sprake van ongeoorloofde toegang dan wordt doorgegaan naar stap 6.
3. Controle autorisatieniveau medewerker: als er ongeoorloofde toegang tot de Webser-ver is geweest dan wordt bekeken of de betreffende medewerker een autorisatieni-veau heeft dat toegang geeft tot beschermde persoonsgegevens. Het gaat hier om de autorisatieniveau's admin en coördinator. Is er geen sprake van een autorisatieniveau dat toegang geeft tot beschermde persoonsgegevens dan wordt doorgegaan naar stap 6.
4. Controle bekeken pagina's: er wordt gekeken welke pagina's onder de betrokken ac-count tijdens de ongeoorloofde toegang zijn geraadpleegd. Als het hier om pagina's gaat waarop geen beschermde persoonsgegevens te zien zijn dan wordt doorgegaan naar stap 6.
5. Escalatie probleem: er is met zekerheid toegang geweest tot beschermde persoons-gegevens door een onbevoegd persoon. De escalatiemanager moet worden ingeseind en deze dient de betrokken partijen in te lichten en melding te doen bij de AP.
6. Externe probleem oplossen (optioneel): het probleem op het externe werkstation van de medewerker wordt opgelost. Dit bijvoorbeeld in het geval van een virusmelding.
7. Communicatie aangepaste wachtwoord: het nieuwe wachtwoord wordt telefonisch aan de medewerker doorgegeven. Hiermee krijgt de medewerker weer toegang tot het systeem.

Checklist n.a.v. een geautomatiseerde veiligheidswaarschuwing gestuurd door de DBN Online Diensten zelf. Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap "incidenten".

1. Toegang dichtzetten (optioneel): afhankelijk van de ernst van de melding wordt de complete of een deel van de toegang tot de DBN Online Diensten afgesloten voor al-le, enkele, of een individuele medewerker(s) / scho(o)l(en). Deze stap wordt binnen 60 minuten na de melding uitgevoerd.

2. Controle toegang tot systeem: er wordt een controle van de logfiles en code op de Webserver uitgevoerd om te constateren of er sprake is geweest van toegang tot on-geautoriseerde toegang tot beschermde persoonsgegevens. Is er geen sprake van ongeoorloofde toegang dan wordt doorgegaan naar stap 4.
3. Escalatie probleem: er is met zekerheid toegang geweest tot beschermde persoons-gegevens door een onbevoegd persoon. De escalatiemanager moet worden ingeseind en deze dient de betrokken partijen in te lichten en melding te doen bij de AP.
4. Interne probleem binnen de code van de DBN Online Diensten oplossen: de fout in de programmatuur wordt hersteld.
5. Aanpassen wachtwoorden (optioneel): afhankelijk van de ernst van de melding worden de wachtwoorden van alle, enkele, of een individuele medewerker(s) / scho(o)l(en) aangepast en gecommuniceerd met deze partijen.
6. Toegang openzetten: de toegang tot de DBN Online Diensten wordt weer opengezet.

Checklist na een melding waaruit blijkt dat er ongeoorloofde toegang tot beschermde persoonsgegevens binnen de DBN Online Diensten is geweest. Alle gevolgde stappen worden per incident gedocumenteerd en met datum en beschrijving vastgelegd op de RDP in de map 6.04, in de submap "incidenten".

1. Toegang dichtzetten: de complete toegang tot de DBN Online Diensten wordt voor al-le medewerkers en alle scholen afgesloten. Deze stap wordt binnen 60 minuten na de melding uitgevoerd.
2. Het probleem wordt geëscaleerd naar de escalatiemanager.
3. Bepalen oorzaak en omvang incident: d.m.v. controle van de logfiles en code op de Webserver wordt zo precies mogelijk in kaart gebracht hoe het lek is ontstaan en wel-ke beschermde persoonsgegevens hierbij betrokken zijn. Dit wordt constant gecom-municeerd met de escalatiemanager.
4. Externe partijen inlichten: in overleg met de escalatiemanager worden de benodigde externe partijen ingelicht via de bij de escalatiemanager bekende contactgegevens. Ook wordt er melding gedaan bij de AP.
5. Oorzaak datalek oplossen: de oorzaak van het datalek wordt opgelost.
6. Aanpassen wachtwoorden: de wachtwoorden van alle medewerkers en scholen wor-den aangepast en aan deze partijen gecommuniceerd.
7. Toegang openzetten: de toegang tot de DBN Online Diensten wordt weer opengezet.