# Algemene Verwerkersovereenkomst 4.0

## Gebaseerd op de model verwerkersovereenkomst 4.0

## behorend bij het Convenant Digitale Onderwijsmiddelen en Privacy 4.0[1]

**Partijen:**

1. Het bevoegd gezag van _____, geregistreerd onder (bevoegd gezag) administratienummer _____ (zoals het BRIN-nummer of RIO-nummer bij de Dienst Uitvoering Onderwijs van het ministerie van Onderwijs, Cultuur en Wetenschap of het KvK-nummer), gevestigd en kantoorhoudende aan _____, te _____, te dezen rechtsgeldig vertegenwoordigd door _____, hierna te noemen: "**Onderwijsinstelling**"

en

2. De Digitale Gesprekscyclus BV, KvK-nummer 5762 8440, gevestigd en kantoorhoudende aan Anthonie Verherentstraat 1, te (1961 GD) Heemskerk, te dezen rechtsgeldig vertegenwoordigd door Daniel Hoopman (directeur), hierna te noemen: "**Verwerker**"

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

**Overwegen het volgende:**

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij is overeengekomen dat Verwerker software levert aan Onderwijsinstelling voor het aanleggen van een digitaal gespreksdossier, het invullen van competentieprofielen en het verwerken van persoonsgegevens. Deze overeenkomst (hierna: Onderliggende Overeenkomst), schriftelijk of op andere wijze afgesloten, leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens Verwerkt;
b. Verwerker levert geen diensten of producten die kwalificeren als digitaal onderwijsmiddel zoals bedoeld in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0;
c. Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 AVG, 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. AVG: de Algemene verordening gegevensbescherming (Verordening (EU) 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);
b. Betrokkene, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, Verwerker en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG
c. Bijlage(n): bijlage(n) bij de Verwerkersovereenkomst;
d. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
e. Instructies: geschreven of elektronisch gestuurde aanwijzing van de Onderwijsinstelling in de hoedanigheid van Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar

[1] Het Convenant Digitale Onderwijsmiddelen en Privacy 4.0 zoals te vinden op www.privacyconvenant.nl

bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Onderliggende Overeenkomst;

f. Onderwijsdeelnemer: een leerling of student in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs, waaronder ook speciaal onderwijs en voortgezet speciaal onderwijs zoals bedoeld in de Wet op de expertisecentra, alsmede de vavo-student en de deelnemer educatie;

g. Onderwijsinstelling: het bevoegd gezag als bedoeld in de artikelen 1 van de Wet op het primair onderwijs, Wet op het voortgezet onderwijs en Wet op de expertisecentra en de instelling als bedoel in artikel 1.1.1. sub b van de Wet educatie en beroepsonderwijs;

h. Onderliggende Overeenkomst: de overeenkomst tussen (scholen die vallen onder de) Onderwijsinstelling en Verwerker, zoals omschreven in Overweging a. met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en de Verwerker voor het betreffende product of de betreffende dienst;

i. Schriftelijk: handgeschreven of gedrukte teksten, zowel in digitale als in analoge vorm;

j. Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Algemene Verwerkersovereenkomst en de Onderliggende Overeenkomst;

k. Subverwerkersovereenkomst: een overeenkomst of andere rechtshandeling waarmee Verwerker minimaal dezelfde verplichtingen inzake gegevensbescherming oplegt aan de door hem ingeschakelde Subverwerker als in deze Verwerkersovereenkomst aan Verwerker zijn opgelegd;

l. Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de 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;

m. Toezichthoudende Autoriteit: toezichthoudende autoriteit als bedoeld in artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

**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 Onderliggende Overeenkomst.
2. Deze Verwerkersovereenkomst vervangt eventuele Verwerkersovereenkomsten die in het verleden tussen Partijen zijn afgesloten in het kader van de onder Overweging a. bedoelde producten/diensten zoals vastgelegd in de Onderliggende Overeenkomst.
3. De Onderwijsinstelling in de hoedanigheid van Verwerkingsverantwoordelijke geeft Verwerker conform artikel 28 AVG Instructies om Persoonsgegevens te Verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling zijn onder meer omschreven in Bijlage 1 van deze Verwerkersovereenkomst. Deze opdracht en eventuele nadere Instructies worden schriftelijk verstrekt door en aan de contactpersonen van Partijen die hiertoe bevoegd zijn verklaard. Deze contactpersonen zijn opgenomen in voornoemde bijlage.
4. De Verwerker informeert de Onderwijsinstelling zo snel mogelijk indien een Instructie naar mening van Verwerker in strijd is met de AVG of andere toepasselijke wetgeving. Onderwijsinstelling is in een dergelijk geval gehouden om te beoordelen of de Instructie inderdaad in strijd is met de AVG of andere toepasselijke wetgeving, gedurende welke beoordeling Verwerker niet gehouden zal zijn de Instructie op te volgen.
5. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen, die plaatsvinden ter uitvoering van de Onderliggende Overeenkomst. 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 haar opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over (het bepalen van) het doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Verwerker draagt er zorg voor dat de Onderwijsinstelling bij 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 gebruik kan maken van eventueel aangeboden optionele diensten.
3. In aanvulling op lid 2 en onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker bij 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 door Verwerker 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. 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.
5. 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: Gebruik Persoonsgegevens**

1. Verwerker verplicht zich om de van de Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel waarvoor de gegevens zijn verstrekt of aan hem bekend zijn geworden. Verwerker Verwerkt de Persoonsgegevens uitsluitend in opdracht van de Onderwijsinstelling en op basis van de Instructies van de Onderwijsinstelling. Verwerker Verwerkt de Persoonsgegevens niet voor eigen doeleinden of doeleinden van derden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking, zoals doorlevering aan een derde, verplicht. In dat geval stelt Verwerker de Onderwijsinstelling voorafgaand aan de Verwerking op basis van dat wettelijke voorschrift in kennis, tenzij de betreffende wetgeving een dergelijke kennisgeving om gewichtige redenen van algemeen belang verbiedt.
2. In aanvulling op lid 1 vindt de Verwerking van Persoonsgegevens met betrekking tot de geleverde producten en/of diensten nooit plaats voor reclamedoeleinden of het doen van ongevraagde aanbiedingen door Verwerker.
3. De Onderwijsinstelling en Verwerker specificeren in Bijlage 1 voor welke, door de Onderwijsinstelling in de hoedanigheid van Verwerkingsverantwoordelijke vastgestelde, doeleinden Persoonsgegevens worden Verwerkt bij het gebruik van zijn product en/of dienst, welke Verwerkingen daarvoor plaatsvinden en welke categorieën Persoonsgegevens van welke Betrokkenen daarbij worden Verwerkt. De Onderwijsinstelling draagt er zorg voor dat er niet meer Persoonsgegevens dan vastgelegd in Bijlage 1 worden doorgegeven aan Verwerker.
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.

**Artikel 5: Vertrouwelijkheid**

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk behandelt. Verwerker zorgt ervoor dat eenieder die hij betrekt bij de Verwerking van Persoonsgegevens, waaronder zijn werknemers, vertegenwoordigers en/of Subverwerkers, een geheimhoudingsplicht heeft die ten minste ziet op de Persoonsgegevens en de omstandigheden waaronder die worden Verwerkt.
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 zoals verwoord in de Onderliggende Overeenkomst; of
    c. indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling tot verstrekking verplicht is.
3. Ingeval door een Derde een beroep wordt gedaan op een wettelijke verplichting als bedoeld in lid 2 sub c, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker – tenzij de betreffende wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt – Onderwijsinstelling onmiddellijk, voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.
4. Verwerker zorgt ervoor dat de onder diens gezag en/of verantwoordelijkheid werkende personen uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

**Artikel 6: Beveiliging en controle**

1. Met inachtneming van het bepaalde in artikel 32 AVG dragen beide Partijen zorg voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en te 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 (vergelijkbaar met de toepasselijke ISO-normering en/of vergelijkbaar met het geldende Certificeringsschema informatiebeveiliging en privacy ROSA);
    b. maatregelen om te waarborgen dat enkel geautoriseerde personen die onder gezag en/of verantwoordelijkheid van de Verwerker werken, 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. De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te (laten) controleren.
3. In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de in lid 1 en 2 bedoelde passende technische en organisatorische beveiligingsmaatregelen.
4. Beide Partijen dragen er zorg voor dat zij de eigen getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.
5. De Verwerker stelt in goed overleg met de Onderwijsinstelling deze in staat om effectief te kunnen voldoen aan haar 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 7 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 Verwerking van Persoonsgegevens in relatie tot de Onderliggende Overeenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen, te (doen) controleren middels een audit:
    a. Partijen spreken in onderling overleg af dat de audit wordt uitgevoerd door een door één van de Partijen, na goedkeuring door de andere Partij, in te schakelen onafhankelijke gecertificeerde externe deskundige die een derdenverklaring (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 derdenverklaring gebruikt kunnen worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
    e. Partijen komen overeen dat de kosten van een audit als bedoeld in sub a 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 7: Datalekken**

1. Beide Partijen hebben een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling of Verwerker een Datalek bij de uitvoering van de Onderliggende Overeenkomst of van deze Verwerkersovereenkomst vaststelt, dan zal deze de andere Partij daarover *zonder onredelijke vertraging* informeren, zodra zij of hij kennis heeft genomen van dat Datalek. Verwerker verstrekt in geval 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. In aanvulling op lid 2 informeert Verwerker de 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, voor zover deze aan Verwerker bekend zijn gemaakt. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking van 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.
6. 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.
7. 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.
8. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, informeert de Verwerker de Onderwijsinstelling conform de afspraken zoals beschreven in Bijlage 2.

**Artikel 8: Medewerking**

1. Verwerker verleent Onderwijsinstelling medewerking bij het nakomen van de op Onderwijsinstelling in de hoedanigheid van Verwerkingsverantwoordelijke rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, waaronder, 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 tot inzage, rectificatie, wissing of beperking van de verwerking van Persoonsgegevens;
   b. het uitvoeren van controles en audits zoals bedoeld in artikel 6 van deze Verwerkersovereenkomst;
   c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB/DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
   d. het voldoen aan verzoeken van een Toezichthoudende Autoriteit of een andere overheidsinstantie;
   e. het (voorbereiden van) onderzoeken (naar), beoordelen en melden van Datalekken zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst.
2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van een Toezichthoudende Autoriteit met betrekking tot de Verwerking van de Persoonsgegevens, wordt door Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek of de klacht.
3. Partijen brengen, onverlet het bepaalde in artikel 6 lid 6 sub e, artikel 7 lid 6 en artikel 12 lid 3, 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 9: Doorgifte aan derde landen buiten de Europese Economische Ruimte**

1. Verwerker is uitsluitend gerechtigd tot doorgifte van Persoonsgegevens aan een derde land buiten de Europese Economische Ruimte (EER) of aan een internationale organisatie indien Onderwijsinstelling daarvoor specifieke schriftelijke toestemming heeft gegeven, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot doorgifte verplicht. In dat geval stelt Verwerker Onderwijsinstelling voorafgaand aan de doorgifte schriftelijk op de hoogte van deze bepaling, tenzij de betreffende wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
2. Indien na toestemming van Onderwijsinstelling Persoonsgegevens worden doorgegeven aan derde landen buiten de EER of aan een internationale organisatie zoals bedoeld in artikel 4 sub 26 AVG, dan zien Partijen erop toe dat dit alleen plaatsvindt conform wettelijke voorschriften en eventuele verplichtingen die in dit verband op Onderwijsinstelling rusten. Indien van toepassing staat in Bijlage 1 bij deze Verwerkersovereenkomst een opgave van de derde 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.
3. Als voor de doorgifte naar een derde land buiten de EER gebruik wordt gemaakt van een door de Europese Commissie goedgekeurd modelcontract (*standard contractual clauses*), dan moeten er indien nodig voldoende aanvullende maatregelen worden genomen om te waarborgen dat het niveau van bescherming van de Persoonsgegevens tijdens en na de doorgifte gelijkwaardig is aan het beschermingsniveau binnen de EER. Deze maatregelen moeten worden beschreven in Bijlage 1.

**Artikel 10: Inschakeling Subverwerker**

1. Onderwijsinstelling geeft Verwerker door ondertekening van deze Verwerkersovereenkomst toestemming tot het inschakelen van Subverwerkers, van wie de identiteit en vestigingsgegevens zijn opgenomen in Bijlage 1.
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. De bezwaartermijn bedraagt 6 weken volgend op schriftelijke inlichting aan Onderwijsinstelling over de voorgenomen toevoeging of wijziging.
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. Verwerker zal op verzoek van Onderwijsinstelling afschriften verstrekken van deze Subverwerkersovereenkomsten, of van de relevante passages uit de Subverwerkersovereenkomst of een andere overeenkomst of een andere bindende rechtshandeling tussen Verwerker en de door deze overeenkomstig artikel 10 lid 1 van deze Verwerkersovereenkomst ingeschakelde Subverwerker.

**Artikel 11: Bewaartermijnen en vernietiging Persoonsgegevens**

1. Onderwijsinstelling informeert Verwerker in Bijlage 1 adequaat over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker Verwerkt de Persoonsgegevens niet langer dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Verwerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst binnen een door Partijen gezamenlijk overeengekomen termijn terug te (doen) leveren aan de Onderwijsinstelling en/of te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van een Unierechtelijke of lidstaatrechtelijke verplichting, dan wel op verzoek van de Onderwijsinstelling.
3. Verwerker bevestigt Onderwijsinstelling Schriftelijk dat vernietiging van de Verwerkte Persoonsgegevens als bedoeld in lid 2 heeft plaatsgevonden. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
4. Verwerker ziet erop toe en waarborgt dat ook alle Subverwerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens, de Persoonsgegevens (laten) terug leveren en/of vernietigen na het verstrijken van bewaartermijnen dan wel de termijn voor het terug leveren en/of vernietigen zoals bedoeld in lid 2.

**Artikel 12: Aansprakelijkheid**

1. Partijen kunnen afspraken over aansprakelijkheid die voortvloeit uit deze Verwerkersovereenkomst, opnemen in de Onderliggende Overeenkomst of in een andere overeenkomst of regeling tussen Partijen.
2. In afwijking van het eerste lid kunnen Partijen geen beroep doen op een aansprakelijkheidsbeperking die is opgenomen in de Onderliggende Overeenkomst of een andere tussen Partijen bestaande overeenkomst of regeling, in geval van een door één van de Partijen 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 Toezichthoudende Autoriteit betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.
3. Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken Partij op grond van de geldende wet- of regelgeving ter beschikking staan. Het bepaalde in lid 2 sub b geldt onverminderd het bepaalde in artikel 13 lid 2.

4. Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of (het voornemen om over te gaan tot) het opleggen van een bestuurlijke boete door de Toezichthoudende Autoriteit, beide 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 (het voornemen tot) een 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 zoveel mogelijk vooraf over deze kosten.
5. De Partij (hierna de “Benaderde Partij”) die door de Toezichthoudende Autoriteit in kennis is gesteld van het voornemen om over te gaan tot het opleggen van een bestuurlijke boete (verder: “Voornemen tot handhaving”) in verband met deze Verwerkersovereenkomst, zal:
    a. in het verweer tegen het Voornemen tot handhaving rekening houden met de redelijke belangen van de andere Partij;
    b. de andere Partij in redelijkheid in de gelegenheid stellen om haar zienswijze met betrekking tot het Voornemen tot handhaving aan de Benaderde Partij te geven, en
    c. geen schikkingsvoorstel van de Toezichthoudende Autoriteit accepteren, of afstand doen van een rechtsmiddel tegen het Voornemen tot handhaving, of een boete, zonder hierover eerst de andere Partij te consulteren.

**Artikel 13: Tegenstrijdigheid en wijziging Verwerkersovereenkomst**

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Onderliggende Overeenkomst, zijn de bepalingen van deze Verwerkersovereenkomst leidend.
2. Indien Partijen bij het afsluiten van deze Verwerkersovereenkomst van de artikelen in deze Algemene Verwerkersovereenkomst willen afwijken, of deze willen aanvullen, dan worden deze wijzigingen en/of aanvullingen door Partijen beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Verwerkersovereenkomst wordt gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.
3. Onverminderd het bepaalde in artikel 10 lid 2 wordt bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten na het afsluiten van deze Verwerkersovereenkomst, die van invloed zijn op de Verwerking van de Persoonsgegevens zoals beschreven in Bijlagen 1 en 2, de Onderwijsinstelling, alvorens zij de wijzigingen aanvaardt, in begrijpelijke taal door de Verwerker geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die kan leiden tot een uitbreiding van de te Verwerken Persoonsgegevens en die gevolgen kan hebben voor de door Onderwijsinstelling vastgestelde doeleinden waarvoor de Persoonsgegevens worden Verwerkt. Deze wijzigingen zullen in Bijlage 1 of Bijlage 2 worden opgenomen.
4. Wijzigingen in de artikelen van de Verwerkersovereenkomst na het afsluiten van de Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid en schriftelijk tussen Partijen 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 14: Duur en beëindiging**

1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Onderliggende Overeenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Onderliggende Overeenkomst. Totdat de Persoonsgegevens door de Verwerker zijn terug geleverd en vernietigd overeenkomstig het bepaalde in artikel 11, blijft de Verwerker ervoor zorgen dat de artikelen van deze Verwerkersovereenkomst worden nageleefd.

**Artikel 15: Toepasselijk recht en geschillenbeslechting**

1. De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.
2. Alle geschillen die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, worden voorgelegd aan de rechter die bevoegd is verklaard in de Onderliggende Overeenkomst. Is in de Onderliggende Overeenkomst geen rechter bevoegd verklaard, dan is de rechter bevoegd in de plaats waar Onderwijsinstelling gevestigd is.

**Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,**

| Onderwijsinstelling, | Verwerker, |
|---|---|
| |  |
| Naam: | Naam: Daniel Hoopman |
| Functie: | Functie: Directeur |
| Datum: | Datum: 12 januari 2023 |

Bijlage 1: Privacybijsluiter
Bijlage 2: Beveiligingsbijlage
Bijlage 3: Wijzigingenbijlage

## Door Partijen in te vullen bijlagen bij de Algemene Verwerkersovereenkomst

# BIJLAGE 1: PRIVACYBIJSLUITER [naam product/dienst]

### A. Contactgegevens

Voor vragen of opmerkingen over deze Privacybijsluiter of de werking van dit product en/of deze dienst, kunt u terecht bij:

| | **Functie en naam contactpersoon** | **Contactgegevens** |
|---|---|---|
| Verwerker | Marten Wilmink (FG) | marten@ddgc.nl |
| Onderwijsinstelling* | | |

* Deze contactpersoon is bevoegd/gemandateerd om namens de Onderwijsinstelling opdrachten en Instructies aan de Verwerker te verstrekken.

### B. Versienummer en versiedatum

Versienummer 1.0 d.d. 12 januari 2023

### C. Algemene informatie *(in te vullen door Verwerker)*

| | |
|---|---|
| Naam product en/of dienst | De Digitale Gesprekscyclus, DDGC |
| Naam Verwerker en vestigingsgegevens | De Digitale Gesprekscyclus BV<br>Anthonie Verherentstraat 1<br>1961 GD HEEMSKERK |
| Link naar Leverancier (website/URL) | https://ddgc.nl |
| Link naar productpagina (website/URL) | https://ddgc.nl |
| Beknopte uitleg en werking product en/of dienst | Met de Digitale Gesprekscyclus vertaal je organisatiedoelen naar individuele afspraken en concrete doelstellingen. Tientallen functies helpen je om de inhoud van de gesprekken, competenties en 360°-feedback digitaal vast te leggen en te analyseren. |
| Doelgroep (po/vo/(v)so/mbo) | Po/vo/(v)so/mbo |
| Gebruikers (Onderwijsdeelnemers/ ouders/verzorgers/medewerkers) | Medewerkers / onderwijs professionals |

### D. Omschrijving specifieke producten en/of diensten
***(in te vullen door Verwerker)***

De Verwerker dient in de onderstaande tabel een omschrijving te geven van de specifiek aangeboden producten en/of diensten en bijbehorende Verwerkingen van Persoonsgegevens. Hierbij worden ook koppelingen en uitwisseling met derde partijen beschreven. Daarbij moet apart worden aangegeven of de verwerking *noodzakelijk* is voor het aanbieden van de producten en/of diensten, dan wel optioneel is.

1. Producten en/of diensten en bijbehorende Verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product en/of de aangeboden dienst.

| Omschrijving product en/of dienst | Bijbehorende Verwerking(en) |
|---|---|
| Digitale Gesprekscyclus | Opslag gespreksverslagen, competentieprofielen en persoonsgegevens |

2. Aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de Verwerker aanbiedt. In de laatste kolom kruist de Onderwijsinstelling aan of deze akkoord gaat met de aanvullende optionele producten en/of diensten en bijbehorende Verwerking(en).

| Omschrijving product en/of dienst | Bijbehorende Verwerking(en) | Akkoord van de Onderwijsinstelling |
|---|---|---|
| | | ☐ |
| | | ☐ |

## E. Doeleinden voor het verwerken van Persoonsgegevens

Opgave van specifieke doeleinden van toepassing zijn op het product of de dienst.

| Doeleinde |
|---|
| Verwerker verwerkt Persoonsgegevens zodat de gebruikers kunnen inloggen op de software en derhalve met de software kunnen werken. Dat betekent concreet, afhankelijk van het type gebruiker, dat er gespreksverslagen kunnen worden vastgelegd, dat er competentieprofielen kunnen worden ingevuld en dat account- en gebruikersgegevens kunnen worden aangepast. |
| |
| |
| |

## F. Categorieën Persoonsgegevens inclusief bewaartermijnen

1. Geef in de onderstaande tabel aan over welke categorieën Betrokkenen welke categorieën Persoonsgegevens worden verwerkt, met waar mogelijk een specificatie.

| Betrokkene: Onderwijsdeelnemer | | |
|---|---|---|
| **Categorie persoonsgegevens** | **Specificatie** | **Aankruisen indien van toepassing op Verwerking(en)** |
| Contactgegevens | Voorna(a)m(en) | ☐ |
| | Voorletter(s) | ☐ |
| | Achternaam | ☐ |
| | Geslacht | ☐ |
| | Woonadres | ☐ |
| | Postcode | ☐ |
| | Woonplaats | ☐ |
| | Telefoonnummer | ☐ |
| | E-mailadres (privé) | ☐ |
| | E-mailadres (school) | ☐ |
| Burgerservicenummer (BSN) of PGN | | ☐ |
| Onderwijsdeelnemer-nummer | Een administratienummer dat Onderwijsdeelnemers identificeert | ☐ |
| Nationaliteit | | ☐ |
| Geboortedatum | | ☐ |
| Geboorteplaats | | ☐ |
| Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen | | ☐ |

| | | |
|---|---|---|
| Gegevens over gezondheid* | Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de Betrokkene of op verzoek van de Onderwijsdeelnemer worden verwerkt, een en ander voor zover noodzakelijk voor het onderwijs | ☐ |
| Godsdienst* | Gegevens betreffende de godsdienst of levensovertuiging van de Betrokkene, voor zover die noodzakelijk zijn voor het onderwijs of op verzoek van de Onderwijsdeelnemer worden verwerkt, een en ander voor zover noodzakelijk voor het onderwijs | ☐ |
| Andere Persoonsgegevens, namelijk | *[Leg hier de andere te verwerken Persoonsgegevens vast. Het moet gaan om Persoonsgegevens die noodzakelijk zijn voor de Verwerking(en) en Doeleinde(n) die zijn omschreven onder D. en E.]* | ☐ |

* Dit zijn bijzondere Persoonsgegevens die niet verwerkt mogen worden, tenzij is voldaan aan de eisen van de AVG en de UAVG.

| **Betrokkene: ouder/voogd/verzorger** | | |
|---|---|---|
| **Categorie gegevens** | **Specificatie** | **Aankruisen indien van toepassing op Verwerking(en)** |
| Contactgegevens | Voorna(a)m(en) | ☐ |
| | Voorletter(s) | ☐ |
| | Achternaam | ☐ |
| | Aanschrijftitel zoals geslacht | ☐ |
| | Woonadres | ☐ |
| | Postcode | ☐ |
| | Woonplaats | ☐ |
| | Telefoonnummer | ☐ |
| | E-mailadres (privé) | ☐ |
| | | ☐ |
| Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen | | ☐ |
| Andere Persoonsgegevens, namelijk: | *[Leg hier de andere te verwerken Persoonsgegevens vast. Het moet gaan om Persoonsgegevens die noodzakelijk zijn voor de Verwerking(en) en Doeleinde(n) die zijn omschreven onder D. en E.]* | |

| **Betrokkene: medewerker Onderwijsinstelling** | | |
|---|---|---|
| **Categorie gegevens** | **Specificatie** | **Aankruisen indien van toepassing op Verwerking(en)** |
| Contactgegevens | Voorna(a)m(en) | ☒ |
| | Voorletter(s) | ☒ |
| | Achternaam | ☒ |
| | Aanschrijftitel zoals geslacht | ☒ |
| | E-mailadres (school) | ☒ |
| | Foto's en videobeelden (**beeldmateriaal**) van Betrokkene met of zonder geluid van activiteiten van de Onderwijsinstelling | ☒ |
| Andere Persoonsgegevens, namelijk: | *Onderstaande gegevens zijn optionele Verwerkingen:*<br>*a. Door verwerkingsverantwoordelijk vastgelegde gegevens rondom functioneren, beoordeling, persoonlijke ontwikkeling, competenties, etc.*<br>*b. Organisatiedeel*<br>*c. Functie*<br>*d. Leidinggevende van*<br>*e. Foto(bestand)* | |

| | | |
|---|---|---|
| | g. Telefoonnummer<br>h. Mobiel nummer<br>i. Datum in dienst<br>j. Personeelsnummer<br>k. Geboortedatum<br>l. Straat of postbus<br>m. Huisnummer<br>n. Postcode<br>o. Stad<br>p. Provincie en land | |

2. Bewaartermijn van de Persoonsgegevens of de criteria om die vast te stellen

Opgave van de (wettelijke) bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen) die van toepassing zijn op de Verwerking van Persoonsgegevens door de Verwerker.

Gegevens worden bewaard voor de looptijd van de Overeenkomst, tenzij Verwerkingsverantwoordelijke zelf gegevens verwijderd. Bij beëindiging van de Overeenkomst is Verwerkingsverantwoordelijke zelf verantwoordelijk voor het verwijderen van de gegevens in de applicatie.

## G. Locatie van opslag en Verwerking Persoonsgegevens

Geef hieronder voor alle bij onderdeel D beschreven Verwerkingen aan in welk land de Verwerking plaatsvindt. Indien een of meer Verwerkingen buiten de Europese Economische Ruimte (EER) plaatsvinden, dient in de tweede tabel nadere informatie over die Verwerking en de doorgifte te worden opgenomen.

| Verwerking (zie onderdeel D) | Plaats/Land van opslag en Verwerking van de Persoonsgegevens |
|---|---|
| 1. Amazon Web Services (AWS) | Frankfurt, Duitsland |

Alle gegevens worden opgeslagen via de RDS database service van Amazon. De bestanden van gebruikers worden opgeslagen via de Simple Storage Service (S3) van Amazon. Amazon is een bedrijf dat gevestigd is in de Verenigde Staten. Amazon garandeert dat persoonsgegevens die in Europa worden opgeslagen nooit naar de Verenigde Staten worden getransporteerd, tenzij zij daartoe wettelijk verplicht is.

Mochten er toch persoonsgegevens naar de Verenigde Staten worden getransporteerd, dan garandeert Amazon dat op die gegevensverwerking in de Verenigde Staten hetzelfde strenge privacy-regime van toepassing is als in Europa. Om deze garantie te kunnen bieden is Verwerker met Amazon een overeenkomst aangegaan (AWS Data Processing Addendum) die Amazon heeft laten goedkeuren door de Europese privacy toezichthouders.

De Persoonsgegevens van de gebruikers worden dus ook op deze servers opgeslagen. Persoonsgegevens in de database zullen worden opgeslagen op servers in Ierland en zullen niet worden gekopieerd of verplaatst naar servers in landen waar een minder streng privacy-regime heerst dan in Europa.

### Back-up

Verwerker slaat back-upgegevens op servers van Amazon. Daartoe gebruikt Verwerker het datacentrum van Amazon in Duitsland.

Via de volgende link is na te lezen hoe Amazon de bescherming van persoonsgegevens garandeert:

https://aws.amazon.com/compliance/data-privacy-faq/

## H. Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst algemene schriftelijke toestemming voor het inschakelen van een Subverwerker.

Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:

| | |
|---|---|
| **Naam Subverwerker** | Amazon Web Services |
| **Soort Verwerking (beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt)** | Hosting code, database, bestanden en backups |
| **(Categorie) Persoonsgegevens die de Subverwerker verwerkt** | Contactgegevens en andere persoonsgegevens medewerkers onderwijsinstelling |
| **Land van opslag/Verwerking Persoonsgegevens door Subverwerker** | Duitsland |
| **Vestigingsland Subverwerker**<br><br>NB Vergeet niet indien de Verwerking van de gegevens buiten de Europese Economische Ruimte plaatsvindt, ook onderdeel G in te vullen. | Luxemburg |

| | |
|---|---|
| **Naam Subverwerker** | TechNative |
| **Soort Verwerking (beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt)** | Beheer hosting, code, database, bestanden, backups |
| **(Categorie) Persoonsgegevens die de Subverwerker verwerkt** | Contactgegevens en andere persoonsgegevens medewerkers onderwijsinstelling |
| **Land van opslag/Verwerking Persoonsgegevens door Subverwerker** | Nederland |
| **Vestigingsland Subverwerker**<br><br>NB Vergeet niet indien de Verwerking van de gegevens buiten de Europese Economische Ruimte plaatsvindt, ook onderdeel G in te vullen. | Nederland |

| | |
|---|---|
| **Naam Subverwerker** | Dinfini |
| **Soort Verwerking (beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt)** | Software architectuur en ontwikkeling, technische support |
| **(Categorie) Persoonsgegevens die de Subverwerker verwerkt** | Contactgegevens en andere persoonsgegevens medewerkers onderwijsinstelling |
| **Land van opslag/Verwerking Persoonsgegevens door Subverwerker** | Nederland |
| **Vestigingsland Subverwerker**<br><br>NB Vergeet niet indien de Verwerking van de gegevens buiten de Europese Economische Ruimte plaatsvindt, ook onderdeel G in te vullen. | Nederland |

| | |
|---|---|
| **Naam Subverwerker** | CodeSeed |
| **Soort Verwerking (beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt)** | Software architectuur en ontwikkeling, technische support |
| **(Categorie) Persoonsgegevens die de Subverwerker verwerkt** | Contactgegevens en andere persoonsgegevens medewerkers onderwijsinstelling |
| **Land van opslag/Verwerking Persoonsgegevens door Subverwerker** | Griekenland |
| **Vestigingsland Subverwerker**<br><br>NB Vergeet niet indien de Verwerking van de gegevens buiten de Europese Economische Ruimte plaatsvindt, ook onderdeel G in te vullen. | Griekenland |

# BIJLAGE 2: BEVEILIGINGSBIJLAGE DDGC

**Versie** 1.0 d.d. 12 januari 2023

In verband met de aantoonbaarheid van de technische beveiligingsmaatregelen van het product of de dienst verklaart Verwerker periodiek 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 hiervoor genoemde minimale beveiligingsmaatregelen wordt voldaan;

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

Voor een weergave van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van standaarden, maakt de Verwerker in beginsel gebruikt van het ‘Certificeringsschema informatiebeveiliging en privacy ROSA’ (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.

**A. Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking**

- Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast.
- Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.
- Verwerker heeft een coördinator voor informatiebeveiliging om risico’s omtrent de verwerking van Persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.
- Verwerker sluit met medewerkers geheimhoudingsverklaringen af en maakt informatiebeveiligingsafspraken.
- Verwerker stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.

**B. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen**

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Verwerker gebruikt hiervoor in beginsel het ‘Certificeringsschema informatiebeveiliging en privacy ROSA’ (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.

| **BIV-classificatie** | Beschikbaarheid=M (2), Integriteit=M (2), Vertrouwelijkheid=H (3) | | |
|---|---|---|---|
| **Categorie** | **Maatregelen** | **Compliance** | **Uitleg** |
| | | | Zie uitleg onder tabel bij ieder onderwerp voor een toelichting. |
| **Beschikbaarheid** | Ontwerp | Voldaan | |
| | Capaciteit beheer | Voldaan | |
| | Onderhoud | Voldaan | |
| | Testen | Voldaan | |
| | Monitoring | Voldaan | |
| | Herstel | Voldaan | |
| **Integriteit** | Herleidbaarheid (gebruikers) | Voldaan | |
| | Back-up | Voldaan | |
| | Application controls | Voldaan | |
| | Onweerlegbaarheid | Voldaan | |
| | Herleidbaarheid (technisch beheer) | Voldaan | |
| | Controle integriteit | Voldaan | |
| | Onweerlegbaarheid | Voldaan | |
| **Vertrouwelijkheid** | Levenscyclus gegevens | Voldaan | |
| | Logische toegang | Voldaan | |
| | Fysieke toegang | Voldaan | |
| | Netwerktoegang | Voldaan | |
| | Scheiding omgevingen | Voldaan | |
| | Transport en fysieke opslag | Voldaan | |
| | Logging | Voldaan | |
| | Omgaan met kwetsbaarheden | Voldaan | |

**Beschikbaarheid (niveau 2)**

***Overbelasting***
De applicatie is ingericht voor gebruik door veel verschillende gebruikers tegelijkertijd en resources kunnen eventueel automatisch worden bijgeschaald in geval dit nodig is. Monitoring houdt 24/7 in de gaten of resources tekort dreigen te schieten. Door de aard van de applicatie loggen veel gebruikers echter slechts enkele malen per jaar in om het systeem te raadplegen. Het aantal 'grootverbruikers' is daardoor relatief laag.

***Business continuity***
Tijdens verruimde kantoortijden (07:00 – 22:00) is de streeftijd voor het opzetten van een volledig nieuwe server stack en terugzetten van een backup maximaal 6 uur (RTO), inclusief communicatie. Daarnaast worden van de laatste 24 uur iedere 3 uur backups van de volledige database en vervolgens worden dagelijkse backups bewaard (RPO).

***Ontwerp***
De Digitale Gesprekscyclus is een op zichzelf staande web applicatie en is naast de AWS servers niet van andere diensten afhankelijk voor de werking. Gebruikers die bij organisaties zijn aangesloten die werken met Single Sign On oplossingen en inloggen via AFAS InSite of Microsoft 365 ondervinden problemen met inloggen als deze diensten offline zijn.

***Monitoring***
De beschikbaarheid en werking van de applicatie en servers wordt via verschillende monitoring tools bijgehouden. Onder andere via CloudWatch, Sentry en FreshPing worden eventuele outages direct gemeld bij de verantwoordelijke personen.

***Testen***
De software van De Digitale Gesprekscyclus wordt automatisch getest op beschikbaarheid.

***Software***
Security patches voor besturingssystemen en server software worden ten minste maandelijks uitgevoerd. Eventuele urgente security issues worden direct toegepast. Upgrades van OS versies en frameworks worden periodiek uitgevoerd, waarbij vooral gekeken wordt naar Long-term Support (LTS) releases.

***Actuele dreigingen (DDoS, ransomware)***
Voor bescherming tegen DDoS aanvallen wordt gebruik gemaakt van Amazon Web Services (AWS) Cloudfront, Shield en Elastic Load Balancing. De combinatie van deze drie zorgt dat de applicatie de meest gebruikelijke vectoren voor een DDoS aanval kan opvangen.

Om eventueel dataverlies bij onbeschikbaarheid of corruptie van een server / database zo veel mogelijk in te perken, worden frequent backups gemaakt (RPO). Backups worden gemaakt volgens het schema:

- 8 backups (iedere 3 uur) van afgelopen 24 uur
- 7 dagelijkse backups bewaren afgelopen 7 dagen
- 4 wekelijkse backups bewaren van afgelopen 4 weken
- 6 maandelijkse backups bewaren van afgelopen 6 maanden

## Integriteit

*Integriteit van gegevens*

***Herleidbaarheid (gebruikers)***
De applicatie biedt alleen toegang aan gebruikers als deze met gebruikersnaam en wachtwoord inloggen dat aan een persoonlijk account gekoppeld is, óf via een token als ze uitgenodigd worden als externe om feedback te geven. Hoe dan ook zijn alle acties te herleiden tot gebruikers en bestaan er geen naamloze gebruikers accounts. Van alle belangrijke wijzigingen die gebruikers doen worden log events gemaakt. Van wijzingen op organisatieniveau worden notificaties aan beheerders gestuurd.

***Backup***
Backups worden meerdere malen per dag gemaakt (iedere 3 uur) en vervolgens worden backups bewaard volgens het schema genoemd in ‘Actuele dreigingen’ onder Betrouwbaarheid. Hiermee is RPO max 3 uur. Een restore wordt minimaal twee maal per jaar getest.

***Application controls***
Alle invoer op de applicatie wordt gecontroleerd en gevalideerd op eventuele gevaarlijke syntax of content (XSS, CRLF, executable file uploads, SQL injectie). Van alle aanpassingen worden logs bijgehouden op applicatie niveau.

***Onweerlegbaarheid***
Alle activiteit van gebruikers vindt plaats na inloggen en gebeurt dus nooit anoniem (dan wel met gebruikersnaam/wachtwoord, of met token). Er zijn logging tools in gebruik die (automatisch) op afwijkende patronen en onregelmatigheden reageren en hier melding van maken.

*Integriteit van de toepassing*

***Herleidbaarheid (technisch beheer)***
De software staat in een versiebeheerde repository (GitLab), waarmee wijzigingen eenvoudig zijn terug te draaien. Systeemaccounts voor server access (AWS) zijn herleidbaar naar beheerders en het is inzichtelijk wanneer welke wijzigingen zijn doorgevoerd.

***Controle integriteit***
Updates aan firware en software worden handmatig uitgerold (OS, server software, framework). Bij de ontwikkeling van de software worden de best practices op het gebied van security gevolgd.

***Onweerlegbaarheid***
Belangrijke aanpassingen door beheerders worden vastgelegd in log events in de applicatie. Alle wijzigingen worden bijgehouden in systeem logging van de software.

***Actuele dreigingen (DDoS, ransomware)***
Zoals bij onderdeel Actuele dreigingen in Beschikbaarheid vemeldt, zijn er maatregelen getroffen om een rollback uit te voeren naar een gecontroleerde situatie van korter dan 24 uur geleden. In het meest gunstige geval zelfs enkele uren. De AWS infrastructuur is in staat om de meest gebruikelijke DdoS aanvallen op te vangen en af te weren. Middels monitoring op storingen en handmatige steekproeven bij vermoedens kan snel worden bepaald of er sprake is van een disruptie.

**Vertrouwelijkheid**

***Levenscyclus gegevens***
De wettelijke bewaartermijnen voor het opslaan van de gegevens worden uitgevoerd volgens de AVG. Klant heeft de rol van Verwerkingsverantwoordelijke en kunnen gegevens verwijderen indien gewenst. DDGC verwijderd in de rol van Verwerker nooit gegevens van Klant en behoudt alleen gegevens voor maximaal 6 maanden in een backup bestand. In de training en richtlijnen voor personeel van De Digitale Gesprekscyclus wordt gemaand tot zeer zorgvuldige omgang met Persoonsgegevens.

***Logische toegang***
Alle gebruikers loggen met hun persoonlijke account in op het systeem via gebruikersnaam en wachtwoord en kunnen hier optioneel gebruik maken van twee-factor authenticatie via SMS of OTP app als Google Authenticator. Een wachtwoord van de Digitale Gesprekscyclus moet uit tenminste 12 karakters bestaan en voldoen aan tenminste 3 van de 4 eisen: 1 Hoofdletter (A t/m Z), 1 Kleine letter karakters (a t/m z), 1 Getal (0 t/m 9), 1 Speciaal karakter (!, $, #, %, etc.). De lengte van het wachtwoord kan desgewenst worden ingesteld door de Klant, met een minimale lengte van 8 karakters.

***Fysieke toegang***
De servers met database gegevens staan bij Amazon AWS in Frankfurt. Hier heeft DDGC geen fysieke toegang tot. Alleen beheerders van AWS hebben hier toegang tot.

***Netwerk toegang***
De server met de database is alleen toegankelijk via een gelogde VPN verbinding met beveiligde sleutels. Alleen applicatie beheerders en ontwikkelaars die server onderhoud plegen hebben toegang tot productieomgevingen.

***Scheiding omgevingen***
De servers van Productie (live) en Acceptatie (test) omgevingen bestaan uit gescheiden server omgevingen.

***Transport en fysieke opslag***
Gegevens worden nooit via fysieke opslag media (externe harddrives of UBS-sticks) opgeslagen voor backups of andere doeleinden.

***Logging***
Toegang tot de servers en acties op de codebase worden via diverse logging systemen bijgehouden.

***Toetsing***
Risico analyse op basis van veelvoorkomende bedreigingen uit OWASP top 10 en security scans worden gebruikt om verbeteringen door te voeren en applicatie up-to-date te houden. Daarnaast wordt gebruik gemaakt van een framework waarvan de core en modules regelmatig worden geupgrade, oa bij melding van security issues die bekend worden gemaakt.

***Actuele dreigingen (DDoS, ransomware)***
Alle medewerkers en ontwikkelaars van DDGC zijn op de hoogte van mogelijke bedreigingen en risico's omtrent datalekken en zijn op de hoogte van de Procedure Datalek in geval van calamiteiten.

**Informatiebeveiligingsbeleid (IBB) De Digitale Gesprekscyclus**

De veiligheid van de software die De Digitale Gesprekscyclus BV (hierna: DDGC) aanbiedt, staat hoog in het vaandel. We hebben daarom een Informatiebeveiligingsbeleid (IBB) met procedures en protocollen opgesteld. Op deze manier is zowel intern als voor voor klanten helder hoe gehandeld dient te worden in verschillende situaties. Het IBB is een formeel beleidsdocument dat tweemaal per jaar wordt herzien en aangevuld.

### Risico Management Team

Binnen de organisatie van De Digitale Gesprekscyclus is een Risico Management Team verantwoordelijk voor de uitvoer van het Risico Management Programma (RMP) en het beheren van alle documenten zoals genoemd in de Leeswijzer. Het Risico Management Team bestaat uit:

- **Data Protection Officer (DPO)** – Marten Wilmink
  Verantwoordelijk voor het Risico Management Programma en voorzitter RMT;
- **Directeur De Digitale Gesprekscyclus** – Daniel Hoopman
  Verantwoordelijk voor De Digitale Gesprekscyclus BV;

### Risico Management Programma

De Digitale Gesprekscyclus heeft voor het beheersen van haar Informatiebeveiligingsbeleid een Risico Management Programma (RMP) ingericht dat wordt uitgevoerd door het Risico Management Team (RMT). Dit team bestaat uit de Data Protection Officer en Directeur DDGC en komt iedere zes maanden bijeen voor:

- Analyse van risico's voor privacy en veiligheid binnen bedrijfsprocessen en uitvoering;
- Evaluatie van eerder geïmplementeerde verbetermaatregelen en voorstel van eventuele aanpassingen;
- Opstellen concrete actiepunten en verbetermaatregelen voor nieuwe en bestaande risico's;
- Verslaglegging (verantwoordelijkheid DPO);

De aanpak van risico's binnen het RMP is gebaseerd op de Plan-Do-Check-Act-cyclus. Dit betekent dat continu wordt gekeken naar optimalisatie van processen en beleid op het gebied van veiligheid, ontwikkeling en risico's:

- **Plan** – Analyse beveiligingsrisico's, vaststellen prioriteit en ontwerpplan van aanpak voor optimalisatie.
- **Do** - Uitvoering geplande optimalisatie;
- **Check** - Evaluatie resultaat van de optimalisatie;
- **Act** - Bijstellen aan de hand van de gevonden resultaten bij Check.

### Interne documenten

- **Calamiteitenplan** – Intern document met beleid en beschrijving van de procedures bij diverse calamiteiten zoals een storing, diefstal, datalek, nalatigheid of uitval;
- **Risico Instructie** – Instructie voor medewerkers en partners van DDGC met beschrijving van mogelijke gevaren en risico's van het werken met gevoelige gegevens en een

beschrijving van de verantwoordelijkheden, functies en taken van de verschillende personen binnen de organisatie;

**Human Resources**

Alle medewerkers en partners van DDGC worden gescreend alvorens ze in dienst treden bij DDGC op basis van een Verklaring Omtrent het Gedrag (VOG). Deze screening zal periodiek worden uitgevoerd.

Nieuwe medewerkers van DDGC en externe partijen die met gevoelige informatie van DDGC werken, tekenen een geheimhoudingsverklaring waarin ze bevestigen dat ze de Informatiebeveiligingstraining (IBT), het Calamiteitenplan en de Procedure Datalek die DDGC voorlegt bij indiensttreding, hebben gelezen en begrepen. De IBT bevat een overzicht van de verantwoordelijkheden die medewerkers aangaan bij indiensttreding en de bewustwording van de mogelijke consequenties van nalatigheid of bepaalde beslissingen.

Alle documenten binnen het Informatiebeveiligingsbeleid worden jaarlijks bijgewerkt als onderdeel van het Risico Management Programma. Medewerkers en externen worden vervolgens van de aanpassingen op de hoogte gesteld. Het opfrissen van de informatie uit de IBT, het Calamiteitenplan en de Procedure Datalek is een vast onderdeel tijdens de jaarlijkse beoordelingscyclus van DDGC met haar medewerkers en wordt als dusdanig ook vastgelegd in het gespreksverslag.

**Logische toegang**

De Data Protection Officer is verantwoordelijk voor het beheer van de logische toegang tot belangrijke gegevens met betrekking tot de applicatie. Hier valt te denken aan toegangscodes, sleutels en wachtwoorden voor servers, software en databases.

De logische toegang voor de verschillende onderdelen van de organisatie, zoals de software, de servers, het CRM, diverse social mediakanalen en de website zijn vastgelegd in wachtwoord software met aparte kluizen voor verschillende niveaus en onderdelen. De directeur van DDCC is verantwoordelijk voor de fysieke toegang tot panden, het sleutelbeleid en de alarminstallatie.

Jaarlijks of indien noodzakelijk geacht, wordt de logische toegang als onderdeel van het PDCA van alle medewerkers en betrokkenen geëvalueerd en waar nodig bijgesteld. Indien gewenst kan een overzicht worden gegeven van alle personen met logische toegang.

**Privacy**

Met betrekking tot de privacy van gebruikers en de verwerking van gegevens is een apart Privacybeleid opgesteld. Deze is te vinden op de website van DDGC (https://ddgc.nl/algemeen/privacy). Klanten van DDGC zijn wettelijk verplicht om in hun rol als Verwerkingsverantwoordelijke, zoals gedefinieerd in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG”), een verwerkersovereenkomst aan te gaan met de Verwerker van persoonsgegevens, in dit geval DDGC. DDGC biedt hiervoor een Verwerkersovereenkomst aan die ondertekend kan worden om aan deze plicht te voldoen. In deze Verwerkersovereenkomst worden de persoonsgegevens beschreven die worden verwerkt in opdracht van de Verwerkingsverantwoordelijke.

**Datalek**

In geval van een datalek treedt de Procedure Datalek in werking en zal de aangestelde Data Protection Officer (DPO) binnen één werkdag melding maken aan de Verwerkingsverantwoordelijke over de aard, omvang en impact van het betreffende incident. Tevens zal binnen twee dagen melding nadat de verantwoordelijke persoon binnen DDGC er kennis van heeft genomen, het incident bij de Autoriteit Persoonsgegevens gemeld worden. Lees voor meer informatie over dit onderwerp het document Procedure Datalek.

**Ontwikkeling**

Bij het ontwikkelen van de software voor DDGC is veiligheid en bescherming van de (persoons)gegevens één van de belangrijkste pijlers. Naast het continu testen van de software door ontwikkelaars en testers, worden ook de best practices aangehouden op het gebied van veilige software. Het bijwerken en updaten van alle gebruikte software, frameworks en modules naar de meest recente versies is hiervan een belangrijk onderdeel.

Bij aanpassingen van de software of serverconfiguratie wordt een impactanalyse uitgevoerd. Concreet worden alle wijzigingen op een acceptatieomgeving die identiek is aan de productieomgeving getest. De software wordt op de acceptatieomgeving softwarematig en handmatig getest om de werking te controleren en de impact van aanpassingen of upgrades op andere onderdelen binnen de software te analyseren. Updates worden volgens het Releasebeleid van DDGC uitgevoerd. Onderdeel van dit beleid is de communicatie richting gebruikers voor en na geplande update.

**Beveiligingsmaatregelen**

Verwerker neemt de bescherming van de Persoonsgegevens zeer serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Verwerker implementeert daartoe de volgende maatregelen met betrekking tot de software en infrastructuur:

Beveiligingssoftware: virusscanner en firewall;

- TLS (voorheen SSL): Verwerker verstuurt Persoonsgegevens (en alle andere gegevens) via een beveiligde internetverbinding;
- DKIM en SPF: zijn twee internetstandaarden die Verwerker gebruikt om te voorkomen dat gebruikers uit naam van Verwerker e-mails ontvangt die virussen bevatten, spam zijn of bedoeld zijn om persoonlijke (inlog)gegevens te bemachtigen.

**Certificering**

Amazon AWS is ISO-27001 gecertificeerde hostingpartij die hiermee voldoen aan de beste praktijken en standaarden met betrekking tot informatiebeveiliging en controle. De Digitale Gesprekscyclus houdt een eigen beveiligingsbeleid aan waarbij tijd wordt besteed aan het up-to-date blijven met de praktijk. DDGC richt zich op het goed op orde hebben van de software en optimalisatie van de software om haar klanten en gebruikers zo goed mogelijk van dienst te kunnen zijn. Met alle beveiligingsmaatregelen en vertrouwde hosting partners voldoet Verwerker aan alle gangbare normen en voor beveiliging.

## C. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Verwerker heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zal Verwerker de Verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- de kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens);
- de oorzaak van de inbreuk;
- hoe de inbreuk is ontdekt;
- de maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht etc. waren;
- de groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen;
- wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor de groep(en) Betrokkene(n);
- de hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Verwerker in beginsel per e-mail contact met elkaar opnemen via onderstaande contactgegevens, dan wel de contactgegevens zoals opgenomen in Bijlage 4.

| | **Naam en functie contactpersoon bij beveiligingsincidenten/Datalekken** | **Contactgegevens (e-mail en telefoonnummer)** |
|---|---|---|
| **Verwerker** | *Marten Wilmink (FG)* | *support@ddgc.nl , 075-670 2715* |
| **Onderwijsinstelling** | | |

***Procedure Datalek De Digitale Gesprekscyclus***

*De Digitale Gesprekscyclus respecteert uw privacy en al uw gegevens worden vertrouwelijk behandeld. De verwerking van persoonsgegevens geschiedt altijd op een manier die in overeenstemming is met de eisen die de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679, hierna AVG) en eventuele andere wet- en regelgeving daaraan stelt. In deze Procedure Datalek wordt in meer detail uiteengezet hoe De Digitale Gesprekscyclus in onverhoopt geval met het verlies van dergelijke gegevens omgaat.*

Dit document beschrijft de verschillende stappen die binnen DDGC genomen worden bij een datalek, die valt onder de Meldplicht Datalekken. De Meldplicht Datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en is met ingang van 1 januari 2016 in werking getreden. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige

verwerking. Een datalek moet onverwijld (binnen 2 dagen) nadat de verantwoordelijke persoon binnen DDGC er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens (voorheen CBP) gemeld worden.

Het datalek moet ook worden gemeld bij de betrokkenen. In het geval van DDGC zijn dit over het algemeen klanten (gebruikers van de software) of medewerkers. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.

De Verwerker is verplicht om een datalek te melden bij de Verwerkingsverantwoordelijke.

1) **Verwerkingsverantwoordelijke (klant DDGC)** - De Verwerkingsverantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De Verwerkingsverantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten), zoals staat beschreven in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG);
2) **Verwerker (De Digitale Gesprekscyclus BV)** - De organisatie die de gegevens ten behoeve van de Verwerkingsverantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. De Verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Verwerkingsverantwoordelijke. De Verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens, zoals tevens staat beschreven in de tussen Verwerkingsverantwoordelijke en Verwerker overeengekomen Verwerkersovereenkomst.

Mogelijke oorzaken van een datalek:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- technisch falen (fouten of bugs in software, verlate updates, storingen);
- menselijk falen (onzorgvuldige omgang gebruikersnaam of wachtwoord, nalatigheid);
- verloren of gestolen hardware (externe harde schijf, USB stick, server-apparatuur of laptop);
- verzenden e-mail naar meerdere gebruikers met openbaring van e-mailadressen;
- calamiteit (brand datacentrum, wateroverlast).

**Melding**

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door de Data Protection Officer (DPO). De melding kan door iedere gebruiker en iedere medewerker of derde partij worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van DDGC. De melding moet direct en telefonisch worden gedaan bij de DPO en schriftelijk worden vastgelegd. Deze meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.

De Data Protection Officer legt vast:

- naam van de melder;
- de contactpersoon voor de melding;
- datum en tijd van de melding;
- aard van de inbreuk en risico op verlies of onrechtmatig gebruik gegevens;
- welke persoonsgegevens vallen onder de melding;
- om welk aantal gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen.

**Escalatie bij afwezigheid**

Bij afwezigheid van de Data Protection Officer wordt diens rol ingevuld door de directeur DDGC. Als deze ook afwezig is, wordt diens rol ingevuld door de Privacy Officer. Buiten kantoortijden en in het weekend wordt de melding gedaan bij de DPO. Bij het niet kunnen bereiken van de DPO, wordt de melding gedaan bij de directeur DDGC.

**Analyse**

De Data Protection Officer en de Privacy Officer beoordelen of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats door de DPO.

Is dit wel het geval, dan voert de DPO de acties uit zoals beschreven in het Calamiteitenplan van DDGC:

1) Telefonisch informeren directeur DDGC;
2) Tijdens kantooruren onmiddellijk bijeenroepen van het Responseteam Datalek, bestaande uit:
    a) **Data Protection Officer** (DPO) – Marten Wilmink
    *Verantwoordelijk voor het Risico Management Programma en voorzitter RMT;*
    *b)* **Directeur De Digitale Gesprekscyclus** – Daniel Hoopman
    *Verantwoordelijk voor De Digitale Gesprekscyclus BV;*
    *c)* **Privacy Officer** (indien noodzakelijk) – mr. J.P. Kuhlmann (extern)
    *Juridisch adviseur wet en regelgeving op het gebied van privacy en IT.*

De DPO neemt overdag telefonisch contact op met de Privacy Officer. Als het mogelijk is, wordt een eventueel benodigd overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is, wordt zoveel als mogelijk telefonisch en elektronisch overleg gevoerd.

**Responseteam Datalek**

Het Responseteam Datalek wordt met hoge prioriteit bijeengeroepen door de DPO. De bijeenkomst wordt voorgezeten door de DPO. Het responseteam bespreekt en legt vast:

- De gegevens die door de DPO zijn vastgelegd bij het aannemen van de melding;

- De noodzakelijke vervolgacties met betrekking tot het datalek (lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- De melding die opgesteld moet worden voor de Autoriteit Persoonsgegevens door de DPO. Naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records:
    - De mogelijke gevolgen voor de betrokkenen;
    - De maatregelen die DDGC neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
    - De maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
    - Contactgegevens voor betrokkenen.
- De wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en manager(s);
- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd), of een onrechtmatige daad;
- Of het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit DDGC zelf, een klant, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de Privacy Officer;
- Wat er intern wordt gecommuniceerd over het incident;
- Wat er extern wordt gecommuniceerd over het incident en vaststellen of de pers geïnformeerd moet worden;
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden;
- Of er individuen, klanten, leveranciers geïnformeerd moeten worden;
- Op welke wijze er intern wordt gerapporteerd;
- Of eventuele schade is gedekt door de verzekeringspolis.

**Afhandeling**

De DPO rapporteert aan de directeur DDGC de uitkomsten van het overleg van het Responseteam Datalek. De directeur DDGC accordeert de uit te voeren activiteiten, zoals vastgesteld door het Responseteam Datalek, of stelt de uit te voeren activiteiten bij. De door de directeur DDGC vastgestelde activiteiten worden uitgevoerd.

**Melding bij de Autoriteit Persoonsgegevens**

De DPO meldt binnen 2 dagen volgens de aangewezen methode het datalek via het Meldpunt Datalek van de Autoriteit Persoonsgegevens (https://datalekken.autoriteitpersoonsgegevens.nl/). In ieder geval zal gemeld moeten worden:

- Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, beschrijving gegevens;

- Beschrijving van de te verwachten gevolgen;
- Getroffen en/of voorgestelde maatregelen;
- Informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- Contactgegevens voor betrokkene;

**Ontvangstbevestiging Autoriteit Persoonsgegevens**

Is er een melding gedaan, dan ontvangt DDGC een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met DDGC om de herkomst van de melding te verifiëren.

**Terugkoppeling betrokken**

Na de melding bij de Autoriteit Persoonsgegevens en eventuele getroffen maatregelen zal terugkoppeling plaatsvinden bij de betrokkenen. Hierna zal het incident worden afgesloten en zullen de getroffen maatregelen worden geëvalueerd binnen de PDCA-cyclus van het Risico Management Programma.

# BIJLAGE 3: WIJZIGINGENBIJLAGE

INDIEN VAN TOEPASSING: VERPLICHTE BESCHRIJVING VAN DE NOODZAKELIJKE AFWIJKINGEN VAN ALGEMENE VERWERKERSOVEREENKOMST

**Versie** [versienummer en datum laatste aanpassing]

Overzicht van afwijkingen, zoals bedoeld in artikel 13, lid 2 van de Algemene Verwerkersovereenkomst, en de motivering daarvan.

**Partijen zijn de volgende wijzigingen overeengekomen:**

| 1. Beschrijving noodzakelijke afwijkingen Algemene Verwerkersovereenkomst | |
|---|---|
| Betreft artikel | |
| Wijziging of aanvulling? | |
| Huidige tekst artikel | |
| Nieuwe tekst artikel (onderstreep wijzigingen en aanvullingen) | |
| Reden van wijziging of aanvulling (noodzaak en motivering) | |

# FACULTATIEVE BIJLAGE 4 (ENKEL INDIEN VAN TOEPASSING): SCHOLEN VALLEND ONDER HET BEVOEGD GEZAG VAN HET BESTUUR

| **Gegevens schoolbestuur** | |
|---|---|
| Naam schoolbestuur | |
| Adres schoolbestuur | |
| Administratienummer schoolbestuur* | |
| Contactpersoon namens het schoolbestuur | |

Deze verwerkersovereenkomst is van toepassing op de onderstaande scholen:

| **Administratie-nummer*** | **Schoolnaam** | **Plaats** | **Mailadres** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

* Administratienummer: het BRIN- of RIO-nummer bij de Dienst Uitvoering Onderwijs van het ministerie van OCW, of het KvK-nummer.