Privacy Impact Assessment

Jij en Je Gezondheid PO

	Vraag	Ja/Nee	Actie	Toelichting
1	**Het type project**			
1.1	Is er sprake van het verwerken van persoonsgegevens?	Ja	Ja: Ga verder. Nee: U kunt stoppen.	
1.2	Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?	Ja	Ja: Ga verder. Nee: Leg vast voor en door wie het project wordt uitgevoerd, wie formeel verantwoordelijk is voor de verwerking van persoonsgegevens en wie de intern contactpersoon is.	JEJG wordt door de afdeling Jeugdgezondheidszorg van de GGD Amsterdam gebruikt bij het bieden van verantwoorde zorg aan kinderen en ouders. Het college van burgemeesters en wethouders Amsterdam is formeel verantwoordelijk voor de verwerking van de persoonsgegevens. Intern contactpersoon: afdelingshoofd Jeugdgezondheidszorg.
1.3	Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: treedt uw organisatie op als verwerker?	Ja	Ja: U kunt stoppen of de PIA vervolgen om beter inzicht te krijgen in de privacy risico's (in de rol van verwerker). Nee: Bepaal wie (bedrijfsonderdeel, persoon) binnen uw organisatie de verantwoordelijke is.	GGD Amsterdam treedt op als verwerker voor andere Instellingen die gebruik maken van JEJG. GGD Amsterdam is verantwoordelijk voor de persoonsgegevens van de regio Amsterdam/Amstelland.

	Privacy Impact Assessment			
1.4	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?	Ja	Ja: Ga verder. Nee: Bepaal wie verantwoordelijk is voor de jaarlijkse uitvoering van de PIA en wie verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen.	De EGZ projectleider van JEJG is verantwoordelijk voor de jaarlijkse uitvoering van de PIA. De betrokken afdelingen (automatisering, EGZ, ITforCare en JGZ) zijn verantwoordelijk voor het in stand houden en realiseren van de maatregelen van hun afdeling.

				Specifiek: Kinderen op het primair onderwijs met (risico op) sociaalmedische en sociaalemotionele problemen en risicogedragingen vroeg opsporen, ondersteunen en zonodig toeleiden naar preventieprogramma's en zorg. Daarnaast door middel van wetenschappelijk statistisch onderzoek de zorg ten behoeve van kinderen te verbeteren. Meetbaar: Aantal ingevulde vragenlijsten door ouders van de beoogde doelgroep. Acceptabel: Vroegsignalering en toeleiding naar hulp is een wettelijke taak vanuit de WPG (bijlage 1, artikel 5) en BPG (bijlage 2, artikelen 3 t/m 6). Wetenschappelijk statistisch onderzoek is een taak vanuit de WPG (bijlage 1, artikel 2) en BPG (bijlage 2, artikel 8). Realistisch: Doelstelling is haalbaar. Ongeveer 65 procent van de ouders vult de JEJG vragenlijst in voor hun kind. Wanneer ouders geen vragenlijst invullen verzamelt JGZ via andere kanalen (digitaal dossier, school en screening) informatie die gebruikt wordt als input voor verdere invulling van het contactmoment. Tijdgebonden: Elk schooljaar vullen de ouders van 5- en 10-jarigen kinderen JEJG in. Kinderen ontvangen waar nodig passende zorg. Gedurende het schooljaar wordt JEJG mogelijk op indicatie ingezet bij kinderen van andere leeftijden die risicovol gedrag vertonen. De gecodeerd anonieme gegevens worden gebruikt voor wetenschappelijk statistisch onderzoek en voor monitoring en advisering (WPG).
1.5	Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?	Ja	Ja: Ga verder. Nee: Omschrijf het doel van de verwerking van persoonsgegevens voldoende SMART.	

1.6 Is er sprake van:

Privacy Impact Assessment

A	Gebruik van een nieuwe technologie?	Ja	Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen. Nee: Ga verder.	Eerder werden in dezelfde context papieren vragenlijsten gebruikt waarbij ouders de persoonsgegevens van het kind op de papieren vragenlijst invulden. Vanaf nu worden de persoonsgegevens uit het digitaal dossier ingelezen in de applicatie van JEJG. De applicatie van JEJG draait in een beveiligde omgeving. Uitsluitend JGZ-professionals die zorg dragen voor desbetreffend kind hebben toegang tot de persoonsgegevens. Daarnaast hebben de applicatie-ontwikkelaars en functioneel beheerders toegang tot persoonsgegevens om hun rol te kunnen vervullen. Voor JGZ professionals is een FAQ opgesteld waarmee zij veel gestelde vragen goed kunnen beantwoorden.
B	Gebruik van technologie die bij het publiek weerstand of vragen kan oproepen (bijvoorbeeld biometrie, RFID of behavioural targeting)?	Ja	Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen. Nee: Ga verder.	Ouders kunnen weerstand hebben tegen het gebruik van niet-anonieme gezondheidsvragenlijsten voor een pro-actieve screening. Zij kunnen zich afvragen wat er met de gegevens gebeurt. Hierom wordt op de publiekswebsite, in de brieven en de folders zo goed mogelijk uitleg gegeven over het doel en de werkwijze van JEJG en wat er met de gezondheidsvragenlijsten gebeurt.
C	De invoering van bestaande technologie in een nieuwe context?	Nee	Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen. Nee: Ga verder.	Er is sprake van een nieuwe technologie in een bestaande context.

D	**(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?**	**Ja**	**Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen.** **Nee: Ga verder.**	**Kindgegevens worden nu samen met de uitslagen op itemniveau van de oudervragenlijst in één systeem opgeslagen. Om uit te sluiten dat uitslagen en gegevens verkeerd gekoppeld worden, wordt gewerkt met het BSN-nummer. Alle betrokken jeugdartsen en -verpleegkundigen hebben uitsluitend toegang tot hun eigen scholen en kinderen. Elke jeugdarts en -verpleegkundige ontvangt unieke inloggegevens die alleen door de lokale helpdesk gegenereerd kunnen worden. Bij inloggen wordt gewerkt met een 2e factor beveiliging. Als een jeugdarts of -verpleegkundige geen toegang heeft tot de kindgegevens in JEJG omdat zij niet aan de school gekoppeld is, belt hij of zij met de JEJG helpdesk en wordt hij of zij gekoppeld. Om zeker te weten dat de jeugdarts of -verpleegkundige inderdaad is verbonden aan de school, checkt de helpdesk dit bij de JGZ teamleider.**
E	Een nieuwe verwerking van persoonsgegevens?	Nee	Ja: Doe een compliance check. Nee: Ga verder .	Gegevens worden uitsluitend verwerkt voor het doel waarvoor ze worden verzameld: vroegsignalering en passende zorg voor PO-leerlingen. In lijn met de WPG (bijlage 1). Dit wijkt niet af van de voorgaande werkwijze en betreft dus een bestaande verwerking.
F	Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen?	Ja	Ja: Doe een compliance check. Nee: Ga verder.	In vergelijking met de papieren vragenlijst worden meer gezondheidsthema's nagevraagd en wordt nu gewerkt met digitale screeningslijsten. De gebruikte screeningslijsten zijn in lijn met de BPG (artikelen 3, 5 en 7) en de JGZ-richtlijnen.
G	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken?	Nee	Ja: Doe een compliance check. Nee: Ga verder.	Verzamelen van nieuwe gegevens voor een bestaand doel en volgens een bestaande werkwijze.
1.7	Heeft u op alle bovenstaande (A t/m G) 'nee' geantwoord?	Nee	Ja: U kunt stoppen. Nee: Ga verder.	

D	**(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?**	**Ja**	**Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen.** **Nee: Ga verder.**	**Kindgegevens worden nu samen met de uitslagen op itemniveau van de oudervragenlijst in één systeem opgeslagen. Om uit te sluiten dat uitslagen en gegevens verkeerd gekoppeld worden, wordt gewerkt met het BSN-nummer. Alle betrokken jeugdartsen en -verpleegkundigen hebben uitsluitend toegang tot hun eigen scholen en kinderen. Elke jeugdarts en -verpleegkundige ontvangt unieke inloggegevens die alleen door de lokale helpdesk gegenereerd kunnen worden. Bij inloggen wordt gewerkt met een 2e factor beveiliging. Als een jeugdarts of -verpleegkundige geen toegang heeft tot de kindgegevens in JEJG omdat zij niet aan de school gekoppeld is, belt hij of zij met de JEJG helpdesk en wordt hij of zij gekoppeld. Om zeker te weten dat de jeugdarts of -verpleegkundige inderdaad is verbonden aan de school, checkt de helpdesk dit bij de JGZ teamleider.**
1.8	Is er (naast de AVG) veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?	Ja	Ja: Breng de van toepassing zijnde wet- en regelgeving in kaart en maak de (privacy) consequenties inzichtelijk. Nee: Ga verder.	WGBO (bijlage 4), Wet BIG (bijlage 5) en de eerder genoemde WPG (bijlage 1) en BPG (bijlage 2).
1.9	Zijn er veel maatschappelijke belanghebbenden?	Ja	Ja: Maak een lijst van maatschappelijk belanghebbenden en een plan hoe deze actief geïnformeerd of betrokken worden. Nee: Ga verder.	Ouders, kinderen, scholen, medewerkers JGZ, wijkteams, preventie- en zorgpartners, GGD-en, onderzoeksinstellingen en kennisinstituten, wetenschappelijke verenigingen, beroepsverenigingen en bestuurlijke organen. Deze belanghebbenden kunnen relevante informatie rondom JEJG vinden op de openbare publiekswebsite. Informatievoorziening rondom de invulling van de JGZ contactmomenten (waar binnen JEJG wordt afgenomen) ligt de JGZ organisaties zelf.

D	**(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?**	**Ja**	**Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen.** **Nee: Ga verder.**	**Kindgegevens worden nu samen met de uitslagen op itemniveau van de oudervragenlijst in één systeem opgeslagen. Om uit te sluiten dat uitslagen en gegevens verkeerd gekoppeld worden, wordt gewerkt met het BSN-nummer. Alle betrokken jeugdartsen en -verpleegkundigen hebben uitsluitend toegang tot hun eigen scholen en kinderen. Elke jeugdarts en -verpleegkundige ontvangt unieke inloggegevens die alleen door de lokale helpdesk gegenereerd kunnen worden. Bij inloggen wordt gewerkt met een 2e factor beveiliging. Als een jeugdarts of -verpleegkundige geen toegang heeft tot de kindgegevens in JEJG omdat zij niet aan de school gekoppeld is, belt hij of zij met de JEJG helpdesk en wordt hij of zij gekoppeld. Om zeker te weten dat de jeugdarts of -verpleegkundige inderdaad is verbonden aan de school, checkt de helpdesk dit bij de JGZ teamleider.**
1.10	Zijn er veel partijen betrokken bij de uitvoering van het project?	Nee	Ja: Verifieer of alle partijen zorgvuldig met de gegevens omgaan die tijdens het project worden verzameld. Nee: Ga verder.	Betrokken partijen van de GGD Amsterdam zijn JGZ, EGZ en automatisering. Vanuit het cluster sociaal gemeente Amsterdam is ITforCare betrokken. Andere partijen hebben geen rol bij het zorgvuldig omgaan met gegevens die tijdens de uitvoering van JEJG in Amsterdam en Amstelland worden verzameld. Andere JGZ organisaties verzorgen hun eigen PIA en maatregelen om risico's te vermijden.
1.11	Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?	Ja	Ja: Ga verder. Nee: Wijs een contactpunt voor vragen en klachten aan en sluit waar mogelijk aan bij een geschillenregeling.	Alle deelnemende JGZ-organisaties hebben een klachtencommissie. Betrokkenen kunnen hier terecht met klachten. Indien klachten specifiek gelinkt zijn aan JEJG kan de JGZ-organisatie contact opnemen met JEJG.
2	**De gegevens**			
2.1	Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?	Ja	Ja: Ga verder. Nee: Zorg dat zo min mogelijk gegevens verzameld worden.	Alle gegevens zijn nodig voor vroegsignalering en vroeghulp bij sociaal-emotionele en sociaal-medische problemen bij kinderen van het (S)PO. Daarnaast worden de gegevens gebruikt voor de monitoring en advisering en wetenschappelijk statistisch onderzoek (WPG, bijlage 1).

D	**(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?**	**Ja**	**Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen.** **Nee: Ga verder.**	**Kindgegevens worden nu samen met de uitslagen op itemniveau van de oudervragenlijst in één systeem opgeslagen. Om uit te sluiten dat uitslagen en gegevens verkeerd gekoppeld worden, wordt gewerkt met het BSN-nummer. Alle betrokken jeugdartsen en -verpleegkundigen hebben uitsluitend toegang tot hun eigen scholen en kinderen. Elke jeugdarts en -verpleegkundige ontvangt unieke inloggegevens die alleen door de lokale helpdesk gegenereerd kunnen worden. Bij inloggen wordt gewerkt met een 2e factor beveiliging. Als een jeugdarts of -verpleegkundige geen toegang heeft tot de kindgegevens in JEJG omdat zij niet aan de school gekoppeld is, belt hij of zij met de JEJG helpdesk en wordt hij of zij gekoppeld. Om zeker te weten dat de jeugdarts of -verpleegkundige inderdaad is verbonden aan de school, checkt de helpdesk dit bij de JGZ teamleider.**
2.2	Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?	Nee	Nee: Ga verder. Ja: Anonimiseer of pseudonimiseer de gegevens en ga periodiek na of de gegevens niet indirect herleidbaar zijn.	Voor het signaleren van kinderen met (verhoogd risico op) beginnende problematiek, waar nodig gepaste zorg verlenen en opvolgen van individuen is het noodzakelijk dat bekend is om welke kinderen het gaat. Voor de uitvoering van wetenschappelijk statistisch onderzoek volstaan gepseudonimiseerde gegevens. Om dit moment wordt een tool ontwikkeld die ervoor zorgt dat persoonsgegevens gepseudonimiseerd ter beschikking komen voor onderzoek.
2.3	Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid, of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?	Ja	Nee: Ga verder. Ja: Zorg dat de betrokkenen of de algemene opinie dit niet als een potentiële bedreiging voor hun privacy zien.	De gegevens worden gebruikt als indicatie om (risico)gedrag in kaart te brengen, dat is onderdeel van het doel. Er zal altijd een gesprek plaats vinden om gegevens te duiden en te valideren. Alleen wanneer nodig voor opvolging en/of zorg worden resultaten opgeslagen in het digitaal dossier. De gegevens worden niet gebruikt om aanwezigheid of prestaties in kaart te brengen.
2.4	Is sprake van het verwerken van:			

D	**(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?**	**Ja**	**Ja: Verklein imagoschade en verstoring van de bedrijfsprocessen.** **Nee: Ga verder.**	**Kindgegevens worden nu samen met de uitslagen op itemniveau van de oudervragenlijst in één systeem opgeslagen. Om uit te sluiten dat uitslagen en gegevens verkeerd gekoppeld worden, wordt gewerkt met het BSN-nummer. Alle betrokken jeugdartsen en -verpleegkundigen hebben uitsluitend toegang tot hun eigen scholen en kinderen. Elke jeugdarts en -verpleegkundige ontvangt unieke inloggegevens die alleen door de lokale helpdesk gegenereerd kunnen worden. Bij inloggen wordt gewerkt met een 2e factor beveiliging. Als een jeugdarts of -verpleegkundige geen toegang heeft tot de kindgegevens in JEJG omdat zij niet aan de school gekoppeld is, belt hij of zij met de JEJG helpdesk en wordt hij of zij gekoppeld. Om zeker te weten dat de jeugdarts of -verpleegkundige inderdaad is verbonden aan de school, checkt de helpdesk dit bij de JGZ teamleider.**
A	Bijzondere persoonsgegevens?	Ja	Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 van de AVG. Nee: Ga verder.	Gezondheid is een bijzonder persoonsgegeven. De opslag en verwerking van de persoonsgegevens voldoet aan de beginselen van de AVG. Zowel automatisering als ITforCare zijn ISO27001 gecertifieerd. De GGD is bezig NEN 7510 gecertificeerd te worden.
B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
C	Wettelijk voorgeschreven persoonsnummers (bijvoorbeeld het burgerservicenummer (BSN))?	Ja	Ja: Verifieer of er een wettelijke basis is voor het gebruik. Nee: Ga verder.	De JGZ heeft een wettelijke basis voor het verplicht hanteren van BSN teneinde te waarborgen dat verwerkte persoonsgegevens op de betrokken cliënt betrekking hebben. Zie Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, artikel 1.B.3 (bijlage 9).

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
D	Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?	Nee	Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn. Nee: Ga verder.	Er worden geen andere gegevens verwerkt met verhoogde gevoeligheid.
2.4.1	Bij een van bovenstaande 'ja': kan het doel met andere gegevens worden bereikt die een verminderd risico op misbruik met zich mee brengen?	Nee	Ja: Gebruik andere minder ingrijpende gegevens. Nee: Ga verder.	De JGZ is conform de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, artikel 1.B.3 (bijlage 9) wettelijk verplicht om gebruik te maken van het BSN. Gegevens over gezondheid zijn noodzakelijk om gerichte zorg te kunnen verlenen aan identificeerbare individuen.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
2.5	Verwerkt u gegevens over kwetsbare groepen of personen?	Ja	Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de betrokkenen de mogelijkheid hebben zich aan de verwerking van persoonsgegevens te onttrekken. Nee: Ga verder.	JEJG is gericht op (kwetsbare) kinderen en hun ouders. Zowel automatisering als ITforCare zijn ISO27001 gecertifieerd. De GGD is bezig NEN 7510 gecertificeerd te worden. Uitsluitend jeugdartsen en -verpleegkundigen die zorg dragen voor de kinderen hebben toegang tot de persoonsgegevens. Voor de toegang tot de persoonsgegevens hebben zij unieke inloggegevens nodig. Jeugdartsen en -verpleegkundigen in de jeugdgezondheidszorg hebben, net als andere hulpverleners in de gezondheidszorg, een geheimhoudingsplicht. Meedoen met JEJG is niet verplicht. In de uitnodigingsbrief en op de publiekswebsite van JEJG wordt hier nadrukkelijk op gewezen. Ouders kunnen beslissen de vragenlijst niet in te vullen en/of niet naar het consult te komen. Waar gewenst kunnen zij zich hiervoor telefonisch afmelden. In de digitale vragenlijst kunnen ouders bezwaar maken voor het gebruik van de gegevens voor wetenschappelijk statistisch onderzoek.
2.6	Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?	Ja	Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn. Nee: Ga verder.	JEJG is gericht op grote groepen kinderen in Amsterdam/Amstelland en ook in andere regio's. Zie voor de beveiliging 2.5.

3 Betrokken partijen

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
3.1	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere *interne* partijen betrokken?	Ja	Ja: Zorg voor een duidelijke beschrijving van de verdeling van verantwoordelijkheden en taken van interne partijen (JGZ, MGGZ, EGZ, ITforCare, Automatisering). Zorg voor een duidelijke gegevensbeschrijving. Nee: Ga verder.	(Moet nog. Stappenplan van JGZ data via Janus tot gecodeerd anonieme data uitwerken en beschrijven.) Na afronding schooljaar of na maximaal anderhalf jaar worden de gegevens uit JEJG gehaald en gecodeerd anoniem gemaakt. Ook de back ups van die periode worden op dat moment verwijderd. Projectleider JEJG vraagt afdelingshoofd EGZ 5.1, 2, e 5.1, 2, e om via Topdesk een aanvraag te oen tot het verwijderen van de data uit de JEJG back-ups van vastgestelde periode.
3.2	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere *externe* partijen betrokken?	Ja	Ja: Zorg voor een duidelijke beschrijving van de verdeling van verantwoordelijkheden en taken van externe partijen. Zorg voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast. Nee: Ga verder.	Geanonimiseerde data worden op aanvraag geleverd aan externe onderzoeksinstellingen. In het contract wordt duidelijk vastgelegd welke variabelen gebruikt worden en voor welke doeleinden de data gebruikt mogen worden. Het contract heeft een einddatum waarna het geleverde en afgeleide databestand(en) vernietigd dient te worden. Dit dient schriftelijk te worden bevestigd.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
3.3	Zijn er partijen betrokken (in het project of bij de verwerking) die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden?	Nee	Ja: Ga na in hoeverre een adequaat beschermingsniveau wordt geboden door het betreffende land of de betreffende organisatie. Maak schriftelijke afspraken over hoe dit beschermingsniveau gehandhaafd kan worden. Nee: Ga verder.	Persoonsgegevens worden alleen in Nederland gebruikt.
3.4	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk verzameld zijn?	Ja	Ja: Ga verder. Nee: Doe een compliance check.	JGZ-professionals sturen in overleg met de ouders gegevens naar zorgpartijen, in lijn met het doel van het JGZ consult en met toestemming van ouders. Externe onderzoekspartijen gebruiken de anonieme gegevens voor statistisch en wetenschappelijk onderzoek teneinde de zorg aan kinderen te verbeteren.
3.5	Worden de gegevens verkocht aan derde partijen?	Nee	Ja: Doe een compliance check. Nee: Ga verder.	Gegevens worden niet verkocht of anderszins gebruikt voor commerciële doeleinden.
4	**Verzamelen van gegevens**			

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
4.1	Kan de manier waarop gegevens worden verzameld worden opgevat als privacy gevoelig (bijvoorbeeld omdat intieme of gevoelige informatie wordt gevraagd in een publiek gebied waar anderen dit kunnen horen, of omdat gebruik gemaakt wordt van (camera)observatie of tracking door cookies of GPS)?	Ja	Ja: Ga na of de gegevens op een andere manier kunnen worden verzameld. Nee: Ga verder.	Andere manieren van gegevensverzameling zou ten koste gaan van de respons en de kwaliteit. De JEJG vragenlijst wordt in een beveiligde digitale omgeving door ouders ingevuld. Ouders loggen in met een inlogcode die ze hebben ontvangen en gebruiken de geboortedatum van hun kind als verificatie. Bij nogmaals inloggen zal gewerkt worden met 2e factor beveiliging via de 06 van de ouders (de vraag van 06-nummer wordt ouders bij de eerste keer inloggen voorgelegd) ter bevestiging.
4.2	Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?	Ja	Ja: Ga verder. Nee: Maak een belangenafweging of het doel van de verwerking opweegt tegen de risico's voor de betrokkenen. .	Alle ouders ontvangen een brief en folder waarin staat vermeld met welk doel ouders de vragenlijst invullen. Ook op de publiekswebsite staat het doel uitgebreid beschreven. Daarnaast geven JGZ-organisaties op de eigen websites informatie over het doel en de invulling van de JGZ contactmomenten.
4.3	Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?	Ja	Ja: Ga verder. Nee: Doe een compliance check.	De gegevens zijn nodig voor het uitvoeren van het Basistakenpakket van de jeugdgezondheidszorg, dat wettelijk zijn beslag heeft gekregen in het BPG (bijlage 2, artikel 8).

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
4.4	Is duidelijk of u de gegevens verzamelt op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft gemaakt)?	Ja	Ja: Ga verder. Nee: Zorg dat de betrokkenen niet verrast worden door de verzameling van gegevens (op basis van opt-out).	De gegevens die verzameld worden voor de JGZ-consulten gaat via opt-in (ouders vullen het in). De gegevens die verzameld worden voor wetenschappelijk statistisch onderzoek gaat ook via opt-in (ouders kunnen aan het eind van de vragenlijst toestemming geven). Er ligt vanuit EGZ een wens voor aanpassing van opt-out naar opt-out bij gebruik gegevens voor wetenschappelijk statistisch onderzoek. Bij VO wordt ook gewerkt met opt-out. Bij wijze van een test is gekeken wat het effect is van opt-in. Omdat nu bijna een kwart van de invullers geen toestemming geeft is het databestand voor wetenschappelijk statistisch onderzoek minder representatief. JGZ werkt echter liever met opt-in, dat vinden ze gebruiksvriendelijker en meer aansluiten bij de uitvoeringspraktijk. Keuze voor opt-in of opt-out moet op hoger niveau worden gemaakt.
4.4.1	Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?	Ja	Ja: Ga verder. Nee: Zorg dat u betrokkenen de mogelijkheid biedt de toestemming in te trekken en maak dit systeemtechnisch mogelijk.	Ja, ouders kunnen op elk gewenst moment vragen de ingevulde vragenlijst te verwijderen. Dit kan zowel via de jeugdarts of jeugdverpleegkundige als via de JEJG helpdesk. Ook kunnen ouders op elk gewenst moment aangeven dat de gegevens niet gebruikt mogen worden voor wetenschappelijk statistisch onderzoek.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
4.4.2	Is de impact van het intrekken van de toestemming groot voor de betrokkene?	Nee	Ja: Zorg dat de betrokkenen uit vrije wil de toestemming kunnen intrekken (artikel 21 AVG). Nee: Ga verder.	Ouders kunnen het bij de jeugdarts of jeugdverpleegkundige aangeven als ze alsnog niet willen dat de ingevulde vragenlijst voor het JGZ consult wordt gebruikt. Jeugdarts of jeugdverpleegkundige kan de JEJG helpdesk vragen de ingevulde vragenlijst te verwijderen.
4.5	Vertelt u de betrokkene dat de gegevens worden verzameld?	Ja	Ja: Ga verder met vraag 4.5.2. Nee: Ga verder met vraag 4.5.1.	Ouders worden via brief, folder en publiekswebsite geïnformeerd over de vragenlijst en omgang met gegevens.
4.5.1	Bij 'nee': kunnen de betrokkenen op de hoogte zijn van het verzamelen van gegevens?	Nvt	Ja: Ga verder met vraag 4.6. Nee: Verken alle mogelijkheden om de betrokkenen op de hoogte te brengen van het verzamelen van gegevens. Ga verder met vraag 4.6.	
4.5.2	Bij 'ja' (op vraag 4.5): meldt u de betrokkene waarom de gegevens worden verzameld (wat u ermee gaat doen)?	Ja	Ja: Ga verder. Nee: Verken alle mogelijkheden om de betrokkenen op de hoogte te brengen waarom de gegevens worden verzameld.	Betrokkenen worden geïnformeerd over het doel van gegevensverzameling via brief, folder en publiekswebsite.
4.5.3	Bij 'ja' (op vraag 4.5): Meldt u de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?	Ja	Ja: Ga verder. Nee: Leg vast wannner aan wie welke gegevens worden verstrekt.	Betrokkenen worden via brief, folder en publiekswebsite geïnformeerd met wie en onder welke voorwaarden de gegevens eventueel worden gedeeld.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
4.6	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?	Nee	Ja: Ga na of de gegevens via een andere weg kunnen worden verzameld, of minder gegevens kunnen worden verzameld of dat de doelen van verder gebruik in lijn zijn met het doel van verzamelen. Nee: Ga verder.	Betrokkenen worden via brief, folder en publiekswebsite geïnformeerd over de opslag en verwerking van de gegevens.
5	**Gebruik van gegevens**			
5.1	Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?	Ja	Ja: Ga verder. Nee: Zorg dat het gebruik van de gegevens in overeenstemming is met het doel van de verwerking.	Alle gegevens zijn nodig voor vroegsignalering en vroeghulp bij sociaal-emotionele en sociaal-medische problemen bij kinderen van het PO. Daarnaast worden de gecodeerd anonieme gegevens gebruikt voor wetenschappelijk statistisch onderzoek.
5.2	Worden de gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?	Nee	Ja: Ga verder met vraag 5.2.1. Nee: Ga verder met vraag 5.3.	Gegevens worden gebruikt voor het JGZ consult en voor wetenschappelijk statistisch onderzoek teneinde de zorg aan kinderen te verbeteren.
5.2.1	Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?	Nvt	Ja: Ga verder. Nee: Zorg dat het doel van nieuwe bedrijfsprocessen past bij het oorspronkelijk doel van verzamelen. .	

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
5.3	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?	Ja	Ja: Ga verder. Nee: Verklein het risco dat op basis van de gegevens verkeerde conclusies worden getrokken of verkeerde acties worden ondernomen.	De vragenlijst wordt enkele dagen/weken voor het consult met de jeugdarts of -verpleegkundige door de ouder(s) ingevuld (juist en actueel). Tijdens het invullen van de vragenlijst wordt de ouder erop gewezen welke vragen nog niet zijn ingevuld (volledig). Er zal altijd een gesprek plaats vinden om gegevens te duiden en te valideren.
5.4	Worden op basis van de gegevens beslissingen genomen over de betrokkenen?	Ja	Ja: Ga verder met vraag 5.4.1. Nee: Ga verder met vraag 5.5.	
5.4.1	Bij 'ja': leveren de gegevens een volledig en actueel beeld van de betrokkenen op?	Nee	Ja: Ga verder. Nee: Verklein het risico dat op basis van de gegevens foutieve beslissingen worden genomen.	Er worden nooit alleen op basis van de ingevulde vragenlijst beslissingen genomen. Er volgt altijd een gesprek met de jeugdarts of –verpleegkundige om gegevens te duiden en te valideren. Bij twijfel kunnen specialisten worden geconsulteerd.
5.5	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?	Ja	Ja: Voorkom function creep. Nee: Ga verder.	Gegevens van JEJG worden vergeleken met gegevens uit digitaal dossier JGZ tijdens het JGZ consult. De kans op function creep is echter minimaal omdat gegevens uit beide bronnen voor hetzelfde doel zijn verzameld en vanuit dezelfde wettelijke grondslag.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
5.6	Worden de gegevens breed verspreid binnen de organisatie?	Nee	Ja: Zorg voor een duidelijke beschrijving van wie (afdelingen en personen) toegang hebben tot de gegevens en met welk doel. Nee: Ga verder.	Alleen direct betrokkenen van de afdeling JGZ (jeugdarts(en), -verpleegkundige(n) en doktersassistenten die zorg dragen voor betreffend kind) hebben toegang tot de persoonsgegevens. Zij zijn verantwoordelijk voor zorg op maat. Daarnaast hebben helpdeskmedewerkers (JGZ), technisch beheerders (ITforcare) en functioneel applicatiebeheerder (EGZ) toegang tot (persoons)gegevens in de applicatie uit hoofde van hun ondersteunende rol voor de juiste werking van het product en het genereren van gebruikersaccounts. De databeheerder (EGZ) heeft na afloop van het schooljaar toegang tot gecodeerd anonieme gegevens. Onderzoekers (intern en extern) kunnen op aanvraag toegang krijgen tot geanonimiseerde gegevens en deze gebruiken voor wetenschappelijk statistisch onderzoek. Onderzoekers krijgen uitsluitend toegang tot de variabelen die zij voor het doel van hun onderzoek nodig hebben.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
5.7	Worden de gegevens verspreid buiten de organisatie?	Nee	Ja: Zorg voor een duidelijke beschrijving van wie (organisaties en personen) toegang hebben tot de gegevens en met welk doel. Geef tevens aan hoe vaak (frequentie) de gegevens worden verstrekt, het medium dat wordt gebruikt en de maatregelen om ander gebruik te voorkomen. Leg afspraken contractueel vast. Nee: Ga verder met vraag 5.8.	Geanonimiseerde data van Amsterdamse en Amstellandse kinderen wordt gepresenteerd op *Gezondheid in Beeld*, dit gebeurt op stadsdeelwijkniveau. Hierbij worden gegevens uitsluitend gepresenteerd wanneer geldt: N>50 en n>5. Onderzoeksinstellingen kunnen geanonimiseerde data opvragen voor wetenschappelijk en statistisch onderzoek. Deze data wordt uitsluitend geleverd wanneer de betreffende onderzoeksinstelling een contract ondertekent (zie 3.2 en bijlage 8). Onderzoeksinstellingen dienen na afloop van het onderzoek de data te vernietigen en dit schriftelijk aan de GGD te bevestigen.
5.7.1	Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?	Nvt	Ja: Ga verder. Nee: Breng de betrokkenen op de hoogte dat gegevens worden doorgegeven aan partijen buiten de organisatie. Zorg dat maatregelen zijn getroffen om de gegevens te beschermen.	
5.8	Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?	Ja	Ja: Ga verder met vraag 5.8.1. Nee: Ga verder met vraag 5.9.	

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
5.8.1	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?	Nee	Ja: Zorg ervoor dat duidelijk is op basis waarvan deze profielen worden opgesteld, welke beslissingen op welke wijze op basis van deze profielen worden genomen, en of uit de profielen gevoelige informatie is af te leiden. Zorg er ook voor dat indien nodig betrokkenen worden geïnformeerd. Nee: Ga verder.	Op basis van de antwoorden wordt voor elke ouder/kind een uitslag met tips opgesteld. Dit profiel is gebaseerd op betrouwbare en valide screeningsinstrumenten. Er vindt geen automatische beslissing plaats op basis van het profiel. Het profiel wordt besproken met de ouder en het kind en in onderling overleg wordt besloten of een vervolgactie nodig is.
5.9	Kunnen de betrokkenen hun gegevens inzien of daarom vragen?	Ja	Ja; Ga verder. Nee: Zorg dat de betrokkenen hun eigen gegevens in kunnen zien of daarom kunnen vragen.	Ouders hebben recht op inzage en verwijdering van de gegevens in JEJG. Zij kunnen daar om vragen bij de jeugdarts of -verpleegkundige. Ouders hebben dit recht tot hun kind 12 jaar oud wordt, daarna besluiten ouder en kind samen. De jeugdarts of -verpleegkundige mag inzage weigeren in het belang van het kind.
5.10	Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?	Ja	Ja: Ga verder. Nee: Zorg dat de betrokkenen hun eigen gegevens kunnen corrigeren of daarom kunnen vragen.	Ouders hebben recht op wijziging van de gegevens in JEJG. Ouders hebben dit recht tot hun kind 12 jaar oud wordt, daarna besluiten ouder en kind samen. De jeugdarts of jeugdverpleegkundige mag verwijdering weigeren als dat in het belang van het kind is.

B	**Uniek identificerende gegevens (bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen)?**	**Nee**	**Ja: Zorg dat de gegevens bijzonder goed beveiligd zijn en dat de verwerking van de gegevens voldoet aan artikel 9 lid 4 van de AVG.** **Nee: Ga verder.**	**Er wordt geen gebruik gemaakt van vingerafdrukken, DNA-profielen of andere biometrische gegevens.**
			Ja: Ga verder.	
5.11	Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?	Ja	Nee: Zorg dat de betrokkenen hun eigen gegevens kunnen verwijderen of daarom kunnen vragen. Of leg de betrokkenen uit welke zwaarwegende redenen er zijn om dit (deels) niet te doen.	Ouders hebben recht op verwijdering van de gegevens in JEJG. Ouders hebben dit recht tot hun kind 12 jaar oud wordt, daarna hebben zij toestemming van hun kind nodig. De jeugdarts of jeugdverpleegkundige mag verwijdering weigeren als dat in het belang van het kind is.

6 Bewaren en vernietigen

<u>Data inclusief persoonsgegevens:</u> Na afronden van het JGZ consult worden de belangrijkste bevindingen en conclusies in Kidos (digitaal dossier) geregistreerd. Delen van de screeningsvragenlijst kunnen als PDF in Kidos worden gehangen wanneer de vragenlijst wordt gebruik voor een verwijzing en/of de vragenlijst van toegevoegde waarde is voor zorg.

Gegevens in het digitaal dossier worden bewaard tot 15 jaar na de behandelrelatie. Dit is wat de WGBO (bijlage 4) voorschrijft voor alle medische dossiers. Gegevens worden na afloop van het schooljaar en afronding van de JGZ consulten (in september) uit de JEJG applicatie

6 Bewaren en vernietigen

6.1	Is een bewaartermijn voor de gegevens vastgesteld?	Ja Ja: Ga verder. Nee: Zorg dat de gegevens niet langer bewaard blijven dan nodig en wettelijk is toegestaan.	verwijderd. <u>Data exclusief persoonsgegevens:</u> Na afloop van het schooljaar (juli) wordt de data uit JEJG geexporteerd. Deze data wordt zodanig bewerkt (gecodeerd anoniem) dat de gegevens niet meer tot een persoon herleidbaar zijn. Zie bijlage 6, tabblad 2 en 3. Deze data wordt beheerd door databeheer van de afdeling EGZ en op aanvraag anoniem beschikbaar gesteld voor wetenschappelijk en statistisch onderzoek. Voor uitgebreid stappenplan zie bijlage 6, tabblad 1. De voorzienbare bewaartermijn van gecodeerd anonieme data is afgelopen nadat het onderzoek is gepubliceerd en het niet meer aannemelijk is dat in de literatuur vragen worden gesteld bij de analyses die hernieuwde beoordeling van de data noodzakelijk maken. Uitgangspunt hierbij is een bewaartermijn van maximaal 5 jaar nadat een jongere uitstroomt bij JGZ (19 jaar). Na die periode treedt de Archiefwet in werking.

6 Bewaren en vernietigen

6.2	Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?	Ja	Ja: Ga verder met 6.2.1. Nee: Zorg dat de gegeven nadat ze niet meer nodig zijn vernietigd worden (als een wettelijke verplichting om ze te bewaren dit niet in de weg staat) of indien dit niet mogelijk is geanonimiseerd worden.	De data inclusief persoonsgegevens worden na de eerder genoemde termijnen (zie 6.1) verwijderd uit JEJG. Projectleider JEJG vraagt afdelingshoofd EGZ 5.1, 2, e5.1, 2, e om via Topdesk een aanvraag te doen tot het verwijderen van de data uit de JEJG back-ups van vastgestelde periode. Verwijderen gecodeerd anonieme data: proces moet nog uitgewerkt.
6.2.1	Zo ja (op vraag 6.2), worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen of te gebruiken zijn?	Ja	Ja; Ga verder. Nee: Bepaal per gegevensdrager op welke wijze de gegevens worden vernietigd of verwijderd.	De data inclusief persoonsgegevens worden na de eerder genoemde termijnen (zie 6.1) verwijderd uit JEJG en back-ups van automatisering. De data exclusief persoonsgegevens wordt volgens eerder genoemde termijnen (zie 6.1) gecodeerd anoniem gemaakt en blijven in die vorm beschikbaar voor wetenschappelijk statistisch onderzoek. Verwijderen gecodeerd anonieme data: proces moet nog uitgewerkt.

7 Beveiliging

6 Bewaren en vernietigen

				Zowel automatisering als ITforCare zijn ISO27001 gecertifieerd.
7.1	Is sprake van intern geformuleerd beleid over het beveiligen van informatie?	Ja	Ja: Ga verder. Nee: Maak duidelijk wie verantwoordelijk is voor dit beleid. Geef aan bij welke algemene beveiligheidsstandaarden wordt aangesloten. Geef aan hoe rekening gehouden wordt met het gevoelige karakter van de gegevens. Zorg dat het beveiligheidsbeleid wordt getoetst.	Bij de afdelingen automatisering en Itforcare geldt het beleid dat applicaties tijdens de ontwikkelfase intern uitgebreid worden getest. Jaarlijks vindt een penetratietest plaats (intern), eens per twee jaar wordt een penetratietest door een onafhankelijk bureau uitgevoerd (extern). Het beleid van automatisering is vastgelegd in de Service Level Agreement (SLA), zie bijlage 7. De GGD is bezig NEN 7510 gecertificeerd te worden.
7.2	Zo ja (op vraag 7.1), is duidelijk met welke maatregelen er voor wordt gezorgd dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?	Ja	Ja: Ga verder. Nee: Stel een informatiebeveiligingsplan op met daarin maatregelen die voor een passende bescherming van de gegevens zorgen.	De GGD Amsterdam voert jaarlijks een privacy impact assessment uit naar de privacybescherming (verwerking van persoonsgegevens). Daarnaast word jaarlijks gekeken naar (1) de Betrouwbaarheid, Integriteit en Vertrouwelijkheid (BIV), (2) de Verkorte Risico Analyse (VRA) en (3) de penetratietesten van de applicatie. Maatregelen die uit deze analyses voortkomen worden doorgevoerd.

6	**Bewaren en vernietigen**		
7.3	Zo ja, is bij het vaststellen van de maatregelen rekening gehouden met de richtlijnen Beveiliging persoonsgegevens die de Autoriteit persoonsgegevens heeft gepubliceerd?	Ja: Ga verder. Nee: Toets alsnog of en zo ja in welke mate de beveiliging van de persoonsgegevens is geborgd in lijn met de eisen van de Richtsnoeren en met relevante beveiligingsstandaarden.	De GGD is bezig met een certificeringstraject NEN7510. Volgens de AVG moeten bedrijven en overheden passende technische en organisatorische maatregelen nemen om persoonsgegevens zo goed mogelijk te beveiligen. (1) Organisaties moeten moderne techniek gebruiken om persoonsgegevens te beveiligen. (2) Organisaties moeten kijken hoe ze met persoonsgegevens omgaan (wie heeft toegang tot welke gegevens). Jaarlijks wordt een penetratietest uitgevoerd, die zowel kijkt naar de technische als organisatorische kant. Maatregelen die uit deze analyse voortkomen worden doorgevoerd.
8	**Meldplicht datalekken**		
8.1	Zijn maatregelen getroffen om datalekken indien noodzakelijk te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?	Ja: Ga verder. Nee: Tref alsnog maatregelen om Ja datalekken te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen.	In de verwerkersovereenkomst staat uitgebreid beschreven hoe te handelen bij datalekken. Melding aan de Autoriteit Persoonsgegevens en aan de getroffen personen is hierbij opgenomen.
8.2	Zo ja, is bij het vaststellen van de maatregelen rekening gehouden met de Richtsnoeren die de Autoriteit persoonsgegevens over de meldplicht datalekken heeft gepubliceerd?	Ja: Einde vragenlijst. Nee: Toets alsnog of en zo ja in welke mate de meldplicht van datalekken is geborgd in lijn met de eisen van de Richtsnoeren. Einde vragenlijst	

6 Bewaren en vernietigen

Bijlagen:

1. Wet Publieke Gezondheid (WPG)
2. Besluit Publieke Gezondheid (BPG)
3. Algemene Verordening Gegevensbescherming (AVG)
4. Wet op de geneeskundige behandelingsovereenkomst (WGBO)
5. Wet op de Beroepen in de individuele gezondheidszorg (Wet BIG)
6. Verantwoordelijkheden, gegevensbewerking en databestanden JEJG (op aanvraag beschikbaar)
7. Service Level Agreement (SLA)
8. Voorbeeld contract datagebruik JEJG
9. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
10. Risico’s en maatregelen