Privacybeleid

Zorggroep Sirjon

Auteur: Bas Keijzer
Datum: v1.06, 12 juni 2019
Status: Vastgesteld RvB

Inhoud

1 Inleiding

Op 1 januari 2016 is de Wet bescherming persoonsgegevens aangescherpt, zie referentie [1]. Organisaties hebben een meldplicht bij datalekken. Bovendien zijn de boetes fors verhoogd en zijn het bestuurlijke boetes geworden. Daarom heeft de stuurgroep ict ondergetekende als functionaris gegevensbescherming (FG) aangesteld en aangemeld voor de gehele zorggroep, te weten Siloah, SVRO en DCS.

Dit document beschrijft het privacybeleid binnen Sirjon. Er worden twee soorten procedures beschreven:

1. Procedures verwerkers (hoofdstuk 3)
2. Procedures melding datalekken (hoofdstuk 6)

Privacybeleid valt binnen het in referentie [3] vastgestelde informatiebeveiligingsbeleid.

Bas Keijzer, 23-2-2016

Bij versie 1.04
Op 25 mei 2018 wordt in de gehele EER (EU plus Noorwegen, IJsland en Liechtenstein) de AVG (Algemene verordening gegevensbescherming) van kracht. Hiervoor zijn een aantal aanvullende procedures nodig. Deze zijn in deze versie toegevoegd.
Tevens is de rol van de stuurgroep ict vervangen door de Raad van Bestuur (RvB), aangezien de FG rechtstreeks aan de RvB rapporteert.

Bas Keijzer, 31-8-2017

1.1 Leeswijzer

Wie	Lezen	Toelichting
Alle medewerkers	Hoofdstuk 2, paragraaf 5.2 paragraaf 6.1	
Managers zorg, manager DCS RvB	Hoofdstuk 2, hoofdstuk 3, hoofdstuk 4, hoofdstuk 5, paragraaf 6.1	
ICT	Hoofdstuk 3	
Cluster K&V	Geheel	

2 Definities privacybeleid

2.1 Datalek

Een datalek is een beveiligingsincident waarbij persoonsgegevens **buiten je bereik** zijn geraakt. Voorbeelden:

- Cliëntrapportage verstuurd naar onjuist mailadres; bijvoorbeeld naar de verkeerde cliëntvertegenwoordiger.
- Vertrouwelijke gegevens op verkeerde printer afgedrukt, bijvoorbeeld op een andere locatie, en het document is verdwenen.
- Verlies/diefstal mobiele telefoon
- Openen van mail met virus, bijvoorbeeld een mail van een bank of een betalingsherinnering. Door sommige van deze virussen worden alle Word- en Excel-bestanden onbruikbaar gemaakt.
- Bestand met vertrouwelijke informatie kwijt geraakt. Je weet immers niet meer waar die bestanden zijn. Het zou kunnen zijn, dat ze per ongeluk op een plaats opgeslagen zijn, waar onbevoegden erbij kunnen.

Datalekken moeten altijd gemeld worden bij de FG. Deze analyseert vervolgens welke vervolgacties noodzakelijk zijn. Zie hoofdstuk 6.

2.2 Betrokkene en (bijzondere) persoonsgegevens

De AVG definieert een **betrokkene** als een persoon van wie persoonsgegevens en/of bijzondere persoonsgegevens verzameld worden.
Voor Sirjon zijn dit bijvoorbeeld: cliënten, medewerkers, wettelijk vertegenwoordigers, huurders, vrijwilligers, oud-medewerkers, sollicitanten, leveranciers, bezoekers, enz.

Persoonsgegevens is *alle* informatie die iets zegt over de identiteit over een betrokkene, bijvoorbeeld naam, e-mailadres, geboortedatum, enz.

Bijzondere persoonsgegevens zijn: ras/etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van vakbond, gezondheid, seksueel gedrag of gerichtheid. (Onderstreepte categorieën zijn voor Sirjon van toepassing).

Deze bijzondere persoonsgegevens zijn vatbaar voor discriminatie en moeten daarom extra beschermd worden.

2.3 Vertrouwelijkheidsgraden

We onderscheiden drie vertrouwelijkheidsgraden:

Graad	*Informatie*	*Applicaties*	*Vertrouwelijkheid*
1.	Bedrijfsinformatie	diversen	vertrouwelijk
2.	Personeelsinformatie	Profit; Rooster	persoonsgegevens
3.	Cliëntinformatie	ECD Cliëntenzorg	persoonsgegevens + bijzondere persoonsgegevens

3 Procedures verwerkers

3.1 Definities

De AVG maakt onderscheid tussen **verwerkingsverantwoordelijke** en **verwerker** (art. 4).

Sirjon is de **verwerkingsverantwoordelijke**, omdat zij 'doel en middelen' van de verwerking bepaalt. (Onder 'middelen' wordt hier de inrichting verstaan, niet 'middelen' in de betekenis van bronnen, zoals machines, geld, mensen, computers, enz.)

Er zijn verschillende categorieën medewerkers die toegang hebben tot persoonsgegevens die onder verantwoordelijkheid van Sirjon verwerkt worden. Afhankelijk van de categorie wordt er een overeenkomst opgesteld om de vertrouwelijkheid van de persoonsgegevens te waarborgen, te weten:

Categorie	*Beschrijving*	*Overeenkomst*
Interne medewerker	- Dienstverband bij Sirjon	Geen aparte overeenkomst: geheimhouding is onderdeel van arbeidsovereenkomst.
Externe medewerker	- Geen dienstverband bij Sirjon - Gebruikt alleen Sirjon-applicaties voor toegang tot persoonsgegevens - Bijvoorbeeld: ZZP'ers, personeel dat door derden wordt ingezet (salarisadministrateur), vrijwilligers	Gedragscode inclusief verklaring geheimhouding (zie ref [7]).
Behandelaar	- Geen dienstverband bij Sirjon - Gebruikt alleen Sirjon-applicatie ECD voor toegang tot persoonsgegevens - Bijvoorbeeld: huisartsen, orthopedagogen	Behandelovereenkomst inclusief verklaring geheimhouding. (gezamenlijke verwerkings-verantwoordelijke volgens AVG art. 26). *Als de behandelovereenkomst geen geheimhoudingsverklaring bevat: aanvullende gedragscode.*
Verwerker	- Geen dienstverband bij Sirjon - Gebruikt eigen applicaties om diensten aan Sirjon te verlenen - Bijvoorbeeld: Geoutsourcete diensten (Afas, Adapcare, Van Essen)	Verwerkersovereenkomst (AVG art. 28:3) getekend door hoogst verantwoordelijken bij Sirjon (RvB) en bij de verwerker.

Van de verwerkers wordt in het register verwerkingsactiviteiten vastgelegd:
1. Contactgegevens
2. Geautoriseerde gebruiker(s)
3. Welke verwerkingen geautoriseerd zijn voor deze gebruiker(s)

3.2 Procedure nieuw account

De leidinggevende is verantwoordelijk welke medewerkers voor zijn/haar locatie(s) toegang hebben tot persoonsgegevens (Afas, ECD, Rooster).

De procedure voor aanvraag van een nieuw account voor niet-interne medewerkers is:
- De leidinggevende dient de aanvraag in bij de applicatiebeheerder.
- De applicatiebeheerder laat de vastgestelde overeenkomst opstellen, eventueel in overleg met de FG.
- De applicatiebeheerder maakt het nieuwe account aan (of laat deze aanmaken) en verstuurt de overeenkomst naar de FG. Deze wordt opgeslagen in het register verwerkingsactiviteiten.

3.3 Procedure controleren bestaande accounts

De procedure hiervoor is:
- De applicatiebeheerder controleert jaarlijks welke accounts er openstaan.
- Deze lijst wordt ter controle aan de verantwoordelijke leidinggevenden voorgelegd. Deze geeft aan welke accounts gehandhaafd blijven en welke gesloten kunnen worden.
- Accounts die 3 maanden niet gebruikt worden, worden automatisch gesloten.

4 Procedures cliëntportaal en cliëntenraden

4.1 Procedure gebruik cliëntportaal

Sirjon heeft twee cliëntportalen: één voor Siloah en één voor SVRO. Dit zijn beveiligde websites, waarmee de cliënt en/of (wettelijk) vertegenwoordiger op een eenvoudige manier gegevens uit het cliëntdossier kan raadplegen. Om gebruik te kunnen maken van die portalen, dient de cliënt en/of wettelijk) vertegenwoordiger de voorwaarden van het cliëntportaal te ondertekenen, zie referentie [5] en [6].
Het doel van deze voorwaarden is (onder meer) een praktische uitwerking te geven van de bepalingen van de AVG.

4.2 Procedure cliëntenraden

De vergaderstukken van de cliëntenraden bevatten geen namen van cliënten.

4.3 Procedure gebruik ECD op eigen apparatuur

Het ECD wordt online via een url ter beschikking gesteld.

Aangezien het ECD persoonsgegevens bevat (zowel reguliere als bijzondere), is buiten het Sirjon-netwerk twee-factor-authenticatie vereist. Naast de gebruikersnaam en het wachtwoord dient een steeds wijzigende sms-code ingevoerd te worden. Binnen het Sirjon-netwerk is allen gebruikersnaam en wachtwoord voldoende.

5 Procedures rechten van betrokkene

(Zie paragraaf 2.3| voor de definitie van betrokkene.)

5.1 Rechten van betrokkene

Elke betrokkene – dus iedere cliënt, medewerker, oud-medewerker, enz. – heeft krachtens de AVG (overweging 59-66, artikel 15-23) de volgende rechten:
- Recht op inzage: een kopie van alle persoonsgegevens die een organisatie van hem/haar bezit.
- Recht op informatie over de verwerking: wie (ontvangers), wat (welke gegevens), waar (opslag), wanneer (bewaartermijn), waarom (doel)
- Recht om de bron van zijn persoonsgegevens te kennen (indien niet zelf aangeleverd).
- Recht op correctie (objectief/subjectief, zie verderop) en verwijdering.
- Recht op opschorting van de verwerking.
- Recht op een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- Recht op gegevensoverdracht in machine-leesbaar formaat.

Het is niet de bedoeling om hier de hele verordening te kopiëren, maar wanneer een betrokkene gebruik maakt van één van deze rechten, bijvoorbeeld recht op inzage, dan moet de verantwoordelijke ook alle andere rechten noemen.

5.1.1 Responsetermijn

De betrokkene moet **binnen een maand** antwoord hebben op zijn aanvraag; of **drie maanden** voor een complex verzoek, maar dan moet binnen een maand wel aangegeven worden waarom dat langer gaat duren.
De verantwoordelijke (Sirjon) heeft het recht om het verzoek om inzage nader te laten **specificeren** door de betrokkene. Zij kan vragen voor welk doel de betrokkene de gevraagde gegevens nodig heeft. Dit schort overigens de responsetermijn niet op, maar biedt wel de gelegenheid om de inzage op maat te maken.

5.1.2 Beperking

Bovengenoemde zijn geen absolute rechten.

Het recht op **inzage** kan niet uitgeoefend worden:
- voor persoonlijke aantekeningen. Deze aantekeningen moeten dan wel echt persoonlijk zijn. Zo snel als ze met anderen (bijvoorbeeld collega's of leidinggevenden) gedeeld zijn, of in een dossier worden opgeslagen, vallen ze wel onder het inzagerecht.
- bij MIC en MIM meldingen. Deze mogen slechts door een kleine groep specifiek genoemde personen ingezien worden.
- als er een andere betrokkene genoemd wordt. Dit zou immers zijn privacy schenden.

Het recht op **correctie** heeft twee aspecten: objectief en subjectief. Objectieve onjuistheden, zoals spelfouten, verkeerd adres, enzovoorts, dienen rechtstreeks gecorrigeerd te worden. Subjectieve onjuistheden, die het gevolg zijn van verschil van mening over een bepaalde zaak, hoeven niet gecorrigeerd te worden. Wel heeft de betrokkene het recht er zijn eigen zienswijze of een second opinion tegenover te stellen.

Het recht op **verwijdering** wordt ingeperkt door de wettelijke bewaarplicht van bijvoorbeeld dienstverbandgegevens of zorghandelingen. Deze wettelijke bewaarplicht heeft voorrang boven het recht op verwijdering.

5.2 Procedure verzoeken door betrokkenen

Let op: De AVG stelt slechts één voorwaarde aan de wijze waarop verzoeken van betrokkenen binnenkomen: schriftelijk. Het maakt niet uit waar of bij wie het verzoek wordt ingediend. Dat kan dus op elke plaats in de organisatie zijn. Omdat de responsetermijn slechts één maand is en het inwilligen van een verzoek een tijdrovende klus kan zijn, moet dit zo snel mogelijk aan de juiste partij worden doorgegeven.

Verzoeken
Het verzoek wordt door iedereen in de organisatie doorgestuurd naar diens leidinggevende en naar privacy@sirjon.nl . Deze komt bij de FG of dienst vervanger terecht.

Opvolging
De FG bepaalt welke actie er uitgezet moet worden en stuurt de applicatiebeheerder(s) aan.
De FG beantwoordt het daadwerkelijke verzoek naar de betrokkene.

Rollen en verantwoordelijkheden

Rol	*Wie*	*Verantwoordelijkheid*
Betrokkene	Zie paragraaf 2.3|	Dient verzoek in Krijgt binnen een maand response Compleet verzoek is binnen drie maanden afgehandeld
Ontvanger	Alle medewerkers Sirjon	Ontvangt verzoek Stuurt verzoek door naar leidinggevende en naar privacy@sirjon.nl
Leidinggevende		Zorgt dat verzoek naar privacy@sirjon.nl wordt gestuurd. Wordt geïnformeerd over response.
FG		Bepaalt welke actie uitgezet wordt. Geeft response aan betrokkene. Informeert leidinggevende over response.
Applicatiebeheerder		Voert actie uit Koppelt deze terug naar de FG

6 Procedures melding datalekken

6.1 Procedure interne melding datalek

Medewerkers van Sirjon moeten een datalek altijd en direct melden.

Melden
Het melden gaat via Insite. Kies daar Meldingen > Meld datalek.
Vul vervolgens alle velden in.
Na het aanmaken van de melding komt deze als taak bij de FG terecht.

Opvolging
De FG registreert deze melding en de vervolgacties in het datalekkenregister.
De FG bepaalt of de melding doorgestuurd wordt naar de Autoriteit Persoonsgegevens en betrokkene. Zie paragraaf 6.3. hoe deze weging plaatsvindt. De uitkomst van deze weging wordt meegedeeld aan de melder.
Daarna vindt de melding plaats aan de Autoriteit Persoonsgegevens en/of de betrokkene.

Reparatie van het beveiligingslek gebeurt in overleg met de RvB, de leidinggevende en eventueel andere betrokkenen.
Rapportage vindt plaats aan de RvB.

Rollen en verantwoordelijkheden

Rol	*Wie*	*Verantwoordelijkheid*
Melder	Alle medewerkers Sirjon	Voert melding uit Wordt geïnformeerd over opvolging melding
FG		Bepaalt opvolging melding Informeert melder, leidinggevende en rapporteert aan RvB. Overlegt met leidinggevende en RvB over reparatie
RvB		Wordt geïnformeerd over opvolging melding Wordt geraadpleegd over reparatie

6.2 Procedure externe melding datalek

Verwerkers moeten conform de verwerkersovereenkomst (referentie [4]) elk datalek binnen 72 uur melden.

Melden
De melding wordt per mail verstuurd naar privacy@sirjon.nl.
In deze melding staat in ieder geval:
- Dat er een lek is geweest.
- Wat de oorzaak van het lek is, voor zover bekend.
- Wat het gevolg is van het lek, voor zover bekend en te verwachten.
- Wat de oplossing/reparatie is.

Opvolging
De FG registreert deze melding en de vervolgacties in het datalekkenregister.
De FG bepaalt of de melding doorgestuurd wordt naar de Autoriteit Persoonsgegevens en betrokkene. Zie paragraaf 6.3. hoe deze weging plaatsvindt. De uitkomst van deze weging wordt meegedeeld aan de melder.
Daarna vindt de melding plaats aan de Autoriteit Persoonsgegevens en/of de betrokkene.
De RvB wordt in het periodieke overleg geïnformeerd over de melding en de opvolging.

Maximaal een maand na de melding wordt een audit uitgevoerd naar de voorgestelde reparatie.

Rollen en verantwoordelijkheden

Rol	*Wie*	*Verantwoordelijkheid*
Verwerker	Alle geregistreerde verwerkers	Voert melding uit Wordt geïnformeerd over opvolging melding
FG		Weegt of betrokkene geïnformeerd wordt Rapporteert RvB Initieert audit naar voorgestelde reparatie
RvB		Wordt geïnformeerd over melding, opvolging en audit na reparatie

6.3 Procedure opvolging interne of externe melding datalek

Als er een melding van een datalek binnenkomt, voert de FG de volgende procedure uit:

1. Maak de melding compleet
2. Is het een datalek?
3. Zo ja: bepaal of melding doorgestuurd moet worden aan de Autoriteit Persoonsgegevens.
4. Zo ja: bepaal of betrokkene ingelicht moet worden.
5. Stuur melding door naar Autoriteit Persoonsgegevens en/of betrokkene.
6. Bewaak reparatie van het datalek.

6.3.1 Maak melding compleet

De melding dient in ieder geval de volgende gegevens te bevatten:

- Wat de oorzaak van het lek is, voor zover bekend.
- Wat het gevolg is van het lek, voor zover bekend en te verwachten (omvang en impact).
- Welke stappen kunnen we direct nemen om de schade te beperken (noodreparatie).
- Wat is de definitieve oplossing/reparatie.
- Welke rechten heeft de betrokkene.
- Contactgegevens voor opvolging van de melding.

Omdat we binnen 72 uur moeten melden, mag het compleet maken van de melding niet te lang duren. Duurt het wel te lang om binnen de wettelijk verplichte termijn te melden, dan wordt eerst een voorlopige weging en eventuele melding uitgevoerd.

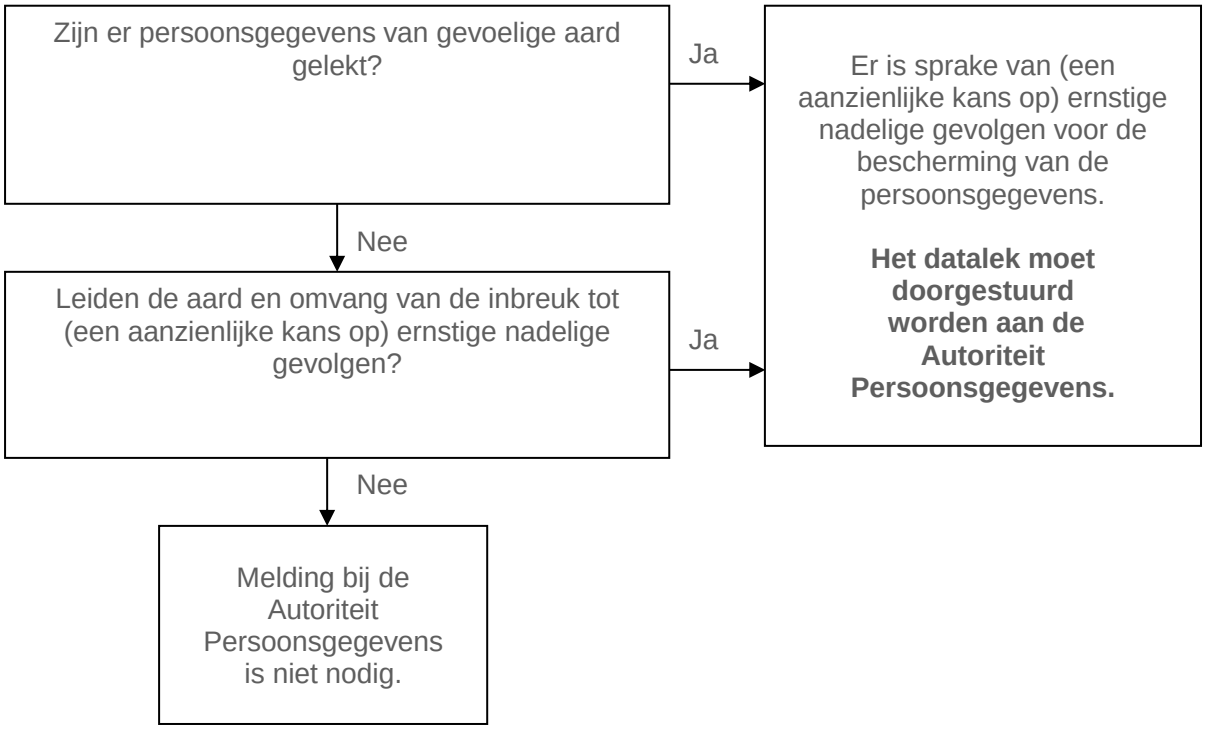
6.3.2 Is het een datalek?

De FG gaat na of de melding daadwerkelijk een datalek is.

Zie hoofdstuk 3 van referentie [2] voor meer informatie en toelichting over deze vragen.

6.3.3 Doorsturen naar Autoriteit Persoonsgegevens?

Is er sprake van een datalek, dan overweegt de FG of het lek doorgestuurd moet worden bij de Autoriteit Persoonsgegevens.

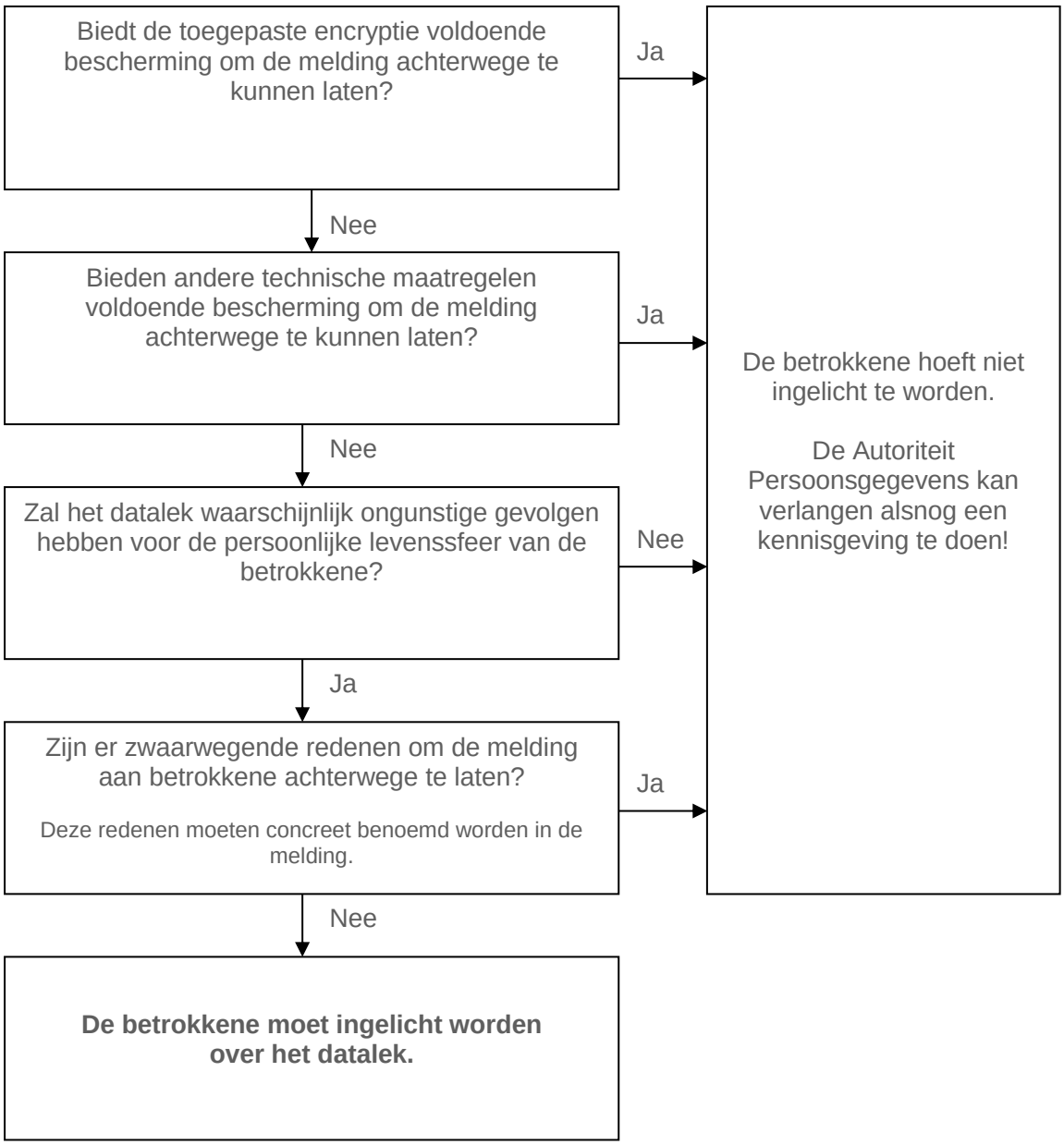


Zie hoofdstuk 4 van referentie [2] voor meer informatie over deze vragen.

Let op: Bij meldingen van een verwerker kan het voorkomen, dat de FG tot een andere uitkomst komt dan de verwerker. In dat geval wordt de melding toch doorgestuurd naar de Autoriteit Persoonsgegevens.

6.3.4 Betrokkene inlichten?

Wanneer de melding doorgestuurd moet worden bij de Autoriteit Persoonsgegevens, dan overweegt de FG of ook de betrokkene ingelicht moet worden.



Zie hoofdstuk 7 van referentie [2] voor meer informatie over deze vragen.

6.3.5 Uitvoeren meldingen

Eis is om binnen 72 uur te melden. Als we dan nog niet volledig zicht hebben op aard en omvang van het incident, doen we een voorlopige melding. Deze kan naderhand aangevuld of zelfs ingetrokken worden.

Het uitvoeren van de melding gaat als volgt:

- Betreft het een melding door een Sirjon-medewerker, dan worden eerst een aantal personen geïnformeerd.
- De FG zet de melding binnen 72 uur door naar de Autoriteit Persoonsgegevens via een webformulier op de site autoriteitpersoonsgegevens.nl. (Zie bijlage 1 van referentie [2] voor de gegevens in de melding).
- In overleg met de melder en RvB wordt een melding aan betrokkene vastgesteld en uitgevoerd. (Zie hoofdstuk 8 van referentie [2] voor toelichting). In deze melding staat in ieder geval:
    - De aard van het datalek
    - Waar betrokkene meer informatie kan krijgen over het datalek (bijvoorbeeld bij de manager zorg, de RvB of de FG).
    - De maatregelen de we betrokkene aanbevelen om negatieve gevolgen van de inbreuk te beperken.

6.3.6 Reparatie van het datalek

De FG dient toe te zien, dat het beveiligingslek is gerepareerd binnen de volgende termijnen:

- Een provisorische reparatie: zo spoedig mogelijk
- Een definitieve reparatie: binnen 1 maand.

7 Referenties

[1] *Wet bescherming persoonsgegevens*, http://wetten.overheid.nl/BWBR0011468/2016-01-01
[2] Autoriteit Persoonsgegevens, *De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)*, 8 december 2015
[3] Simon van der Weijden e.a., *Informatiebeveiligingsbeleid Zorggroep Sirjon*, versie 1.03, 2 oktober 2014
[4] Verwerkersovereenkomst
[5] Voorwaarden Cliëntportaal 'Mijn Siloah'
[6] Voorwaarden Cliëntportaal 'Mijn SVRO'
[7] Gedragscode gebruik ict-faciliteiten

8 Documenthistorie

Datum	***Versie***	***Auteur***	***Wijziging***
23-2-2016	1.00	Bas Keijzer	Initieel
15-3-2016	1.01	Bas Keijzer	Opmerkingen stuurgroep ict verwerkt + uitbreiding
24-8-2016	1.02	Bas Keijzer	idem (stuurgroep overleg datalekken)
25-11-2016	1.03	Bas Keijzer	Vastgesteld door CMT
25-5-2018	1.04	Bas Keijzer	Aanpassing n.a.v. AVG
22-1-2019	1.05	Bas Keijzer	Vastgesteld door werkgroep privacy
1-5-2019	1.06	Bas Keijzer	Tekstuele aanpassing
12-6-2019			Ongewijzigd vastgesteld door RvB