Informatieveiligheid en Privacy
Stichting Wijkteams Arnhem

Inhoud

Inleiding

Met de decentralisatie van het Sociaal Domein in 2015 heeft de gemeente Arnhem de wettelijke taken op het gebied van de WMO 2015 en de Jeugdwet belegd bij de sociale wijkteams.
Op 1 januari 2017 is de Stichting Wijkteams Arnhem als zelfstandige entiteit verder gegaan en voert ook werkzaamheden in het kader van de gemeentelijke schulddienstverlening uit.
Afspraken in het kader van de relatie Stichting - gemeente zijn opgenomen in de DVO's en in de overeenkomst gegevensverwerking. In die laatstgenoemde overeenkomst is in artikel 4 bepaald dat de Stichting een 'plan van aanpak' vaststelt betreffende de informatieveiligheid en privacy.
Voorliggend document voorziet daarin.

Het afgelopen jaar heeft voor wat betreft privacy met name in het teken gestaan van de implementatie van de in werking getreden Algemene Verordening Gegevensbescherming. De activiteiten die in dat verband zijn uitgevoerd, worden in dit Plan genoemd.

Arnhem, januari 2019

Privacybeleid

Het college van burgemeester en wethouders heeft in december 2014 het Privacybeleid Sociaal Domein vastgesteld. Hierin zijn de uitgangspunten voor de wijze waarop wordt omgegaan met gegevensverwerking in het sociale domein.
Hoewel er sindsdien een nieuw wettelijk kader is in de vorm van de AVG, staan deze uitgangspunten nog steeds overeind:

- dataminimalisatie; privacy begint met het níet verzamelen van persoonsgegevens
- transparantie: we zijn helder in welke persoonsgegevens we verwerken
- alleen die persoonsgegevens worden verwerkt voor een bepaald, concreet doel en niet meer dan strikt noodzakelijk, waarbij een onderscheid bestaat tussen 'wat' en 'dat'-informatie;
- persoonsgegevens worden niet langer dan noodzakelijk bewaard;
- Wijkteam komt in actie op grond van een menselijk signaal en niet op grond van door een computer gegenereerde gegevens

In de aankomende periode zal worden bezien of er in de AVG en de gewijzigde relatie tussen Stichting en college van Arnhem aanleiding moet worden gevonden het beleid aan te passen en te laten vaststellen door het bestuur van de Stichting.

Informatieveiligheid

Doelstelling

De doelstelling van een informatiebeveiligingsplan is het beschermen van belangrijke bedrijfsmiddelen van de sociale wijkteams Arnhem. Onder bedrijfsresources verstaan we in dit kader alle bedrijfskritische informatie en de geautomatiseerde en niet geautomatiseerde informatievoorziening waarin die informatie wordt verwerkt.

Het beschermen van de bedrijfsmiddelen wordt gedaan om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te borgen.

Vertrouwelijkheid: De wijze waarop we zorgen dat bedrijfsmiddelen niet ongeautoriseerd op straat komen te liggen of in verkeerde handen valt.

Integriteit: De wijze om te voorkomen dat bedrijfsmiddelen worden gemanipuleerd c.q. ongeautoriseerd worden gewijzigd.

Beschikbaarheid: De wijze om te voorkomen dat we ons dagelijks werk niet kunnen uitvoeren omdat bedrijfsmiddelen niet beschikbaar zijn.

Organisatie en governance

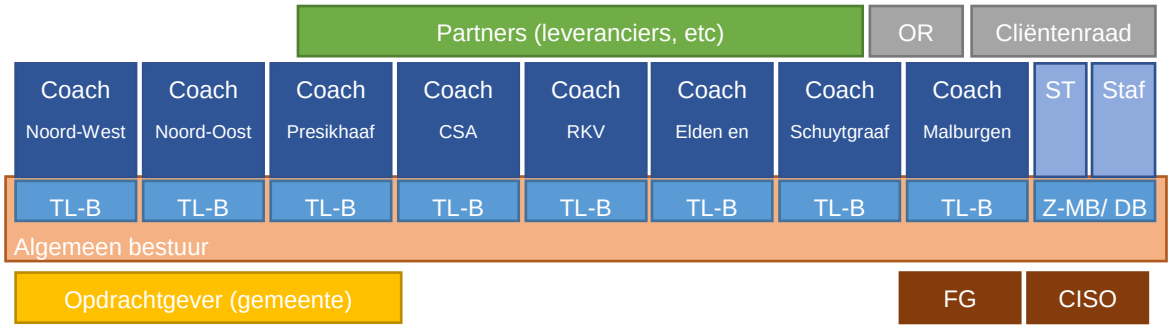
Aan de onderwerpen informatieveiligheid en privacy wordt veel belang gehecht door het bestuur van de Stichting. Het algemeen bestuur bestaat uit acht teamleider-bestuurders (TL-B) en één zakelijk medebestuurder (Z-MB). De zakelijk medebestuurder vormt het dagelijks bestuur (DB).

Het volledige bestuur is verantwoordelijk voor het collectief, zo ook informatieveiligheid en privacy. De teamleider-bestuurders geven leiding aan de dagelijkse praktijk. De dagelijks praktijk bestaat uit het leiding geven aan het sociale wijkteam bestaande uit coaches jeugd en volwassenen. De coach legt verantwoording af aan de teamleider-bestuurder. De zakelijk medebestuurder draagt zorg voor de bedrijfsvoering en is daarmee de aandachtsfunctionaris voor informatieveiligheid en privacy. De zakelijk medebestuurder stimuleert en legt de noodzakelijke verbindingen met de overige bestuurders.

Het algemeen bestuur heeft een functionaris gegevensbescherming (FG) aangewezen die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG): privacy. De FG vervult deze taak en verplichting onafhankelijk.

Ook is een Chief Information Security Officer (CISO) aangewezen die toezicht houdt op de informatiebeveiliging en adviseert over een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen de organisatie. Met als doel dat inbreuken op de informatiebeveiliging worden voorkomen. Of, als ze toch voorkomen, de gevolgen geminimaliseerd worden.

De zakelijk medebestuurder, overlegt periodiek (eens in de drie weken) met de FG en de CISO van de Stichting. Als er sprake is van een beveiligingsincident, zullen medewerkers van de sociale wijkteams dit melden via een daarvoor bestemd mailadres en bij hun teamleider/bestuurder. Voor het melden van beveiligingsincidenten/datalekken is een protocol opgesteld, die als bijlage bij dit Plan is gevoegd.



Personele bewustwording & instructie

Het privacybewustzijn bij de medewerkers van de Stichting is hoog. Dat is, gezien de gevoelige informatie die wordt verwerkt, noodzakelijk. Het is belangrijk dat medewerkers zich bewust zijn en blijven van het doel waarvoor de persoonsgegevens verwerkt, dat dit op een veilige manier gebeurt en niet meer persoonsgegevens verwerkt worden dan nodig is. Aan het bewustzijn werken gebeurt doorlopend door de gesprekken die regelmatig over deze onderwerpen worden gevoerd binnen de wijkteams. Daarnaast hebben medewerkers van de Stichting deelgenomen aan de campagne Safe en Sound die ook binnen de gemeente Arnhem door medewerkers is gevolgd. Omdat het bewustzijn moet worden onderhouden, zullen er regelmatig activiteiten worden gepland ter bevordering daarvan. Teamleiders-bestuurders nodigen de functionaris gegevensbescherming en de CISO halfjaarlijks uit om met de teams in gesprek te gaan over privacy en informatieveiligheid.

Gecertificeerde hostingsomgevingen

SWTA streeft erna dat alle hostingsomgeving aantoonbaar ISO27001 of NEN7510 gecertificeerd zijn of aantoonbaar voldoen aan de Baseline Informatieveiligheid Gemeenten (BIG). Hierin worden nog enkele acties ondernomen.

Leveranciersafspraken & verwerkersovereenkomsten

SWTA maakt gebruik van leveranciers die in opdracht bedrijfsgegevens verwerken. SWTA heeft als verwerkingsverantwoordelijke daarom afspraken gemaakt met leveranciers over de verwerking van bedrijfsgegevens.

Leverancier	**Dienst**	**Soort afspraak**
ICT de Connectie	Leverancier digitale werkplek en hosting regiesysteem	Verwerkersovereenkomst
AAG Connect	Leverancier financiële/ salaris/ personeel administratie	Verwerkersovereenkomst
Computron / nieuwe leverancier	Hoster website	Contract + verwerkersovereenkomst sluiten
Einder communicatie	Vormgever en functioneel beheerder website	Onderhoudscontract + verwerkersovereenkomst sluiten
Embrace	Leverancier en hosting intranet	Contract + verwerkersovereenkomst sluiten
Gemeente Arnhem	Opdrachtgever	Verwerkersovereenkomst
Accountant	Controle financiële administratie, jaarrekening	Geen, is zelf verwerkingsverantwoordelijke
Arbodienst/bedrijfsarts	Arbeidsmedisch onderzoek	Geen, is zelf verwerkingsverantwoordelijke
Arbodienst/bedrijfsarts	Uitvoering PvA, begeleiding, advies	Geen, is zelf verwerkingsverantwoordelijke

Informatieplicht & privacyverklaring

In de AVG staat dat organisaties de informatie over verwerkingen in principe schriftelijk moet geven. De beste manier om er zeker van te zijn dat deze informatie voor de meeste mensen goed vindbaar is, is het publiceren van een online privacyverklaring. SWTA volgt dit advies.

De AVG stelt een aantal specifieke eisen waar een privacyverklaring aan moet voldoen. Deze eisen gaan over de inhoud, de toegankelijkheid en de duidelijkheid van informatie. SWTA heeft langs deze eisen haar privacyverklaringen opgesteld.

SWTA beschikt over twee privacyverklaringen,:

- Voor betrokkenen (klanten en opdrachtgevers) op website
- Voor medewerkers centraal (o.a. op intranet)

Privacy by design en privacy by default

Privacy by design	Privacy by design houdt in dat bij het ontwerpen van producten en diensten bedrijfsinformatie goed worden beschermd.
Privacy by default	Privacy by default houdt in dat technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat, als standaard, alleen bedrijfsinformatie wordt verwerkt die noodzakelijk zijn voor het specifieke doel
Uitgangspunt SWTA	Het uitgangspunt van SWTA is bij het ontwerp en inrichting alleen benodigde bedrijfsinformatie uit te vragen en te registreren die benodigd zijn voor het doel. SWTA heeft dataminimalisatie als uitgangspunt.

Functionaris Gegevensbescherming

In april 2018 is besloten een externe functionaris voor de gegevensbescherming te benoemen tot 1 januari 2019. Deze benoeming is verlengd tot 1 januari 2020. De taken en bevoegdheden van de functionaris zijn verwoord in de AVG, maar zijn door het bestuur van de Stichting ook vastgelegd in het Statuut voor de FG. Dit statuut treft u als bijlage 2 bij dit Plan aan.

Data protection impact assessment (DPIA)

Als verantwoordelijke moet SWTA een data protection impact assessment (DPIA) uitvoeren wanneer de gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. SWTA bepaalt dit zelf. De werkgroep van Europese privacytoezichthouders (WP29) heeft een lijst van 9 criteria opgesteld om hierbij te helpen.

Criteria	Antwoord
Beoordelen van mensen op basis van persoonskenmerken	Ja, SWTA beoordeelt op basis van persoonskenmerken welke vorm van ondersteuning en zorg benodigd is
Geautomatiseerde beslissingen	Nee, SWTA doet niet aan geautomatiseerde beslissingen
Stelselmatige en grootschalige monitoring	Nee, SWTA doet hier niet aan
Gevoelige gegevens	Ja, doelmatig voor ondersteuning of veiligheid van medewerkers en anderen
Grootschalige gegevensverwerkingen	Nee
Gekoppelde databases	Ja, met administratieve backoffice
Gegevens over kwetsbare personen	Ja, doelmatig voor ondersteuning of veiligheid van medewerkers en anderen
Gebruik van nieuwe technologieën	Nee
Blokkering van een recht, dienst of contract	Ja, zonder adequate persoonsgegevens kan SWTA ondersteuningbehoevende niet ondersteunen. Dit is een logisch vervolg met wettelijke basis.
Conclusie & verantwoording	SWTA heeft een hoog privacyrisico en voert daarom een DPIA uit.

In 2019 zal SWTA een algehele DPIA uitvoeren. Regulier voert SWTA een DPIA uit bij het inzetten van nieuwe informatiesystemen, wijzigingen in werkwijzen of andere organisatorische wijzigingen die impact hebben op gegevensverwerkingen.

Technische maatregelen

Accounts & inlog beleid & monitoring

Iedereen die geautoriseerd toegang heeft tot bedrijfsmiddelen heeft:

- Een persoonlijk account;
- Afgedwongen "sterk' wachtwoordbeleid;
- Afgedwongen multi-factor authenticatie; via een soft/hard token;
- Pogingen worden bijgehouden in digitale audit logs.

Afgesloten dossierkasten

SWTA maakt uitsluitend gebruik van af te sluiten dossierkasten om ongeautoriseerde fysieke toegang tot bedrijfsmiddelen te voorkomen.

Verbindingen via SSL

Toegang tot de websites/ intranet/ digitale werkplek/ etc maken geforceerd gebruik van een Secure Socket Layer (SSL) verbinding. Dit zorgt voor een versleutelde verbinding.

Beveiligde mail

Ondanks het uitgangspunt zo min mogelijk privacygevoelige gegevens te mailen zijn soms uitzonderingen nodig. In de driehoek van gemeente, administratieve backoffice en SWTA is beveiliging (o.a. TLS) op reguliere mail afgedwongen. Voor andere ontvangers is Cryptshare als beveiligde mailoplossing neergezet. Als actie voor 2019 is het maken van afspraken met alle zorg aanbieders om conform de landelijke "Intentieverklaring Veilige E-mail Coalitie".

Backups

De totale digitale werkomgeving van SWTA loopt mee in een dagelijkse incrementele backup, 3 wekelijkse full backup en een 13 maanden backup.

Apparaten + apparaatbeleid

SWTA heeft drie soorten apparaten: laptops, printers en mobiele telefoons. De laptops en telefoons zijn voorzien van Mobiel Device Management (MDM) en Mobiel Applicatie Management (NAM). Lokaal worden er geen bedrijfsmiddelen opgeslagen. Deze zijn alleen toegankelijk via Citrix.

Naleving en controle

Regulier overleg

Op regelmatige basis bespreken de zakelijk medebestuurder, de CISO en de FG van de Stichting de ontwikkelingen op het gebied van informatieveiligheid en privacy. Met de CISO en FG van de gemeente Arnhem is contact op basis van noodzaak en behoefte.

DigiD beveiligingsassessment

Het burgerportaal is publiekelijk toegankelijk via DigiD. Hierin kunnen inwoners hun dossier online inzien. Jaarlijks wordt als onderdeel van de ENSIA een beveiligingsassessment uitgevoerd op de DigiD aansluiting en de achterliggende regieapplicatie.

Kwetsbaarheidsscans

Periodiek worden er kwetsbaarheidsscans door ICT de Connectie uitgevoerd. Dit proces dient het komende jaar nog meer geautomatiseerd te worden ingezet.

Werkwijzen

Proces: Verwerkingsregister

Om transparantie te realiseren met betrekking tot de persoonsgegevens die worden verwerkt door de Stichting, is er op 23 juli 2018 een verwerkingsregister door het bestuur vastgesteld. Dit register, dat als bijlage 1 aan dit plan van aanpak is toegevoegd, is een dynamisch document en bevat een opsomming van bedrijfsprocessen en de persoonsgegevens die daarbij worden verwerkt binnen de Stichting. Dit zijn met name de processen en persoonsgegevens die voortvloeiende uit de opdracht van de gemeente Arnhem worden uitgevoerd (hulpverlening in het kader van Jeugdwet, Wet Maatschappelijke Ondersteuning 2015, leerlingenvervoer, Schuldhulpverlening). Daarnaast zijn er interne bedrijfsprocessen opgenomen. Behalve de categorie van persoonsgegevens en de betrokkenen is in het register aangegeven wat de wettelijke bewaartermijnen zijn voor deze persoonsgegevens. Bij uitbreiding of wijziging van werkzaamheden, waarbij persoonsgegevens verwerkt worden, wordt het register aangepast en jaarlijks werkafspraken vastgesteld**.**
Door het bestuur van de Stichting zijn in het voorjaar van 2018 werkafspraken vastgesteld over hoe coaches geacht worden, in het licht van hun werkzaamheden, om te gaan met persoonsgegevens. De werkafspraken zijn niet van boven opgelegd, maar worden breed gedragen door coaches in alle wijkteams. Ze zijn voorafgaand aan vaststelling gedeeld met de wijkcoaches en getoetst aan de praktijk. In bijlage 3 van dit Plan treft u de werkafspraken privacy aan. De werkafspraken maken deel uit van het handboek voor de wijkcoach. Bij het aantrekken van nieuwe medewerkers wordt door de teamleider specifieke aandacht aan gegevensbescherming besteed. Ook de werkafspraken zijn dynamisch; bij ontwikkelingen (zoals de aanschaf van een nieuw regiesysteem met nieuwe functionaliteiten) worden ze aangepast.

Proces: Datalek

Uiteraard is het uitgangspunt dat iedereen zorgvuldig met persoonsgegevens om gaat, maar het kan voorkomen dat persoonsgegevens in verkeerde handen terechtkomen. Voor een dergelijk datalek is een meldingsproces vastgesteld. In bijlage 4 is dit proces terug te vinden. Er is een centrale registratie van beveiligingsincidenten, die wordt bijgehouden door de CISO.

Proces: Rechten van betrokkenen

Inwoners van de gemeente Arnhem zijn de grootste groep van betrokkenen als het gaat om persoonsgegevens die door de Stichting worden verwerkt. Zij hebben toegang tot het regiesysteem, waarin hun gegevens in 'Mijn Plan Ons Plan' zijn geregistreerd. Inwoners kunnen hun gegevens in het regiesysteem wijzigen. Het bestuur van de Stichting heeft het daarom niet opportuun geacht om een apart werkproces in te richten voor de rechten van inzage, correctie en verwijdering van persoonsgegevens. Inwoners kunnen zich bij vragen hieromtrent rechtstreeks tot hun coach richten en bij onduidelijkheden kan de coach contact opnemen met de Functionaris voor de Gegevensbescherming. Ten aanzien van verwijdering van persoonsgegevens heeft de Stichting zich wel te houden aan de wettelijke bewaartermijnen. Mocht in de praktijk blijken dat er wel behoefte bestaat aan de inrichting van een werkproces, dan zal dat alsnog gebeuren.

Bijlage 1 Verwerkingsregister juli 2018

Verwerkingsactiviteit	Doeleinde (werkproces)	Grondslag	Verantwoordelijke(n)	Categorie betrokkenen	Categorie gegevens	Ontvangers (waaraan gegevens worden verstrekt; geen verwerkers)	Verwerker + verwerkersovereenkomst?	Buiten de EU	Bewaartermijn	Applicatie
Ondersteuning en inzet specialistische zorg										
Het beoordelen van hulpvraag op het gebied van WMO, Jeugdwet, Wet op Gemeentelijke Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs: **1. aanvraag afspraak inwoner**	Leveren van maatwerk aan inwoner zodat ze zelf weer verder kunnen: het maken van een afspraak voor intake	WMO, Jeugdwet en Wet op Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs	Stichting en college	inwoners gemeente Arnhem	NAW, geboortedatum, telefoonnummer inwoner	medewerker serviceteam, wijkcoach	**p.m.**	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	Timeblocker
Het beoordelen van hulpvraag op het gebied van WMO, Jeugdwet, Wet op Gemeentelijke Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs: **2. keukentafelgesprek**	Leveren van maatwerk aan inwoner zodat ze zelf weer verder kunnen: het voeren van een gesprek om de hulpvraag te kunnen beoordelen	WMO, Jeugdwet en Wet op Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs	Stichting en college	inwoners gemeente Arnhem	NAW, geboortedatum, geslacht, telefoonnummer, BSN, beschrijving van feiten, beleving, doelen inwoner op meerdere leefgebieden, gezondheidsgegevens inwoner (al dan niet aangeleverd door derden), beschikking Rechtbank.	wijkcoach	n.v.t.	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	CVS (mijn Plan Ons Plan MPOP; dossier aanmaken)
Het beoordelen van hulpvraag op het gebied van WMO, Jeugdwet, Wet op Gemeentelijke Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs: **3. toekennen/afwijzen specialistische zorg**	Leveren van maatwerk aan inwoner zodat ze zelf weer verder kunnen: het beslissen op de hulpvraag	WMO, Jeugdwet en Wet op Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs	Stichting en college	inwoners gemeente Arnhem	NAW en BSN inwoner, inhoud uit MPOP, productomschrijving toegekende zorg	1. medewerkers wijkteam 2. medewerkers gemeente Arnhem (Beheer PDC, FB, backoffice OSD) 3. leveranciers specialistische zorg	Zorglokaal verwerkersovereenkomst d.d. 29/30-12-2014	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	1. CVS (mijn Plan Ons Plan MPOP; product toekennen) 2. PTRM 3. Mybility

Het beoordelen van hulpvraag op het gebied van WMO, Jeugdwet, Wet op Gemeentelijke Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs: **berichtenverkeer**	Leveren van maatwerk aan inwoner zodat ze zelf weer verder kunnen: klaarzetten en versturen opdracht specialistische zorg	WMO, Jeugdwet en Wet op Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs	Stichting en college	inwoners gemeente Arnhem	1. NAW, telefoonnr inwoner 2. naam en telefoonnr wijkcoach 3. gegevens zorgaanbieder (productomschrijving)	medewerkers wijkteams	Zorglokaal verwerkersovereenkomst d.d. 29/30-12-2014	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	CVS
Het beoordelen van hulpvraag op het gebied van WMO, Jeugdwet, Wet op Gemeentelijke Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs: **Rapport OSD**	Leveren van maatwerk aan inwoner zodat ze zelf weer verder kunnen: informatievoorziening OSD	WMO, Jeugdwet en Wet op Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs	Stichting en college	inwoners gemeente Arnhem	1. NAW, telefoonnr inwoner 2. naam en telefoonnr wijkcoach 3. gegevens zorgaanbieder (productomschrijving)	1. medewerkers wijkteams 2. medewerkers gemeente Arnhem (backoffice OSD)	n.v.t.	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	CVS
Het beoordelen van hulpvraag op het gebied van WMO, Jeugdwet, Wet op Gemeentelijke Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs: **Rapport Leerlingenvervoer**	Leveren van maatwerk aan inwoner zodat ze zelf weer verder kunnen: informatievoorziening leerlingenvervoer	WMO, Jeugdwet en Wet op Schuldhulpverlening, Wet op primair onderwijs, Wet op expertisecentra, Wet op voortgezet onderwijs	Stichting en college	inwoners gemeente Arnhem	1. NAW, telefoonnr inwoner 2. naam en telefoonnr wijkcoach 3. gegevens zorgaanbieder (productomschrijving)	medewerkers wijkteams	n.v.t.	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	CVS
Procedure vrijwillige gesloten plaatsing.	Het verzoeken om machtiging gesloten plaatsing en het afgeven van de beschikking gesloten plaatsing.	Jeugdwet	Stichting en college	jeugdigen en ouderlijk gezag	NAW, BSN, gezondheidsgegevens inwoner	1. wijkcoach 2. gedragswetenschapper 3. gecertificeerde instellingen 4. Raad voor de Kinderbescherming	n.v.t.	neen	Jeugdwet: 15 jaar	CVS
Procedure kinderbeschermingsmaatregel (MUHP, (V)OTS)	Het verzoeken tot het doen van een onderzoek door de Raad voor de Kinderbescherming en het afgeven van een beschikking gedwongen kader.	Burgerlijk Wetboek	Stichting en college	jeugdigen en ouderlijk gezag	NAW, BSN, gezondheidsgegevens inwoner, beschikking Rechtbank	1. wijkcoach 2. gedragswetenschapper 3. gecertificeerde instellingen 4. Raad voor de Kinderbescherming 5. medewerker Veiligheidshuis gemeente Arnhem	n.v.t.	neen	Jeugdwet: 15 jaar	CORV
Het opnemen van een jongere in de verwijsindex	Vroegtijdige signalering, sluitende aanpak, informatie verzamelen	Jeugdwet	Stichting en college	jeugdigen en ouderlijk gezag	NAW, BSN	1. wijkcoach 2. Veilig Thuis 3. Jeugdbescherming	n.v.t.	neen	2 jaar	VIRA

Meldcode kindermishandeling en huiselijk geweld	Aanpak kindermishandeling en huiselijk geweld	Wet verplichte meldcode huiselijk geweld en kindermishandeling	Stichting en college	inwoners gemeente Arnhem	NAW, BSN, gezondheidsgegevens inwoner	1. wijkcoach 2. Veilig Thuis 3. Jeugdbescherming	n.v.t.	neen	WMO en Jeugdwet: 15 jaar	CVS
Deelname aan Overleg en Zorg Overleg (OZO)	Vroegtijdige signalering, sluitende aanpak	Algemeen belang	Stichting en college	inwoners gemeente Arnhem	NAW	1. wijkcoach 2. medewerker Veiligheidshuis gemeente Arnhem	n.v.t. Er is wel een samenwerkingsdocument Stichting Wijkteams Arnhem en OZO (d.d. 1-2-2017)	neen	WMO en Jeugdwet: 15 jaar Wet op de Gemeentelijke Schuldhulpverlening: 5 jaar Leerlingenvervoer: 10 jaar.	CVS
Bedrijfsvoeringsprocessen										
Verwerken van de personeelsadministratie	Behandelen van personeelszaken	Overeenkomst	Stichting	Medewerkers	Arbeidsgerelateerde gegevens (NAW, BSN, werkprestatie, verzuim/verlof en arbeidsconflict)	1. teamleiders-bestuurders 2. staf-ondersteuners Stichting	AAG Payroll & HRM services b.v. verwerkersovereenkomst d.d.4/11 juni 2018	neen	7 jaar	Youforce/Beaufort
Verwerken van de salarisadministratie	Uitbetalen van loon	Overeenkomst	Stichting	Medewerkers	Etiketgegevens (NAW, geboortedatum en medicatiegegevens)	1. teamleiders-bestuurders 2. staf-ondersteuners Stichting	AAG Payroll & HRM services b.v. verwerkersovereenkomst d.d. 4/11 juni 2018	neen	7 jaar	Youforce/Beaufort
Verwerken loonbelasting	Loonbelasting	Overeenkomst	Stichting	Medewerkers	Financiële gegevens (NAW, BSN, salaris en bankgegevens)	Belastingdienst	n.v.t.	neen	7 Jaar	Exact Financials
Verwerken verzuimgegevens tbv vangnet	Uitbetalen van loon	Overeenkomst	Stichting	Medewerkers	Arbeidsgerelateerde gegevens (Identiteit, NAW, BSN, werkprestatie, verzuim/verlof en arbeidsconflict)	1. teamleiders-bestuurders 2. staf-ondersteuners Stichting 3. UWV/Bedrijfsarts	n.v.t.	neen	7 jaar	Youforce/Beaufort
Het opstellen van rapportages mbt de personeelsinzet en financiën.	Inzicht in kosten en personeelsverloop	Overeenkomst	Stichting	Medewerkers	NAW, BSN, financiële gegevens,	1. teamleiders-bestuurders 2. staf-ondersteuners Stichting	AAG Financial Services b.v. verwerkersovereenkomst d.d. 4/11 juni 2018	neen	7 jaar	1. Exact Financials 2. ProActive

.

Statuut van de Functionaris voor Gegevensbescherming van de Stichting Wijkteams Arnhem

De Stichting heeft een Functionaris voor Gegevensbescherming (FG). De FG houdt toezicht op de naleving van privacy-wetgeving door de (medewerkers van de) Stichting en legt rechtstreeks verantwoording af aan het bestuur;

Het bestuur van de Stichting:

- betrekt de FG tijdig en naar behoren bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- ondersteunt de FG bij de uitvoering van zijn taken en zal hem toegang verschaffen tot persoonsgegevens en verwerkingsactiviteiten;
- stelt de FG de nodige middelen ter beschikking voor de vervulling van zijn taken en het in stand houden van zijn deskundigheid;
- zal de FG geen instructies geven met betrekking tot de uitvoering van zijn taken; ontslag als gevolg van de uitoefening van zijn taken zal niet plaatsvinden.

De FG:

- informeert het bestuur over privacy-wetgeving en - aangelegenheden;
- adviseert het bestuur gevraagd en ongevraagd inzake privacy-aangelegenheden;
- ziet toe op de naleving van privacywetgeving en - beleid door medewerkers van de Stichting;
- organiseert trainingen voor medewerkers ten behoeve van het privacy-bewustzijn;
- is aanspreekpunt voor de Autoriteit Persoonsgegevens;
- heeft een ombudsfunctie voor betrokkenen bij klachten over privacy;
- zorgt in overleg met de FG van de gemeente Arnhem voor het opstellen van een Plan van Aanpak, zoals genoemd in de overeenkomst met de gemeente Arnhem;
- heeft periodiek overleg met de zakelijk medebestuurder als portefeuillehouder privacy en de CISO;
- is gehouden tot geheimhouding / vertrouwelijkheid;
- bepaalt samen met de CISO en de zakelijk medebestuurder hoe op te treden in geval van een beveiligingsincident / datalek en zal in overleg met de CISO voor een eventuele melding bij de Autoriteit Persoonsgegevens zorgdragen;
- coördineert de totstandkoming van het verwerkingsregister als bedoeld in artikel 30 AVG;
- doet jaarlijks verslag van de wijze waarop de Stichting voldoet aan de regelgeving op het gebied van gegevensbescherming.

Bijlage 2 Statuut Functionaris Gegevensbescherming

Bijlage 3 Werkafspraken Privacy

Privacy

Werkafspraken Stichting Wijkteams Arnhem, maart 2018

Algemeen

1. Het is als wijkcoach belangrijk om ondersteuning te bieden aan een inwoner vanuit een vertrouwensrelatie. In onze rol past geen handhavende taak.
2. Wijkcoaches overleggen met collega's, juridische zaken, teamleider als ze dilemma's hebben op het gebied van privacy.
3. Wijkcoaches en teamleiders spreken elkaar en derden aan op gedrag in privacy-zaken.

Contact inwoner

4. Bij ieder eerste huisbezoek wordt de folder "Wijkteams; steun en advies dichtbij" en de folder "informatie van de wijkteams over; privacyregeling, klachtenregeling, bezwaar en beroep en vertrouwenspersoon" uitgereikt en toegelicht.
5. Contact met de inwoner vindt plaats op vraag van de inwoner, of outreachend na signaal van derden, maar altijd met medeweten van de inwoner.

Informatie verkrijgen

6. Persoonsgegevens worden alleen voor een bepaald doel verzameld en alleen die gegevens die noodzakelijk zijn voor dat doel.

7. Wijkteams werken met gegevens die afkomstig zijn van de inwoner zelf. Uitzondering hierop bestaat als de veiligheid van één of meerdere inwoners of wijkcoach in het geding is/kan zijn.

Delen van informatie

8 Het delen van informatie met derden kan alleen met toestemming van de inwoner, deze toestemming wordt schriftelijk vastgelegd in MPOP/afspraken.
Het uitgangspunt is dat we niet over inwoners spreken maar met.

9. Wijkteams geven geen informatie aan derden op de checkvraag of inwoner bij hen bekend is. (uitzondering: Veiligheidshuis, Veilig Thuis en OZO)
   - VHH: vraagt bij een vast contactpersoon van het wijkteam na of een inwoner bekend is, voorafgaand aan bespreken van een melding in het VHH.
   - VT: partijen die benaderd worden door VT moeten antwoord geven op de vragen, bijv. op de vraag "zijn jullie betrokken?" VT heeft recht om deze informatie op te halen (is juridisch vastgelegd)
   - OZO: De o**verlastcoördinator** checkt - bij alle nieuwe aanmeldingen - bij de teamleider / vast contactpersoon van het wijkteam of inwoner bekend is/wijkteam betrokken is (ja/nee vraag).
     Het **wijkteam** checkt, als er sprake is van één of meerdere van onderstaande componenten, of een inwoner bekend is bij de Overlastcoördinator (is er al plan van aanpak vanuit het OZO ?) of legt de casus anoniem voor bij de overlastcoördinator of checkt of we elkaar kunnen aanvullen als er sprake is van:

o vermoeden of signalen van overlast
o vermoeden van meervoudige problematiek
o vermoeden van (of feitelijk) een eerder drang of dwang traject of hulpverlening onder voorwaarden.
o inwoner is sterk gefocust op bespreken van hulpvraag op 1 leefgebied, wil niet praten over mate van zelfredzaamheid op andere gebieden.
o zorg mijdend gedrag
o en verder bij alle casuïstiek die “onderbuik” gevoelens oproept

- Het wijkteam participeert aan de OGGZ tafel en de OGGZ tafel jeugd. De VGGM organiseert en faciliteert deze tafels waar meerdere partijen zijn aangesloten. Het doel is een integrale ketenaanpak voor de doelgroep te bewerkstelligen.

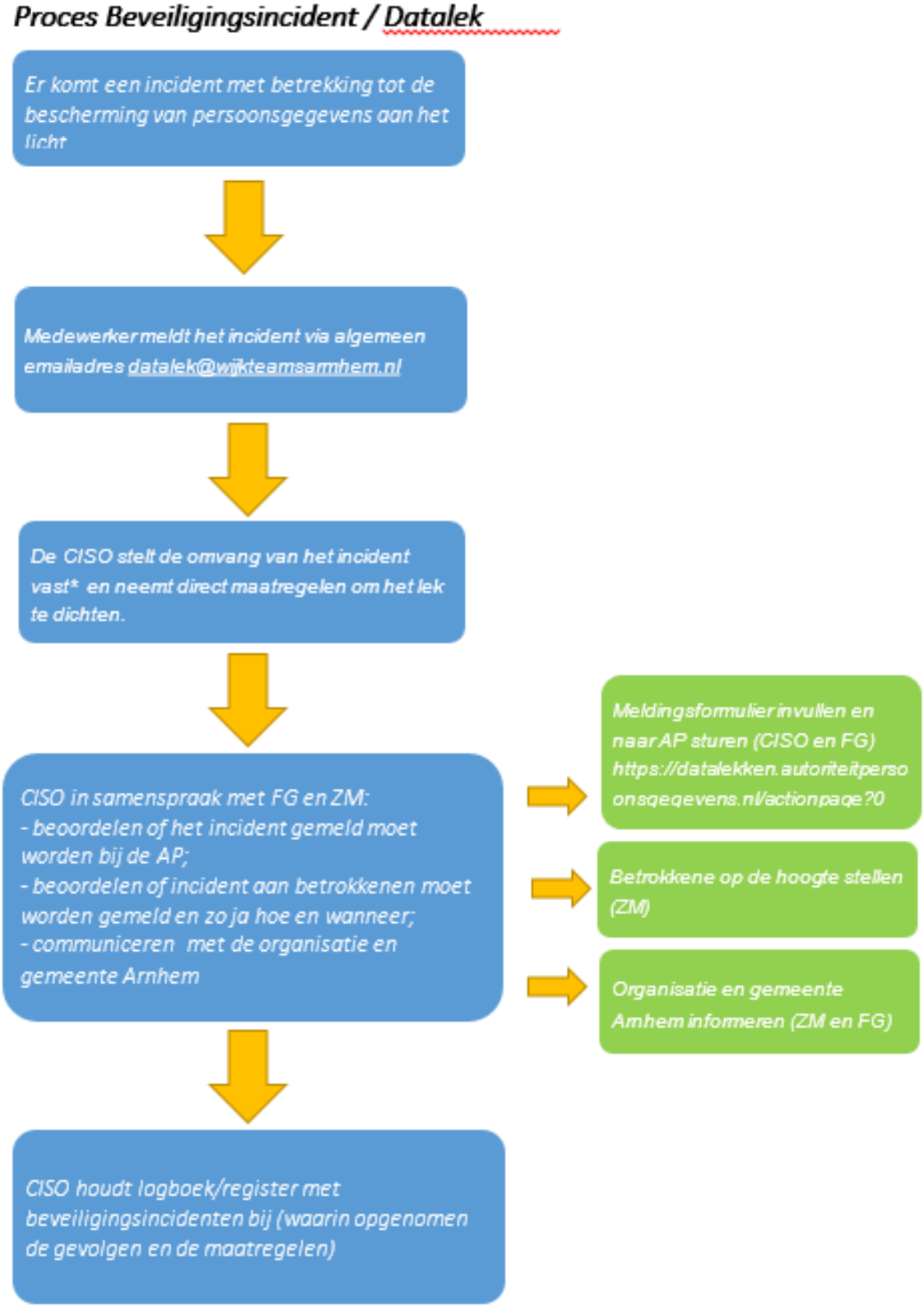
10. Er wordt niet gepraat over, maar met inwoners (en hun netwerk), tenzij de veiligheid van de inwoner of zijn/haar omgeving in het gedrang komt.
11. Casuïstiek over inwoners wordt anoniem besproken in de wijkteams. Ook als externe partijen uitgenodigd zijn bij casuïstiek. Denk bv aan leden van de expertisepool.
12. Indien de locatie van het wijkteam wordt bezocht door een inwoner of externe partijen, spreken de coaches niet over casuïstiek.
13. Hoe gevoeliger de informatie, des te bewuster wijkcoaches afwegen welke manier van communiceren wordt gebruikt.
14. Whatsapp is geen middel om privacygevoelige informatie te delen, zoals namen, NAW gegevens of ingezette zorg.
15. Online MPOP: coach kan alleen informatie opnemen met toestemming van de persoon die het betreft. Denk aan persoonlijke info van/over ouders, en info van derden (opnemen e-mails als contactjournaals: afzender moet expliciet toestemming geven voor opnemen letterlijke informatie)
16. Bij verhuizing van inwoners van wijk a naar b, mailen wijkcoaches elkaar onderling (via wijkteammail) met verzoek om contact op te nemen. Er wordt daarbij geen privacygevoelige informatie gedeeld. Zo voorkomen we dat er via de wijkteammail privacygevoelige info met alle coaches gedeeld wordt.
17. Bij zorgen rondom veiligheid over de inwoner en/of zijn kinderen hanteren wijkcoaches bij hun afweging omtrent delen van informatie de meldcode huiselijk geweld en kindermishandeling.

Jeugd

18. Rechtspositie ouders en jeugdigen m.b.t. Inlichten/ informatie verstrekken:
    - Jeugdige onder de 12 jaar: coach moet info verstrekken aan ouders met gezag of voogd.
    - Jeugdige tussen 12 en 16 jaar: zowel de jeugdige inlichten als de ouders
    - Jeugdige vanaf 16 jaar: alleen de jeugdige zelf inlichten; slechts met toestemming van de jeugdige kan de coach ook de ouders met gezag of voogd inlichten. In geval de jeugdige niet in staat is tot een redelijke waardering van zijn belangen, dan wordt de info wel verstrekt aan de ouders met gezag of de voogd
    - Geen info verstrekken als dit “ernstig nadeel” zou opleveren voor de ouders of de jeugdige. Altijd 4-ogen principe toepassen bij een dergelijk besluit.
19. Toestemmingsvereiste voor het inzetten van jeugdhulp:
    - Onder de 12 jaar: toestemming nodig van beide ouders met gezag of van de voogd
    - Tussen 12 en 16 jaar: zowel de jeugdige als de ouders met gezag of de voogd moeten instemmen
    - Vanaf 16 jaar: alleen toestemming van de jeugdige zelf nodig (tenzij jeugdige niet in staat is tot een redelijke waardering van zijn belangen, dan toestemming ouders met gezag of voogd nodig)
    - 18 jaar en ouder: alleen toestemming jeugdige nodig. Uitzondering: jeugdige staat onder curatele/ heeft mentor. Dan toestemming curator/mentor nodig.

Bijlage 4 Proces Datalekken

/



1. Er komt een incident met betrekking tot de bescherming van persoonsgegevens aan het licht. Er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek kan het gevolg zijn van een technisch beveiligingsprobleem (uitgelekte computerbestanden), maar het kan ook om een menselijke fout gaan, zoals het ergens laten liggen van een gevoelig dossier (in papieren vorm of in de vorm van een laptop of een USB-stick bijvoorbeeld) of het verzenden van een e-mail naar een verkeerd adres. Een medewerker van het wijkteam kan een dergelijke situatie zelf ontdekken of krijgt dit van een inwoner te horen.

2. Medewerker meldt het incident onmiddellijk na het ontdekken via het algemeen emailadres datalek@wijkteamsarmhem.nl De melding moet duidelijk weergeven wat er is gebeurd en om welke soort gegevens het gaat. De CISO (Ludo Klein Holte) krijgt de melding binnen en zal vervolgens contact met de medewerker leggen om meer duidelijkheid over de ontstane situatie te krijgen. De CISO informeert de Functionaris voor de Gegevensbescherming (FG) en de Zakelijk Medebestuurder (ZM) direct over het datalek.

3. De CISO stelt de omvang van het incident vast en neemt direct maatregelen om het lek te dichten: De CISO zal bij de beoordeling van het incident, samen met de functioneel beheerder (Gökçe en Frank) een onderzoek doen naar de volgende vragen (deze opsomming is gebaseerd op de gegevens die de AP vraag bij een melding)

   - wat is de (vermeende) oorzaak van het incident;
   - wat is het (vooralsnog bekende en/of te verwachten) gevolg;
   - wat is de (voorgestelde) oplossing;
   - hoe groot is het aantal personen waarvan gegevens betrokken zijn bij het incident (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij het incident);
   - een omschrijving van de groep personen van wie gegevens betrokken zijn bij het incident;
   - het soort of de soorten persoonsgegevens die betrokken zijn bij het incident;
   - de datum waarop het incident heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen het incident heeft plaatsgevonden);
   - de datum en het tijdstip waarop het incident bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
   - of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
   - wat de reeds ondernomen maatregelen zijn om het incident te beëindigen en om de gevolgen van het incident te beperken.

4. Als duidelijk is wat de aard en omvang van het incident is, dan neemt de CISO contact op met de FG en de ZM om samen te bepalen of:
   - het datalek gemeld moet worden bij de AP;
   - het datalek aan betrokkenen moet worden gemeld en zo ja hoe en wanneer.

   Melden aan de Autoriteit Persoonsgegevens is nodig als het waarschijnlijk is dat de inbreuk op de bescherming van persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

   Melden aan betrokkenen is daarnaast nodig indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

   Het datalek zal door de ZM aan de eigen organisatie worden gecommuniceerd en de FG zal de FG van de gemeente Arnhem op de hoogte stellen. De FG van de gemeente Arnhem zal de CISO van de gemeente Arnhem informeren.

5. De CISO houdt een logboek/register met beveiligingsincidenten bij (waarin zijn opgenomen de gevolgen en de maatregelen). Afgeronde onderzoeken naar datalekken worden hierin opgenomen. Een link naar dit register zal op de website worden opgenomen. De CISO zorgt ervoor dat deze link naar een actueel register verwijst.