Verwerkersovereenkomst

Jij en Je Gezondheid – Voortgezet onderwijs

Versie 30 januari 2019

Partijen:

1. ……[naam instelling], gevestigd en kantoorhoudende aan ……[straat, postcode] te ……[plaats], te dezen rechtsgeldig vertegenwoordigd door ……[functie + naam], hierna te noemen: 'Instelling',

en

2. De GGD Amsterdam, gevestigd en kantoorhoudende aan Nieuwe Achtergracht 100, 1018 WT, te Amsterdam, te dezen rechtsgeldig vertegenwoordigd door directeur José Manshanden, hierna te noemen: 'Verwerker',

Hierna gezamenlijk te noemen: 'Partijen', of afzonderlijk 'Partij',

Overwegende het volgende:

a) Instelling en Verwerker zijn een overeenkomst aangegaan waarbij de Verwerker producten en diensten aan de Instelling levert zoals omschreven in de Product- en Dienstenovereenkomst van *Jij en Je Gezondheid* (kortweg: JEJG). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Instelling Persoonsgegevens verwerkt.

b) Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Verwerkersovereenkomst wordt verstaan onder:

a) AVG: de Algemene Verordening Gegevensbescherming inclusief de uitvoeringswet van deze verordening.
b) Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG.
c) Bijlage: een bijlage bij deze Verwerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt.
d) Datalek: een inbreuk op de beveiliging van Persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG.
e) Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenoverenkomst.
f) Product- en Dienstenovereenkomst: de overeenkomst tussen Instelling en Verwerker, zoals omschreven in overweging a.
g) SubVerwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.
h) TOPdesk: een service management systeem van de Verwerker voor de registratie en afhandeling van meldingen en incidenten.
i) Verwerkersovereenkomst: deze Verwerkersovereenkomst, inclusief Bijlagen.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst, en geeft invulling aan verplichtingen op grond van de AVG en op deze wet van toepassing zijn de jurisprudentie.

2. Instelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te Verwerken namens de Instelling. De Instructies van de Instelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.

3. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen zoals opgenomen in **Bijlage 1** (Privacy bijsluiter), die plaatsvinden ter uitvoering van de Product- en Dienstenovereenkomst. Verwerker brengt Instelling onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker tijdelijk niet langer aan de Verwerkersovereenkomst kan voldoen.

Artikel 3: Rolverdeling

1. Instelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. Instelling heeft en houdt zelfstandige zeggenschap over het (bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.

2. Verwerker draagt er zorg voor dat de Instelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de diensten die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Instelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Instelling een keuze kan maken voor eventueel aangeboden optionele diensten.

3. Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker voorafgaand aan het sluiten van deze Verwerkersovereenkomst de Instelling in **Bijlage 1** over de in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, en de Verwerkingen die in dat kader plaatsvinden. De in **Bijlage 1** opgenomen informatie moet in begrijpelijke taal zijn beschreven, waardoor Instelling geïnformeerd akkoord kan gaan met de afname van deze diensten en de uitvoering van de bijbehorende Verwerkingen.

4. De Instelling neemt de in lid 2 genoemde Verwerking van de Persoonsgegevens op in een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.

5. Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Instelling verricht.

6. Instelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de AVG betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

7. Verwerker zal geen SubVerwerker inschakelen om Persoonsgegevens te Verwerken. Verwerking van Persoonsgegevens vindt uitsluitend in Nederland plaats.

Artikel 4: Gebruik Persoonsgegevens

1. Verwerker verplicht zich om de van Instelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Instelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan.

2. Lid 1 is van toepassing behoudens een eventueel afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een rechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat. In dat geval stelt Verwerker de Instelling voorafgaande aan de Verwerking van dat wettelijke voorschrift dan wel de rechtelijke uitspraak in kennis, tenzij dergelijke kennisgeving om gewichtige redenen van algemeen belang verboden is.

3. Een overzicht van onder meer de categorieën Persoonsgegevens en het, door de Verwerkersverantwoordelijke vastgestelde, doel waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in **Bijlage 1.** Indien Verwerker in strijd met de AVG het doel van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.

4. Verwerker mag, in aanvulling op lid 1, Persoonsgegevens Verwerken voor wetenschappelijk en statistisch onderzoek, mits anoniem en onder de voorwaarden zoals genoemd in de Product- en Dienstenovereenkomst.

Artikel 5: Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van Derden. Verwerker waarborgt dat met de tot het Verwerken van Persoonsgegevens geautoriseerde personen een geheimhoudingsovereenkomst of –beding is gesloten, of dat deze door een wettelijke verplichting tot geheimhouding is gebonden.

2. De in lid 1 bedoelde geheimhoudingsplicht geldt niet in de hierna genoemde gevallen:
   a) voor zover Instelling 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 Instelling te verlenen diensten; of
   c) indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling dan wel gerechtelijke uitspraak, voor zover daartegen geen beroep openstaat, tot verstrekking verplicht is.

3. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaande de verstrekking de wettelijke grondslag van de verstrekking en de identiteit van de ontvanger. Daarnaast stelt Verwerker Instelling onmiddellijk, in beginsel voorafgaand aan de verstrekking, in kennis van relevante informatie inzake deze verstrekking, tenzij wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

4. Verwerker zorgt er voor dat de onder diens gezag werkende medewerkers uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

Artikel 6: Beveiliging en controle

1. Met inachtneming van het bepaalde in artikel 32 AVG zal Verwerker, gelijk Instelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en te beschermen tegen ongeoorloofde of onrechtmatige Verwerking en tegen verlies, vernietiging of beschadiging.

2. 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, met inachtneming van de risico’s die het Verwerken van Persoonsgegevens, en de aard daarvan, meebrengen.

3. De maatregelen zoals genoemd in lid 1 en 2 omvatten, waar passend, in ieder geval maatregelen als genoemd in artikel 32 AVG:
   a) maatregelen om Persoonsgegevens te versleutelen en te pseudonimiseren;
   b) maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van verwerkingssystemen te borgen (BIV-triade);
   c) maatregelen om de toegang tot de Persoonsgegevens tijdig te herstellen bij een fysiek of technisch incident (incident-response);
   d) maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens (toegangscontrole);
   e) maatregelen om te controleren of de geïmplementeerde technische en organisatorische maatregelen effectief genoeg zijn (evaluatie).

4. In **Bijlage 2** (Beveiligingsbijlage) zijn de maatregelen zoals bedoeld in lid 1, 2 en 3 nader omschreven.

5. Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.

6. Verwerker stelt in goed overleg de Instelling in staat om effectief te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door Verwerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 7 genoemde verplichtingen ten aanzien van Datalekken.

7. Instelling heeft te allen tijde het recht om, in overleg met Verwerker en met inachtneming van een redelijke termijn, op eigen kosten, de naleving van de in artikel 28, derde lid van de AVG neergelegde verplichtingen betreffende de Verwerking van Persoonsgegevens, de Product- en Dienstenovereenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen te (doen) controleren middels een audit uitgevoerd door een onafhankelijke gecertificeerde deskundige:
   a) Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Verwerker, in overleg met de Instelling, in te schakelen externe deskundige die een derden-verklaring (Third Party Memorandum) afgeeft.
   b) De auditor verstrekt het auditrapport alleen aan Partijen.
   c) Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
   d) Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Instelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.

Artikel 7: Datalekken

1. Verwerker heeft een passend beleid voor de omgang met Datalekken. Het beleid is nader uitgewerkt in **Bijlage 2**.

2. Indien Instelling of Verwerker een Datalek vaststelt, dan zal deze de andere Partij daarover zonder onredelijke vertraging en in ieder geval binnen 24 uur informeren zodra hij kennis heeft genomen van dat Datalek. Verwerker verstrekt ingeval van een Datalek alle relevante informatie aan Instelling met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen.

3. Verwerker stelt bij een Datalek de Instelling in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Verwerker dient hierbij aansluiting te zoeken bij de bestaande processen die Instelling daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking van de Persoonsgegevens te voorkomen of te beperken.

4. In geval het Datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Instelling de Autoriteit Persoonsgegevens informeren over het Datalek.

5. Partijen informeren elkaar onverwijld en in ieder geval binnen 24 uur 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.

6. In geval het Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Instelling de Betrokkenen informeren over het Datalek.

7. Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.

8. Partijen documenteren alle Datalekken in een (incidenten)register, met inbegrip van de feiten omtrent de inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

Artikel 8: Bijstand

1. Verwerker verleent Instelling bijstand bij het doen nakomen van de op Instelling rustende verplichtingen op grond van de AVG betreffende de Verwerking van Persoonsgegevens, zoals met betrekking, maar niet beperkt, tot:
   a) het, voor zover redelijkerwijs mogelijk, vervullen van de plicht van Instelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
   b) het uitvoeren van controles en audits zoals bedoeld in artikel 6 van deze Verwerkersovereenkomst;
   c) het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
   d) het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
   e) het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst.

2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Instelling, die verantwoordelijk is voor de afhandeling van het verzoek.

3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

Artikel 9: Bewaartermijnen en vernietiging Persoonsgegevens

1. Instelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen. Instelling is geautoriseerd de Persoonsgegevens zelfstandig te verwijderen uit de applicatie, zonder tussenkomst van de Verwerker.

2. Instelling kan de Verwerker verplichten om de in opdracht van Instelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst te (doen) vernietigen,

tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van Instelling. Instelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.

3. Verwerker zal Instelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.

Artikel 10. Aansprakelijkheid

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

      Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken Partij op grond van de geldende wet- of regelgeving ter beschikking staat.

2. Het bepaalde in lid 1 sub b geldt onverminderd het bepaalde in artikel 11 lid 2.

3. Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Autoriteit Persoonsgegevens, 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 boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij. Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Artikel 11: Tegenstrijdigheid en wijziging Verwerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.

2. Indien Partijen van de artikelen in deze Verwerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als **Bijlage 3** aan deze Verwerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de **Bijlagen 1** en **2**.

3. Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens Instelling de keuze hiertoe aanvaardt, Instelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens en de doeleinden waaronder de Persoonsgegevens worden Verwerkt. De wijzigingen zullen in **Bijlage 1** worden opgenomen.

4. Wijzigingen in de artikelen van deze Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.

5. In het geval enige bepaling van deze Verwerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Verwerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 12: Duur en beëindiging

1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.

2. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder in ieder geval artikel 4 lid 1, en de artikelen 5, 8 en 9.

3. Wijzigingen van deze overeenkomst zullen uitsluitend schriftelijk worden overeengekomen.

4. Deze Verwerkersovereenkomst maakt integraal onderdeel uit van de Product- en Dienstenovereenkomst.

5. Deze Verwerkersovereenkomst vervangt alle eerdere versies van deze overeenkomst.

Aldus overeengekomen en in tweevoud ondertekend,

Verwerker	**Instelling**
Plaats:	Plaats:
Datum:	Datum:
Naam:	Naam:
Handtekening:	Handtekening:

Bijlage 1. Privacy Bijsluiter *JEJG*

Versie 30 januari 2019

A. ALGEMENE INFORMATIE

1. Beknopte uitleg en werking product en diensten
Jij en je gezondheid (JEJG) heeft als doel om jongeren op het voortgezet onderwijs (VO) met (risico op) sociaal-medische en sociaalemotionele problemen en risicogedragingen vroeg op te sporen, te ondersteunen en indien nodig toe te leiden naar preventieprogramma's en zorg. Leerlingen vullen op school klassikaal een digitale vragenlijst in over hun gezondheid. De antwoorden zijn via de JGZ-medewerkersmodule inzichtelijk voor de jeugdarts of jeugdverpleegkundige die zorg draagt voor desbetreffende leerling. Op basis van de antwoorden wordt de leerling al dan niet uitgenodigd voor een gezondheidsconsult bij de jeugdarts of de jeugdverpleegkundige. Soms is nader onderzoek nodig omdat er nog vragen zijn over de ernst of de aard van problemen en om te zorgen dat de juiste leerlingen bij de juiste zorg terecht komen. Dit nader onderzoek kan bestaan uit een extra vragenlijst of een klinisch interview. *Jij en je gezondheid* biedt daarnaast de functionaliteit om op groepsniveau (anoniem), via het schoolgezondheidsprofiel, inzicht te geven in de gezondheidssituatie van de leerlingen op school. Op basis van dit profiel kan de school verantwoorde keuzes maken voor maatregelen om de gezondheid van leerlingen op school te bevorderen. Daarnaast kan een data-export worden gedraaid, deze data kan (na anonimiseren) gebruikt worden voor wetenschappelijk en statistisch onderzoek.

2. Links naar web applicatie:
Inlog professionals: www.jijenjegezondheid.nl/beheer
Inlog leerlingen: www.jijenjegezondheid.nl/vo
Publiekswebsite: www.jijenjegezondheidinfo.nl

3. Doelgroep:
Voortgezet onderwijs

4. Gebruikers:

Leerlingen

JGZ organisaties:
- Jeugdartsen en jeugdverpleegkundigen en assistenten
- Helpdesk-medewerkers (regionaal)
- Planners
- Data-beheerders

Verwerker:
- Helpdesk-medewerkers (centraal - Afdeling EGZ)
- Applicatie ontwikkelaars (Afdeling ITforCare)
- Technisch beheerders (Afdeling Automatisering)

5. Contactgegevens Verwerker:
GGD Amsterdam (Afdeling EGZ)
Nieuwe Achtergracht 100,
1018 WT Amsterdam
020-5555495 (secretariaat EGZ)
info@jijenjegezondheid.nl

B. OMSCHRIJVING SPECIFIEKE DIENSTEN

1. Verwerker biedt de Instelling een afgesloten omgeving binnen *JEJG,* met de naam van de regio, waarin de Instelling werkzaam is. Verwerker geeft de Instelling toegang tot de omgeving via een Helpdesk-medewerker account. Met dit account kan de Instelling zelf aan de slag om de applicatie in gebruik te nemen. Zie Handleidingen voor toelichting op de volgende diensten binnen de applicatie:
    a. Gebruikers-accounts aanmaken. Typen gebruikers:
        1. Helpdesk
        2. Arts, verpleegkundige of assistent
        3. Planner
        4. Databeheer
    b. Scholen aanmaken
    c. Oproepindicaties onderwerpen aanpassen (regio-niveau - optioneel)
    d. Onderwerpen aan/uit zetten (regio-niveau - vast)
    e. Onderwerpen aan/uit zetten (schoolniveau - optioneel)
    f. Leerlingen inlezen (optioneel)
    g. Vragenlijsten Nader Onderzoek (optioneel)
    h. Schoolgezondheidsprofielen aanmaken (optioneel)
    i. Data-exports maken voor onderzoeksdoeleinden (optioneel)

2. Instelling kan het inlezen (zo staat het nu onder 1f) van de leerlingen (zie 1f:) ook automatisch via een koppeling met het digitaal dossier Kidos laten lopen. Een koppeling met ander type digitaal dossier is ook mogelijk: Verwerker kan hiervoor de benodigde technische informatie aanleveren bij de leverancier van het digitaal dossier en zorgen dat het aan de kant van *JEJG* in orde gemaakt wordt. Het initiatief hiervoor ligt bij de Instelling.

3. Via screeningsvragenlijsten wordt de sociale veiligheid en het sociaal emotioneel welbevinden van de leerlingen gevolgd en wordt gekeken of er reden tot zorg is. De vragenlijsten voor leerlingen wordt door de leerling zelf ingevuld. Deze is zodanig beveiligd dat de leerling alleen bij de eigen lijst kan en niet bij andere gegevens in *JEJG*. De gegevens worden per leerling opgeslagen, elke leerling hangt aan een school. Op basis daarvan kunnen rapportages worden gemaakt voor intern gebruik in de school (zie 1g: het schoolgezondheidsprofiel). In het schoolgezondheidsprofiel zijn de resultaten niet herleidbaar tot individuele leerlingen.

4. Verwerker stelt bij alle onderwerpen zogenaamde ‘Gezondheidsboodschappen’ op: uitslagteksten met informatie, tips en handige links die de leerlingen direct na invullen te zien krijgen. Aan iedere verkleuring binnen een onderwerp hangt een op maat geschreven tekst, welke jaarlijks worden herzien door zowel inhoudelijke- als communicatie-experts binnen de organisatie van de Verwerker. Instelling neemt bij ingang van de overeenkomst automatisch de door de Verwerker opgestelde teksten over. Deze kunnen voor de Instelling op aanvraag worden aangepast voor de eigen omgeving.

5. Om de Instelling te ondersteunen heeft de Verwerker toegang tot de applicatie. Vanuit de ambtseed van de Verwerker hebben alle medewerkers een geheimhoudingsplicht.

C. DOELEINDEN VOOR HET VERWERKEN VAN GEGEVENS

1. Het toegang krijgen tot en in gebruik kunnen nemen van *JEJG*.

2. Analyse en interpretatie van de resultaten van leerlingen die de JEJG screeningsvragenlijst hebben ingevuld.

3. Het monitoren van de sociaal emotionele ontwikkeling en sociale veiligheid op zowel leerling-, school- als regioniveau.

4. Continuïteit en goede werking van *JEJG* volgens de Product- en dienstenovereenkomst. Hieronder valt het oplossen van problemen (mits niet op te lossen door de Instelling), de centrale? helpdeskfunctie en het oplossen van geconstateerde fouten.

5. Organisatie van de afnames.

D. VERWERKINGEN VAN (CATEGORIEËN VAN) PERSOONSGEGEVENS

Leerlingen	
Persoonsgegeven	**BSN nummer**
Verwerkingen	Door BSN nummer zijn leerlingen identificeerbaar. Om uit te sluiten dat uitslagen en gegevens aan een verkeerd individu gekoppeld worden, wordt idealiter gewerkt met BSN nummer.
Persoonsgegeven	**Dossiernummer (nummer uit digitaal dossier)**
Verwerkingen	Indien BSN ontbreekt, kan het dossiernummer leerlingen identificeren.
Persoonsgegeven	**Voornaam en achternaam**
Verwerkingen	Indien BSN en dossiernummer ontbreekt, kan de voornaam en achternaam (in combinatie met geboortedatum en geslacht) leerlingen identificeren.
Persoonsgegeven	**Geboortedatum**
Verwerkingen	Uitslagen naar aanleiding van de gezondheidsvragenlijst worden (mede) bepaald op basis van de leeftijd van de leerling. Indien BSN en dossiernummer ontbreekt, kan de geboortedatum (in combinatie met voornaam, achternaam en geslacht) leerlingen identificeren.
Persoonsgegeven	**Geslacht**
Verwerkingen	Uitslagen naar aanleiding van de gezondheidsvragenlijst worden (mede) bepaald op basis van het geslacht van de leerling. Indien BSN en dossiernummer ontbreekt, kan het geslacht (in combinatie met voornaam, achternaam en geboortedatum) leerlingen identificeren.
Persoonsgegeven	**Naam school**
Verwerkingen	De naam van de school is nodig om het schoolgezondheidsprofiel te voorzien van de juiste naam. Daarnaast is de schoolnaam handig voor de jeugdartsen en -verpleegkundigen om leerlingen op te zoeken in de JGZ-medewerkersmodule.
Persoonsgegeven	**BRIN-nummer school**
Verwerkingen	Het BRIN-nummer van de school(locatie) is uniek en nodig zodat leerlingen via dit nummer aan de juiste school(locatie) gekoppeld

	kunnen worden.
Persoonsgegeven	**Schooljaar**
Verwerkingen	Het schooljaar is nodig om het klassenoverzicht in de JGZ-medewerkersmodule te genereren. Daarnaast is het handig voor de jeugdartsen en -verpleegkundigen om leerlingen op te zoeken in de JGZ-medewerkersmodule. Het schooljaar is nodig om het schoolgezondheidsprofiel per schooljaar te kunnen uitdraaien.
Persoonsgegeven	**Leerjaar**
Verwerkingen	Het leerjaar is nodig om de resultaten binnen het schoolgezondheidsprofiel per leerjaar te presenteren (uitgangspunt gezonde school) en voor het planproces van de afnames.
Persoonsgegeven	**Opleidingsniveau**
Verwerkingen	Het opleidingsniveau is nodig om de resultaten binnen het schoolgezondheidsprofiel naar opleidingsniveau te presenteren.
Persoonsgegeven	**Administratieve groep (leerjaar en opleidingsniveau)**
Verwerkingen	De administratieve groep kan gebruikt worden om informatie over leerjaar en opleidingsniveau van de leerling in de applicatie op te nemen (gebruikmakend van een vertaaltabel). Beide zijn nodig om de resultaten van de leerling mee te nemen in het schoolgezondheidsprofiel.
Persoonsgegeven	**Klas**
Verwerkingen	De klas is nodig om het klassenoverzicht in de JGZ-medewerkersmodule te genereren. Daarnaast is het handig voor de jeugdartsen en -verpleegkundigen om leerlingen op te zoeken in de JGZ-medewerkersmodule.
Persoonsgegeven	**Postcode**
Verwerkingen	De postcode is nodig om bij data-analyses onderscheid te kunnen maken tussen verschillende gemeenten of stadsdelen. Dit is noodzakelijk voor beleidsdoeleinden.
Persoonsgegeven	**Gezondheid van de leerling**
Verwerkingen	Deze gegevens worden uitsluitend verwerkt voor het doel waarvoor ze worden verzameld: vroegsignalering van problemen en waar nodig passende zorg voor VO-leerlingen en MBO-studenten. En daarnaast wordt geanonimiseerde data gebruikt voor het schoolgezondheidsprofiel en statistisch onderzoek.
Persoonsgegeven	**E-mailadres**
Verwerkingen	Het e-mailadres is nodig om de resultaten naar de leerling op te sturen. Aan het eind van de vragenlijst, op de pagina waar de resultaten getoond worden, kunnen leerlingen optioneel hun e-mailadres invullen. Leerlingen ontvangen dan een mail met een link naar hun resultaten , ze kunnen ze met hun geboortedatum inloggen.
Persoonsgegeven	**06-nummer**
Verwerkingen	Het 06-nummer is een manier voor de arts of verpleegkundige om contact te leggen met de leerling, wanneer een consult gewenst is. Andere manieren zijn bv. de leerling uit de klas te halen.

Jeugdartsen en jeugdverpleegkundigen	
Persoonsgegeven	**Voornaam en achternaam**
Verwerkingen	De naam wordt gebruikt voor de juiste werking van het product *Jij en je gezondheid* en het genereren van gebruikersaccounts. *Jij en je gezondheid* bevat een gebruikersadministratie waarin jeugdartsen en -verpleegkundigen op basis van naam identificeerbaar moeten zijn.
Persoonsgegeven	**06-nummer**
Verwerkingen	Het 06-nummer wordt gebruikt voor de tweede factor beveiliging. Inloggen in de applicatie *Jij en je gezondheid* is uitsluitend mogelijk na invoeren van de pincode die gebruikers via hun 06-nummer ontvangen na het invoeren van hun inlogcode en wachtwoord.
Persoonsgegeven	**Naam school**
Verwerkingen	De naam van de school waar jeugdartsen en –verpleegkundigen werkzaam zijn is nodig omdat jeugdartsen en –verpleegkundigen uitsluitend toegang krijgen tot de scholen en leerlingen waarvoor zij zorg dragen.
Persoonsgegeven	**E-mailadres**
Verwerkingen	Het e-mailadres kan in theorie nodig zijn om de gebruiker notificaties te sturen. Om deze reden is dit veld bij de ontwikkeling van de applicatie opgenomen. Deze functionaliteit is echter niet in gebruik; invullen is optioneel. Mocht hier in de toekomst gebruik van gemaakt worden door de Verwerker, zal de gebruiker eerst om toestemming gevraagd worden.

Helpdesk-medewerkers (regionaal); Planners; Databeheerders; Helpdesk-medewerkers (centraal – afdeling EGZ); Applicatie ontwikkelaars (afdeling ITforCare); Technisch beheerders (afdeling Automatisering)	
Persoonsgegeven	**Voornaam en achternaam**
Verwerkingen	De naam wordt gebruikt voor de juiste werking van het product *Jij en je gezondheid* en het genereren van gebruikersaccounts. *Jij en je gezondheid* bevat een gebruikersadministratie waarin medewerkers met een helpdeskfunctie op basis van naam identificeerbaar moeten zijn.
Persoonsgegeven	**06-nummer**
Verwerkingen	Het 06-nummer wordt gebruikt voor de tweede factor beveiliging. Inloggen in de applicatie *Jij en je gezondheid* is uitsluitend mogelijk na invoeren van de pincode die gebruikers via hun 06-nummer ontvangen na het invoeren van hun inlogcode en wachtwoord.
Persoonsgegeven	**E-mailadres**
Verwerkingen	Het e-mailadres kan in theorie nodig zijn om de gebruiker notificaties te sturen. Om deze reden is dit veld bij de ontwikkeling van de applicatie opgenomen. Deze functionaliteit is echter niet in gebruik; invullen is optioneel. Mocht hier in de toekomst gebruik van gemaakt worden door de Verwerker, zal de gebruiker eerst om toestemming gevraagd worden.

Bijlage 2. Beveiligingsbijlage *JEJG*

Versie 30 januari 2019

A. OVERZICHT BEVEILIGINGSMAATREGELEN

1. Maatregelen om Persoonsgegevens te versleutelen en te pseudonimiseren:

Alle gebruikers-typen hebben toegang tot de Persoonsgegevens van de leerlingen in het systeem, m.u.v. de resultaten van de vragenlijst. Hier hebben alleen de artsen en verpleegkundigen toegang toe (incl. de databeheerder, die arts of verpleegkundige moet zijn). Alle gebruikerstypen hebben de Persoonsgegevens namelijk nodig om hun werk goed uit te kunnen voeren.

2. Maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van verwerkingssystemen te borgen (BIV-triade):
De beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van JEJG wordt jaarlijks geclassificeerd volgens het Certificeringsschema informatiebeveiliging en privacy ROSA. Op basis hiervan wordt het gewenste niveau van beveiliging bepaald.

In verband met vertrouwelijkheid zijn de resultaten van de jaarlijkse BIV-triade op verzoek in te zien op kantoor van de Verwerker.

3. Maatregelen om de toegang tot de Persoonsgegevens tijdig te herstellen bij een fysiek of technisch incident (incident-response):

Zie de Service Level Agreement (SLA) die als bijlage bij de Product- en dienstenovereenkomst is toegevoegd.

4. Maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens (toegangscontrole):

Het platform waarop de web applicatie draait wordt intern gehost bij de Verwerker. De toegang tot de server waar de applicatie op draait is gelimiteerd tot technisch beheerders (afdeling Automatisering) en applicatie beheerders/ontwikkelaars (afdeling ITforCare) van de Verwerker. De applicatie beheerders/ontwikkelaars hebben gelimiteerde toegang ter diagnose.

De eerste toegang tot de web applicatie kan alleen toegekend worden door een helpdeskmedewerker van de Verwerker. Meestal is dit voor de projectleider en Helpdesk-medewerker van de Instelling. Hierbij wordt een account aangemaakt met persoonlijke gebruikersnaam en wachtwoord. Zij kunnen vervolgens een persoonlijk wachtwoord aanmaken. Alle wachtwoorden worden opgeslagen met een niet herleidbare cryptografische hash. Mocht een hacker ooit binnen komen dan kan hij geen wachtwoorden achterhalen van gebruikers.

Er wordt gewerkt met een tweede factor beveiliging via het 06-nummer. Inloggen in de applicatie is uitsluitend mogelijk na invoeren van de pincode die de gebruikers via hun 06-nummer ontvangen na het invoeren van hun inlogcode en wachtwoord.

De applicatie werkt met een rechten systeem met gebruikerstypen en bijbehorende rechten. Deze rechten werken op niveau van type data en bewerkingsmogelijkheden. De Instelling is verantwoordelijk voor de toekenning van de typen aan de medewerkers. Alle activiteiten binnen de web applicatie en op de server worden gelogd op individueel niveau. In Tabel 1 (eind van dit document) staan de rechten naar gebruikerstype weergegeven.

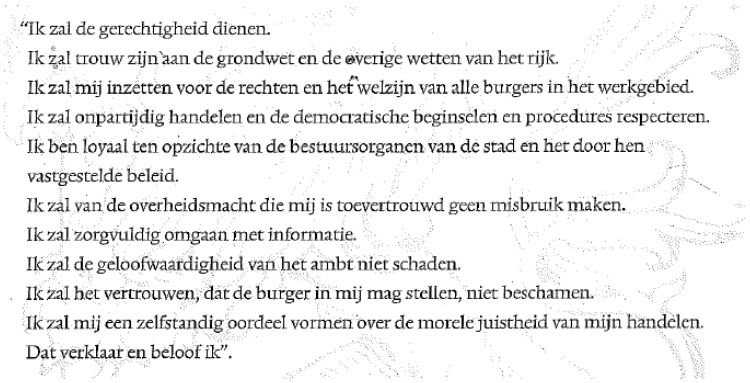
5. Maatregelen om te controleren of de geïmplementeerde technische en organisatorische maatregelen effectief genoeg zijn (evaluatie):

De Automatiserings- en IT afdeling van de Verwerker worden elke 3 jaar onderworpen aan een audit voor de ISO 27001 Informatiebeveiliging certificering door een externe partij. Daarnaast voert ITforCare intern periodieke beveiligingstesten uit met behulp van Qualys, en externe penetratietesten (door een onafhankelijke partij). Maatregelen die voortkomen uit deze beveiligingstesten worden zo snel en secuur mogelijk doorgevoerd.

Verwerker voert jaarlijks een data protection impact assessment (DPIA) uit naar de privacy risico's van *JEJG.* Bij deze DPIA zijn een juridisch beleidsadviseur en de coördinator informatiebeveiliging van de Verwerker betrokken. In verband met vertrouwelijkheid zijn de resultaten van de jaarlijkse DPIA op verzoek in te zien op kantoor van de Verwerker.

6. Overige maatregelen:

Geheimhoudingsplicht
Alle medewerkers van de GGD leggen een ambtseed af waarin zij het volgende verklaren en ondertekenen:


"Ik zal de gerechtigheid dienen.
Ik zal trouw zijn aan de grondwet en de overige wetten van het rijk.
Ik zal mij inzetten voor de rechten en het welzijn van alle burgers in het werkgebied.
Ik zal onpartijdig handelen en de democratische beginselen en procedures respecteren.
Ik ben loyaal ten opzichte van de bestuursorganen van de stad en het door hen vastgestelde beleid.
Ik zal van de overheidsmacht die mij is toevertrouwd geen misbruik maken.
Ik zal zorgvuldig omgaan met informatie.
Ik zal de geloofwaardigheid van het ambt niet schaden.
Ik zal het vertrouwen, dat de burger in mij mag stellen, niet beschamen.
Ik zal mij een zelfstandig oordeel vormen over de morele juistheid van mijn handelen.
Dat verklaar en beloof ik".

Maatregelen om de anonimiteit van de gegevens ten behoeve van wetenschappelijk en statistisch onderzoek te waarborgen:
Gegevens die gebruikt worden voor onderzoek zijn anoniem en dus niet tot de persoon herleidbaar. Verwerker volgt de richtlijnen zoals vastgelegd in de Gedragscode Gezondheidsonderzoek.

B. BELEID BIJ DATALEKKEN (INCIDENTRESPONS PROTOCOL)

1. Identificeren van een beveiligingsincident (Datalek)

Indien zich binnen de organisatie van de Instelling of de Verwerker een inbreuk op de beveiliging voordoet, zal de ene Partij dit direct melden bij de andere Partij. De Verwerker (afdeling EGZ) maakt direct een melding van het beveiligingsincident in TOPdesk. De melding wordt per email en sms direct doorgezet naar de Technical Security Officer (TSO).

2. Beoordelen aard/ernst van het beveiligingsincident (Is het een Datalek?)

Door de Verwerker (i.e. TSO en afdeling Automatisering) wordt, in ieder geval, de volgende informatie verzameld:

a. datum en tijd van het incident;
b. frequentie van incident;
c. de betrokken systemen en eventueel IP-adressen;
d. URL's die erbij betrokken zijn;
e. de foutmeldingen;
f. eventuele logfiles

Op basis van de verzamelde informatie beoordeelt de Verwerker (i.e. TSO en afdeling Automatisering) zo spoedig mogelijk of er daadwerkelijk sprake is van een Datalek. In geval dat het beveiligingsincident heeft geleid tot (een aanzienlijke kans op) verlies of onrechtmatige Verwerking van Persoonsgegevens is er sprake van een Datalek (artikel 33 lid 1 AVG).

In geval van een Datalek beoordeelt de Verwerker (i.e. TSO, afdeling Automatisering en afdeling ITforCare) of er per direct maatregelen genomen moeten worden om schade te beperken, waaronder het doen van een (voorlopige) melding aan Betrokkene(n).

De verzamelde informatie en de daaruit getrokken conclusies worden door de Verwerker (afdeling EGZ) schriftelijk of digitaal gedeeld met de Instelling.

3. Melden van het Datalek aan de Autoriteit Persoonsgegevens (AP)

De Instelling meldt het Datalek, zonder onredelijke vertraging en binnen 72 uur, bij de AP, tenzij het Datalek geen *risico* voor de rechten en vrijheden van Betrokkene(n) met zich meebrengt (artikel 33 lid 1 AVG). Als een Datalek geen inbreuk op de privacy oplevert, hoeft het dus niet gemeld te worden.

Op de website van de AP (www.autoriteitpersoonsgegevens.nl) is voor de melding een web formulier beschikbaar gesteld. Via dit web formulier kan de melding indien nodig aangevuld of ingetrokken worden.

In de melding wordt ten minste het volgende omschreven of meegedeeld:

a. de aard van de inbreuk in verband met Persoonsgegevens, waar mogelijk onder vermelding van de categorieën van Betrokkenen en registers van Persoonsgegevens in kwestie en, bij benadering, het aantal Betrokkenen;
b. de naam en de contactgegevens van de Verwerker (TSO) waar meer informatie kan worden verkregen;
c. de waarschijnlijke gevolgen van de inbreuk in verband met Persoonsgegevens;

d. de maatregelen die de Instelling, als Verwerkingsverantwoordelijke, heeft voorgesteld of genomen om de inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

4. Melden van het Datalek aan Betrokkene(n)

Indien een Datalek is gemeld aan de AP dient tevens vastgesteld te worden of het Datalek door de Instelling ook moet worden gemeld aan Betrokkene(n). De Instelling meldt het Datalek bij Betrokkene(n), indien het Datalek een *hoog risico* voor de rechten en vrijheden van Betrokkene(n) inhoudt (artikel 34 lid 1 AVG).

Voor de beantwoording van deze vraag heeft de Artikel 29-werkgroep negen criteria opgesteld (*noot 1*). De werkgroep gaat ervan uit dat er sprake is van een hoog risico indien minstens twee van de negen criteria van toepassing zijn. Voor *JEJG* zijn zes criteria relevant:

- Evaluatie of scoretoekenning (criterium 1);
- Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg (criterium 2);
- Stelselmatige monitoring (criterium 3);
- Gevoelige gegevens of gegevens van zeer persoonlijke aard (criterium 4);
- Op grote schaal Verwerkte gegevens (criterium 5);
- Gegevens met betrekking tot kwetsbare Betrokkenen (criterium 7).

In andere bewoording, er kan in principe van uit gegaan worden dat het Datalek niet alleen gemeld moet worden aan de AP, maar ook aan de Betrokkene(n).

Deze melding kan achterwege blijven indien (artikel 34 lid 3 AVG): a) de Persoonsgegevens versleuteld zijn en niet toegankelijk voor Derden en er inmiddels maatregelen getroffen zijn die het hoge risico hebben weggenomen, en b) de melding een onevenredige inspanning vergt. In dit laatste geval kan worden volstaan met een openbare mededeling.

In de melding wordt in duidelijke en eenvoudige taal ten minste de aard van de inbreuk in verband met Persoonsgegevens omschreven, alsmede de gegevens en maatregelen zoals genoemd bij b, c en d onder punt 3.

5. Melden aan de gemeente Amsterdam

Ernstige datalekken worden door de Verwerker (TSO) gemeld bij de gemeente Amsterdam. Intern wordt de directeur van de Verwerker op de hoogte gebracht. De Coördinator Privacy en Informatiebeveiliging (PIB) van de afdeling Informatievoorziening (Cluster Sociaal) van de gemeente Amsterdam wordt in deze gevallen bij de vervolgstappen betrokken.

6. Verrichten van Datalek onderzoek

De Verwerker (i.e. TSO en afdeling Automatisering) doet nader onderzoek naar de feitelijk toedracht van het beveiligingsincident en hoe dergelijke incidenten in de toekomst kunnen worden voorkomen.

De verzamelde informatie en de daaruit getrokken conclusies worden door de Verwerker (afdeling EGZ) schriftelijk of digitaal gedeeld met de Instelling.

De Instelling maakt, indien nodig, een definitieve melding aan de AP en de Betrokkene(n).

7. Nemen van corrigerende maatregelen

De manager in wiens domein de corrigerende maatregelen liggen is ervoor verantwoordelijk dat deze worden geïmplementeerd. Ook zorgt hij dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering. De Verwerker (i.e. TSO en afdeling Automatisering) bewaakt de voortgang van de corrigerende maatregelen.

De genomen corrigerende maatregelen worden door de Verwerker (afdeling EGZ) schriftelijk of digitaal gedeeld met de Instelling.

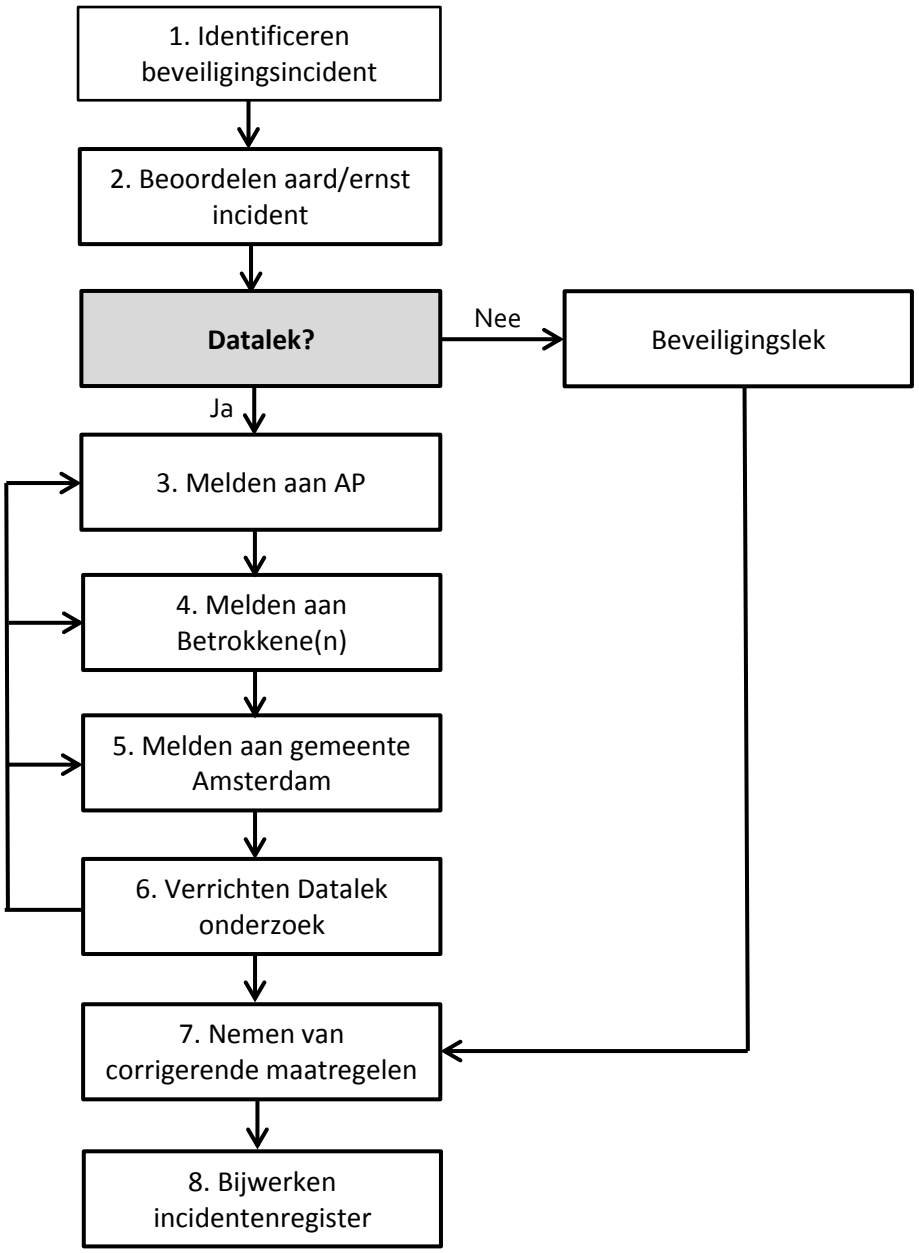
8. Bijwerken van het incidentenregister

De Instelling, alsook de Verwerker, documenteert elke inbreuk op de beveiliging, ongeacht of deze wordt gemeld bij de AP, met inbegrip van de feiten omtrent de inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen (artikel 34 lid 4 AVG). Daarnaast wordt in het register opgenomen of het Datalek is gemeld bij de AP en de Betrokkene(n).

De verzamelde informatie en de genomen corrigerende maatregelen worden door de Verwerker (i.e. TSO en afdeling Automatisering) ingevoerd in TOPdesk.

Noot 1: Groep Gegevensbescherming Artikel 29. Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679. Brussel: Europese Commissie, Directoraal-generaal Jusititie en Consumenten Zaken (JUST), 2017.

Activiteitenflow



Tabel 1. Rechten naar gebruiker

Rechten \ Type gebruiker	Verwerker (beheer+)	Helpdesk	Arts, VPK of assistent	Planner	Data beheerder[1]
Vragenlijsten					
Vragenlijst toevoegen	Ja	Nee	Nee	Nee	Nee
Vragenlijst wijzigen	Ja	Nee	Nee	Nee	Nee
Afkappunten toevoegen	Ja	Nee	Nee	Nee	Nee
Afkappunten wijzigen	Ja	Nee	Nee	Nee	Nee
Gezondheidsboodschappen toevoegen	Ja	Nee	Nee	Nee	Nee
Gezondheidsboodschappen wijzigen	Ja	Nee	Nee	Nee	Nee
Indicatie voor oproepen wijzigen	Ja	Ja	Nee	Nee	Nee
Algemene schoolgegevens					
Nieuwe school invoeren	Ja	Ja	Nee	Ja	Nee
School verwijderen	Ja	Ja	Nee	Ja	Nee
Gegevens school wijzigen	Ja	Ja	Nee	Ja	Nee
Algemene klasgegevens					
Nieuwe klas invoeren	Ja	Ja	Nee	Ja	Nee
Klas verwijderen	Ja	Ja	Nee	Ja	Nee
Gegevens klas wijzigen	Ja	Ja	Ja	Ja	Nee
Algemene leerlinggegevens					
Reservecodes aanmaken	Ja	Ja	Ja	Ja	Nee
Nieuwe leerling invoeren	Ja	Ja	Ja	Ja	Nee
Leerling verwijderen	Ja	Ja	Nee	Nee	Nee
Gegevens leerling wijzigen	Ja	Ja	Ja	Ja	Nee
Leerlingvragenlijst					
Inlogkaartjes uitprinten	Ja	Ja	Ja	Ja	Nee
Uitslagen inzien	Ja	Nee	Ja	Nee	Nee
Bezwaar invullen	Ja	Ja	Ja	Ja	Nee
Leerlingvragenlijst resetten[2]	Ja	Ja	Nee	Nee	Nee

[1] Dit moet i.v.m. privacy een arts, verpleegkundige, assistent, of iemand anders die onder de jeugdgezondheidszorg organisatie van de regio valt.
[2] Verwijderen van alle antwoorden en uitslagen: alle ingelezen gegevens blijven bewaard.

Rechten \ Type gebruiker	Verwerker (beheer+)	Helpdesk	Arts, VPK of assistent	Planner	Data beheerder[3]
Vragenlijst voor nader onderzoek					
Starten	Ja	Ja	Ja	Nee	Nee
E-mailen	Ja	Ja	Ja	Nee	Nee
Uitslagen inzien	Ja	Ja	Ja	Nee	Nee
Overig					
Inlezen leerlingen	Ja	Ja	Nee	Ja	Nee
Nieuws in *Jij en Je Gezondheid*	Ja	Nee	Nee	Nee	Nee
Landenlijst aanpassen	Ja	Nee	Nee	Nee	Nee
Onderdelen in leerlingvragenlijst uitsluiten/aanzetten	Ja	Ja	Ja	Nee	Nee
Aanmaken schoolgezondheidsprofiel	Ja	Ja	Ja	Ja	Nee
Exporteren databestand	Ja	Nee	Nee	Nee	Ja
Alle leerlingen van een schooljaar verwijderen	Ja	Nee	Nee	Nee	Ja
Aanmaken, wijzigen of verwijderen JGZ-medewerker	Ja	Ja	Nee	Nee	Nee
Toekennen autorisaties	Ja	Ja	Nee	Nee	Nee
Inloghistorie bekijken	Ja	Ja	Nee	Nee	Nee

[3] Dit moet i.v.m. privacy een arts, verpleegkundige, assistent, of iemand anders die onder de jeugdgezondheidszorg organisatie van de regio valt.