Model Bewerkersovereenkomst Versie 2.0

Deze Model Bewerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant) afgesloten tussen de PO-Raad, VO-raad en de brancheorganisaties van educatieve uitgeverij (GEU), distributeurs van leermiddelen (leden van sectie educatief van de Koninklijke Boekverkopersbond) en digitale dienstverleners in het onderwijs-ICT (VDOD).

De uitgangspunten van deze Model Bewerkersovereenkomst sluiten aan bij de bepalingen in het Convenant, de Wet bescherming persoonsgegevens (hierna: Wbp), en de uitgangspunten zoals in jurisprudentie en de toezichthouder de Autoriteit Persoonsgegevens deze in richtsnoeren en uitspraken heeft aangegeven.

De model bewerkersovereenkomst versie 2016 is de opvolger van de model bewerkersovereenkomst die in 2015 in het kader van het *Convenant Digitale Onderwijsmiddelen en Privacy, leermiddelen en toetsen* is opgesteld. De versie 2.0 ziet naast het gebruik van leermiddelen en toetsen ook op School- en Leerlinginformatiemiddelen. Daarnaast is de overeenkomst op onderdelen bijgesteld naar aanleiding van recente ontwikkelingen in wet- en regelgeving, waaronder de wijziging van de Wbp in verband met de meldplicht datalekken.

De nieuwe Model Bewerkersovereenkomst 2.0 komt in de plaats van de Model Bewerkersovereenkomst uit 2015. Reeds afgesloten bewerkersovereenkomsten op basis van het oude model uit 2015 blijven in beginsel hun gelding houden totdat deze bewerkersovereenkomsten door partijen worden beëindigd en aansluitend worden opgevolgd door een nieuwe bewerkersovereenkomst op basis van de nieuwe Model Bewerkersovereenkomst 2.0.

In het Convenant is afgesproken dat Onderwijsinstellingen en Ketenpartijen dit model gebruiken bij het maken van afspraken. Indien geen gebruik kan worden gemaakt van (onderdelen van) de Model Bewerkersovereenkomst, dan kan daar alleen gemotiveerd en schriftelijk van worden afgeweken. Gezien het aantal bepalingen dat ofwel wettelijk is voorgeschreven, of waarvan de Autoriteit Persoonsgegevens aangeeft dat deze in de bewerkersovereenkomst moeten worden opgenomen, is de ruimte voor afwijking van de bepalingen in het model beperkt.

Deze Model Bewerkersovereenkomst bevat twee bijlagen:

1. In de Privacy Bijsluiter (Bijlage 1) wordt een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en onder welke doeleinden deze verwerkingen vallen.
2. In de Technische en Organisatorische Maatregelen (Bijlage 2) wordt omschreven welke beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven

Informatie over het Convenant en de model bewerkersovereenkomst is te vinden op de website *http://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 en VO-raad en bij Kennisnet.

Juni 2016

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: **"Bewerker"**

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

Overwegen het volgende:

a. Onderwijsinstelling en Bewerker zijn een overeenkomst aangegaan waarbij de door Bewerker 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 Bewerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
b. Partijen wensen, mede gelet op het bepaalde in artikel 14 Wet bescherming persoonsgegevens, in deze Bewerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Bewerkersovereenkomst wordt verstaan onder:

a. Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de Wbp;
b. Bewerkersovereenkomst: deze Bewerkersovereenkomst, inclusief Bijlagen;
c. Bijlage: een bijlage bij deze Bewerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;
d. Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy;
e. Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen, dan wel ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zoals bedoeld in artikel 34a, lid 1, Wbp;
f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;

g. 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;
h. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling administratiesysteem, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, een elektronische leeromgeving en een leerling volgsysteem;
i. Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
j. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a;
k. Model Bewerkersovereenkomst: het model voor een bewerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
l. Subbewerker: de partij die door Bewerker wordt ingeschakeld als Bewerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Bewerkersovereenkomst en de Product- en Dienstenovereenkomst;
m. Wbp: Wet bescherming persoonsgegevens.

Artikel 2: Onderwerp en opdracht Bewerkersovereenkomst

1. Deze Bewerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling verstrekt aan de Bewerker de opdracht tot Verwerking van Persoonsgegevens ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst.

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verantwoordelijke. Bewerker is bewerker in de zin van de Wbp. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Bewerker draagt zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Bewerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Bewerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie moet de Onderwijsinstelling in staat stellen een keuze te maken met betrekking tot de aangeboden diensten als zodanig, en daarnaast een afzonderlijke keuze te maken voor eventueel aangeboden optionele diensten.
3. De in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, moeten in de Privacy Bijsluiter bij deze Bewerkersovereenkomst in begrijpelijke taal zijn beschreven, waarna de Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en).
4. De Onderwijsinstelling kan verplicht zijn de Verwerking van de Persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De Onderwijsinstelling onderzoekt of zij hiervan is vrijgesteld en doet melding bij de Autoriteit Persoonsgegevens indien zij hiertoe verplicht is.
5. Onderwijsinstelling en Bewerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de relevante privacywet- en regelgeving mogelijk te maken.

Artikel 4: Privacy convenant

1. Partijen onderschrijven de bepalingen in het Convenant Digitale Onderwijsmiddelen en Privacy.

Artikel 5: Gebruik Persoonsgegevens

1. Bewerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Bewerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (mondeling, schriftelijk dan wel elektronisch) aan Bewerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan.
2. Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst.
3. De Bewerker dient in de Privacy Bijsluiter aan te geven of de Privacy Bijsluiter ziet op een Leermiddel en Toets en/of School- en Leerlinginformatiemiddel. Bewerker specificeert in de Privacy Bijsluiter voor welke (in het Convenant opgenomen) doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt. Indien aangegeven in de toelichting in de Privacy Bijsluiter, dient de Bewerker tevens aan te geven onder welke van de in het Convenant omschreven doeleinden bij het gebruik van het product en/of de dienst de Verwerking van Persoonsgegevens plaatsvindt.

4. Bewerker onthoudt zich van verstrekking van Persoonsgegeven aan een Derde, tenzij deze uitwisseling plaatsvindt in opdracht van de Onderwijsinstelling of wanneer dit noodzakelijk is om te voldoen aan een op de Bewerker rustende wettelijke verplichting. In geval van een wettelijke verplichting, verifieert Bewerker voorafgaande de verstrekking de grondslag van het verzoek en de identiteit van de verzoeker. Daarnaast informeert Bewerker de Onderwijsinstelling – indien wettelijk toegestaan - onmiddellijk, zo mogelijk voorafgaand aan de verstrekking.
5. *SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN HET ONDERWIJSKUNDIG RAPPORT: In aanvulling op het bepaalde in lid 4, geldt dat indien Bewerker wordt verzocht Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde Derde, zijnde een andere onderwijsinstelling, de Bewerker slechts tot die verstrekking zal overgaan nadat deze onderwijsinstelling zijn administratieve onderwijsidentiteit (bijvoorbeeld BRIN of OiN), voor zover hij daarover beschikt, kenbaar heeft gemaakt.*
6. *[SPECIFIEKE BEPALING IN GEVAL VAN DISTRIBUTIE VAN LEERMIDDELEN: Partijen zullen jaarlijks bij 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 aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt, met betrekking tot de (digitale) leermiddelen die op de desbetreffende leermiddelenlijsten worden opgenomen.]*

Artikel 6: Geheimhouding

1. Bewerker zorgt er voor dat een ieder, waaronder haar werknemers, vertegenwoordigers en/of Subbewerkers, die betrokken zijn bij de Verwerking van de Persoonsgegevens deze gegevens als vertrouwelijk behandelt. Bewerker bewerkstelligt dat voor een ieder die betrokken is bij de Verwerking van de Persoonsgegevens een geheimhoudingsovereenkomst of –beding is gesloten.
2. De in dit artikel bedoelde geheimhoudingsplicht geldt niet voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Bewerker aan Onderwijsinstelling te verlenen diensten, of indien er een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 7: Beveiliging en controle

1. Bewerker zal, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. Deze maatregelen zullen, met inachtneming van de stand van de techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van Persoonsgegevens, en de aard daarvan, meebrengen.
2. De maatregelen zoals genoemd in artikel 7.1 omvatten in ieder geval:
   a. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Bewerkersovereenkomst worden verwerkt;
   b. maatregelen om de Persoonsgegevens te beschermen tegen met name onopzettelijke of onrechtmatige vernietiging, verlies, onopzettelijke wijziging, onbevoegde of onrechtmatige opslag, toegang of openbaarmaking;
   c. maatregelen 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;
   d. een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens.
3. Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, 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 technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud en de frequentie van de rapportages die Bewerker aan de Onderwijsinstelling oplevert over de beveiligingsmaatregelen. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de Onderwijsinstelling moet treffen.
5. De Bewerker stelt de Onderwijsinstelling in staat om te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Bewerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken. Naast rapportages door de Bewerker kan dat aan de hand van, maar niet beperkt tot, een geldige certificering of een gelijkwaardig controle- of bewijsmiddel.
6. In aanvulling op artikel 7, lid 4 heeft de Onderwijsinstelling te allen tijde het recht om, in overleg met de Bewerker en met inachtneming van een redelijke termijn, op eigen kosten, de door Bewerker genomen technische en organisatorische beveiligingsmaatregelen te laten toetsen door een onafhankelijke Register EDP auditor. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Bewerker in te schakelen gecertificeerde en onafhankelijke auditor die een derden-verklaring (TPM) afgeeft. De Onderwijsinstelling wordt geïnformeerd over de uitkomsten van de audit.

Artikel 8: Datalekken

1. Bewerker heeft een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling dan wel Bewerker een Datalek vaststelt, dan zal deze de andere Partij onverwijld informeren. Bewerker verstrekt ingeval van een Datalek alle relevante informatie aan Verantwoordelijke met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Bewerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen. Aanvullend informeren Partijen elkaar onverwijld indien blijkt dat de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van Betrokken zoals bedoeld in artikel 34a, lid 2, Wbp.
3. Bewerker stelt bij een Datalek de Verantwoordelijke in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek Bewerker dient hierbij aansluiting te zoeken bij de bestaande processen die Verantwoordelijke 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 Wbp of andere regelgeving betreffende de Verwerking van de Persoonsgegevens, te voorkomen of te beperken.
4. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. Partijen kunnen in onderling overleg bepalen of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten. Op verzoek van de Onderwijsinstelling kan Bewerker Onderwijsinstelling hierbij bijstaan en adviseren. De Onderwijsinstelling zal de Betrokkenen, indien wettelijk vereist, informeren over een dergelijke inbreuk. 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.
5. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e, informeert de Bewerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9: Procedure rechten betrokkenen

1. Een klacht of verzoek van een Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens wordt door de Bewerker onverwijld doorgestuurd naar de Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
2. Bewerker verleent Onderwijsinstelling – voor zover redelijkerwijs mogelijk - volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van Betrokkenen zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens. Partijen zullen te goeder trouw overleggen over de redelijke verdeling van de eventuele kosten die hiermee gemoeid zijn.

Artikel 10: Verwerking buiten de Europese Economische Ruimte

1. Partijen zien er op toe dat voor zover Persoonsgegevens buiten de Europese Economische Ruimte (verder: EER) worden Verwerkt, dit alleen plaatsvindt conform wettelijke voorschriften, en eventuele verplichtingen die in dit verband op Onderwijsinstellingen rusten. Indien gegevens buiten de EER worden verwerkt wordt dit in Bijlage 1 aangegeven, inclusief een opgave van de landen waar de gegevens worden verwerkt.

Artikel 11: Inschakeling Subbewerker

1. Bewerker kan een Subbewerker inschakelen, van wie de identiteit en vestigingsgegevens zullen worden opgenomen in de Privacy Bijsluiter.
2. Bewerker verplicht iedere Subbewerker contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na te leven met betrekking tot de Verwerking van Persoonsgegevens welke verplichtingen en maatregelen minimaal dienen te voldoen aan het bepaalde in deze Bewerkersovereenkomst.
3. Bewerker verplicht iedere Subbewerker contractueel om Persoonsgegevens niet verder te verwerken anders dan in het kader van deze Bewerkersovereenkomst is overeengekomen.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Bewerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Bewerker. Bewerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Bewerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Bewerkersovereenkomst 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. Bewerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
4. Bewerker zal alle Subbewerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Bewerkersovereenkomst en zal waarborgen dat alle Subbewerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Tegenstrijdigheid en wijziging Bewerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Bewerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Bewerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Bewerkersovereenkomst 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 Bewerkersovereenkomst 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, de doeleinden waaronder de Persoonsgegevens worden Verwerkt en het inschakelen van een (andere) Subbewerker. De wijzigingen zullen in Bijlage 1 worden opgenomen.
4. Wijzigingen in de artikelen van de Bewerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
5. In het geval enige bepaling van deze Bewerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Bewerkersovereenkomst 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 14: Duur en beëindiging

1. De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Bewerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Bewerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Bewerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren.

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:	13-07-2017
Plaats:		Plaats:	Lisse

BIJLAGE 1: PRIVACY BIJSLUITER

[Online diensten t.b.v. de leermethode Alles-in-1]
Scholen 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 leerlingen). Scholen moeten met Bewerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft scholen informatie over de dienstverlening die bewerker verleent en welke persoonsgegevens de Bewerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen wiens gegevens worden uitgewisseld.
Het gebruik van deze Privacy Bijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld.
In het kader van de herkenbaarheid is het wenselijk dat Bewerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacy Bijsluiter. 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 Bewerkersovereenkomst gehecht.

A. Algemene informatie

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

B. De specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen

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 oefenresultaten 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 bewerker aanbiedt

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 (opdracht te geven) 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 ☑).
Instemming kan ook plaatsvinden 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 kunnen doen.

a. [N.V.T]
b. [N.V.T]

C. Doeleinden voor het verwerken van gegevens

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

☑ 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 Bewerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de mogelijke doelstellingen van deze producten en diensten omschreven in het daarop betrekking hebbende onderdeel van artikel 5 lid 1 van het Convenant Digitale Onderwijsmiddelen en Privacy 2.0. Deze hoeven in deze Bijsluiter verder niet benoemd te worden.

Ad II. (Alleen) indien de bewerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan dient in deze Privacy Bijsluiter expliciet te worden aangegeven voor welke doeleinden er Persoonsgegevens worden verwerkt bij het gebruik van het product en/of de dienst. De Bewerker dient hierbij zo veel mogelijk aansluiting te zoeken bij de in artikel 5 lid 2 van het Convenant Digitale Onderwijsmiddelen en Privacy 2.0 opgenomen lijst met doeleinden.

D. Categorieën en soorten persoonsgegevens

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:
(leerlinggegevens): naam, school, groep, behaalde oefenresultaten, loginnaam, wachtwoord en tijden van inloggen.
Eventuele optionele Persoonsgegevens (die worden niet standaard gevraagd en opgeslagen): (leerlinggegevens): leeftijd, geboortedatum, pasfoto.
Soorten van gegevens (zoals bijzondere gegevens, of financiële gegevens): n.v.t.

E. Algemene informatie over getroffen beveiligingsmaatregelen:

Voor de genomen veiligheidsmaatregelen wordt kortheidshalve verwezen naar Bijlage 2 bij de Bewerkersovereenkomst.
Specifieke beveiligingsmaatregelen voor deze dienst/product [indien van toepassing]: n.v.t.
Eventuele certificeringen: n.v.t.
Audits/derden-verklaringen: n.v.t.
Plaats/Land van opslag en Verwerking van de Persoonsgegevens: Nederland

F. Subbewerkers

Bewerker maakt voor dienst/product gebruik van de volgende Subbewerkers:

Maketime:	programmeur Alles-in-1 Online
Pixelbyte:	(technische) ondersteuning bij gebruik Alles-in-1 Online, systeemarchitect Alles-in-1 Online
Yeti:	ontwikkelaar Alles Toetsen

Plaats/Land van opslag en Verwerking van de Persoonsgegevens (indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt). N.v.t.

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

H. Versie 1.0, 13-7-2017

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-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://ww.privacyconvenant.nl.

BIJLAGE 2: Technische en organisatorische beveiligingsmaatregelen

De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.
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 2A", "Bijlage 2B", etc.. Deze Bijlagen worden aan de Bewerkersovereenkomst gehecht.

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

I. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Meer in het bijzonder de uitwerking welke (groepen) medewerkers van de Bewerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

a. (groepen van) medewerkers die toegang hebben tot welke Persoonsgegevens:
Er zijn geen DBN medewerkers die direct toegang hebben tot persoonsgegevens
b. handelingen die deze medewerkers uitvoeren met de Persoonsgegevens:

II. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Meer in het bijzonder de uitwerking van de door Bewerker getroffen technische en organisatorische (beveiligings-) maatregelen en de daarbij gehanteerde beveiligingsnorm.
[beschrijving beveiliging applicatie/platform]
[beschrijving wijze van identificatie/authenticatie/autorisatie en beveiliging daarvan]
[beschrijving beveiliging van wijze van uitwisseling/transport van gegevens]

De Alles-in-1 Online code draait op een eigen VPS bij TransIP. Deze server is ingericht met een up-to-date installatie van de Open Source pakketten CentOS7, PHP7 en MariaDB. De server is beschermd met ConfigServer Security & Firewall en een heel strak afgestelde bruteforce monitor. Alleen Pixelbyte heeft als ICT leverancier van bewerker 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

De code staat buiten de webserver in een externe subversion repository van Maketime ter backup en t.b.v. release management. Alleen medewerkers van Maketime hebben na authenticatie toegang tot deze repository.

De PHP code is gebaseerd op de nieuwste PHP versie (7) en het Symfony Framework versie 2.8, dat is een LTS versie met security fixes t.m. november 2019. Na deze datum wordt er overgegaan op de dan geldende LTS versie.

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 10 versie, beveiligd met een wachtwoord. Na twee minuten inactiviteit logt het systeem automatisch uit. Virusscanner Kaspersky Total Security is geïnstalleerd, up-to-date en draait wekelijks scans naast de standaard monitoring.

III. Omschrijving van de maatregelen 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.

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.

Rapportage (artikel 7.4 van de Bewerkersovereenkomst

Bewerker rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 31-12 aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.
Contactgegevens helpdesk/servicedesk voor beveiligingsincidenten: Pixelbyte, Aert de Gelderlaan 312, 1816NG, Alkmaar. Tel: 0224-799870.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

Afspraken over het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging, met name over

- De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
  - Zie bijlage 2a 'Procedure datalek DBN'
- De wijze waarop informatie wordt gedeeld:
  - Op welke manier (via e-mail, telefoon); primair via telefoon, mocht telefonisch contact niet mogelijk zijn dan via de e-mail.
  - Aan wie gericht (contactpersonen en contactgegevens); aan de door de Onderwijsinstelling in het beheerscherm van de Alles-in-1 Online omgeving aangegeven primaire contactpersoon. Is deze primaire contactpersoon niet bereikbaar dan via de andere contactpersonen.
  - Met wie kan (bij vervolgacties) contact worden opgenomen.
- Informatie die in ieder geval over een incident gedeeld moet worden
  - Zie bijlage 2a 'Procedure datalek DBN'
  - 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, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie 1.0 13-7-2017

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-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://ww.privacyconvenant.nl.

BIJLAGE 2A: Procedure datalek DBN

Laatst bijgewerkt: 13-7-2017

1. Definities

Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen, dan wel ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zoals bedoeld in artikel 34a, lid 1, Wbp;

Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de Wbp;

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 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 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 opgeslagen.
- 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 autorisatieniveau heeft dat toegang geeft tot mappen en/of email waarin zich bestanden / informatie 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 toegang 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 medewerkers 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 toegang 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 doorgegeven.
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 medewerkers 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 bestanden hierbij betrokken zijn. Dit wordt constant gecommuniceerd 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. 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 aangepast 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 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 e-mail is geweest dan wordt bekeken of zich in de desbetreffende e-mailbox informatie met beschermde persoonsgegevens bevindt. Is er geen sprake van aanwezigheid van beschermde persoonsgegevens dan wordt doorgegaan naar stap 5.
4. Escalatie probleem: op dit moment kan geconcludeerd worden dat er mogelijk toegang 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 wachtwoord 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 Exchange 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 betrokken zijn met dit mailadres ingesteld op een extern werkstation): het aangepaste wachtwoord 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.

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 Webserver is geweest dan wordt bekeken of de betreffende medewerker een autorisatieniveau 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 account 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 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.
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 alle, 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 ongeautoriseerde 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 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 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 alle 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 welke beschermde persoonsgegevens hierbij betrokken zijn. Dit wordt constant gecommuniceerd 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 worden aangepast en aan deze partijen gecommuniceerd.
7. Toegang openzetten: de toegang tot de DBN Online Diensten wordt weer opengezet.