RAADSINFORMATIEBRIEF
19R.00794

Van : college van burgemeester en wethouders
Datum : 15 oktober 2019
Portefeuillehouder(s) : Wethouder Noorthoek
Portefeuille(s) : jeugdhulp
Contactpersoon : A. van der Ploeg
Tel.nr. : 8283
E-mailadres : ploeg.a@woerden.nl

Onderwerp:
voortgang onderzoeken en verbeterplan Samen Veilig Midden Nederland (SVMN)

Kennisnemen van:

De stand van zaken mbt het onderzoek nav het datalek van SVMN en het verbeterplan van SVMN.

Inleiding:

Tijdens een raadsinformatieavond van 16 april 2019 bent u oa geïnformeerd over een omvangrijk datalek bij Samen Veilig Midden Nederland (SVMN), zie Raadsinformatiebijeenkomst Veiligheid in Gezinnen (16-04-2019).

Ook heeft de fractie van VVD en van D'66 hierover in mei 2019 vragen gesteld, zie 19r.00427 rib beantwoording art. 42 vragen d66 inzake datalekken voorkomen (RIB 19R.00389 en RIB 19R.00427).

De afgelopen maanden werden hieromtrent verschillende onderzoeken en verbeterplannen uitgevoerd. Graag informeren wij u in deze raadsinformatiebrief over de uitkomsten van de onderzoeken naar het datalek van Samen Veilig, de verbetering van de aansturing van SVMN en de verbetering van de samenwerking van de keten rond jeugdbescherming.

Kernboodschap:

SVMN rapporteert over de onderzoeken en verbeterplannen aan de Ambtelijke Stuurgroep (ASG) die bestaat uit de managers Jeugd van de 6 jeugdzorgregio's in onze provincie. De ASG informeert het bestuurlijk overleg SAVE-Veilig Thuis (bestaande uit vertegenwoordigende wethouders jeugdhulp van de Utrechtse gemeenten en de Raad van Toezicht van SVMN) en het Breed Wethouders Overleg (alle wethouders jeugdhulp in de provincie Utrecht).

De uitkomsten van het onderzoek naar gegevensbeveiliging bij SVMN zijn op 27 september jl gepresenteerd aan het bestuurlijk overleg SAVE-Veilig Thuis op . Wethouder Duindam was hierbij als vertegenwoordigend wethouder aanwezig namens de Utrecht West gemeenten.

Naar aanleiding van het in april 2019 geconstateerde datalek bij SVMN hebben de gezamenlijke Utrechtse Jeugdregio's opdracht gegeven aan het COT/Aon (onafhankelijk instituut voor Veiligheids- en crisismanagement) om de gegevensbescherming bij SVMN te onderzoeken.
De onderzoekers COT/Aon hebben beoordeeld:

- hoe SVMN is omgegaan met de afhandeling van het datalek;
- hoe de informatiebeveiliging is ingericht binnen de organisatie van SVMN.

Op basis van de bevindingen van COT/Aon zijn 6 aanbevelingen geformuleerd voor SVMN. De conclusies en aanbevelingen vindt u in de managementsamenvatting van het onderzoeksrapport van het COT/Aon (zie bijlage 1, corsa 19.089337).

SVMN heeft constructief meegewerkt aan het onderzoek in goede interactie met het COT/Aon. De uitkomsten geven aan dat SVMN adequaat heeft gehandeld na constatering van het datalek. De onderzoekers hebben ook vastgesteld dat informatiebeveiliging beleidsmatig en organisatorisch is ingericht binnen SVMN. Zij signaleren dat daarin qua niveau en qua implementatie nog verdere stappen te zetten zijn. Het COT/Aon beveelt aan om de aansluiting met de relevante omgeving, zoals cliënten en opdrachtgevers, te versterken.

Er zijn naast deze aanbevelingen uit het onderzoek van COT/Aon ook andere ontwikkelingen waar opgaven voor SVMN uit voortvloeien. De onderzoeken van COT/Aon plaatsen we in het bredere kader van de veranderagenda van SVMN (zie https://www.samen-veilig.nl/wp-content/uploads/2019/05/Veranderagenda-Samen-Veilig-Midden-Nederland.pdf), namelijk:

- Versterken van het vertrouwen van cliënten in zorgvuldig handelen van SVMN;
- Blijvend bouwen aan het vertrouwen van burgers (meldingsbereidheid) en samenwerking met ketenpartners en opdrachtgevers;
- Verstevigen van het lerend vermogen van SVMN.

Financiën:

Nvt

Vervolg:

Over de uitkomsten van het onderzoek en de implementatie van de aanbevelingen hebben de samenwerkende Jeugdregio's – als opdrachtgever - nadere afspraken gemaakt met SVMN. De samenwerkende gemeenten in de provincie Utrecht nemen de aanbevelingen en de uitvoering zeer serieus en geven dit hoge prioriteit. SVMN koppelt de voortgang frequent terug aan de ASG en aan het Bestuurlijk Overleg, waarin wethouder Duindam namens de Utrecht West gemeenten in deelneemt.

Bijlagen:

Bijlage 1, onderzoeksrapport databeveiliging SVMN van COT/ Aon (corsa 19.089337)
Bijlage 2, raadsinformatiebrief gemeente Utrecht (corsa 19.089336)

De secretaris,

drs. M.H.J. van Kruijsbergen MBA

De burgemeester,

V.J.H. Molkenboer

COT | Instituut voor Veiligheids- en Crisismanagement
an Aon company

Gegevensbescherming door Samen Veilig Midden-Nederland

Onderzoek en aanbevelingen n.a.v. datalek 9 april 2019

Versiebeheer

Datum	Versie	Toelichting
12 juli 2019	Conceptversie	Ten behoeve van review door begeleidingsgroep en SVMN
30 augustus 2019	Tweede conceptversie	Verwerking review van begeleidingsgroep en SVMN
19 september 2019	Definitieve versie	Verwerking review van begeleidingsgroep

COT Instituut voor Veiligheids- en Crisismanagement – An Aon Company

Inhoudsopgave

1 Managementsamenvatting

Achtergrond

Op 9 april 2019 wordt bekend dat Samen Veilig Midden-Nederland (hierna: SVMN) getroffen is door een datalek van cliëntgegevens. Het datalek bij SVMN heeft geleid tot veel impact op cliënten, politieke en maatschappelijke aandacht en vragen/zorgen onder medewerkers van SVMN. Naar aanleiding van het datalek bij SVMN heeft de gemeente Utrecht namens de overige Utrechtse gemeenten een onafhankelijk onderzoek laten uitvoeren naar hoe SVMN met de persoonsgegevens en privacy van betrokken kinderen en gezinnen is omgegaan. De gemeente Utrecht heeft COT Instituut voor Veiligheids- en Crisismanagement (hierna: COT) gevraagd dit onderzoek uit te voeren. Dit onderzoek is gericht op het inzichtelijk maken van ervaringen, verklaringen, uitdagingen en lessen, zowel in relatie tot zaken die goed zijn verlopen alsook zaken waar vragen of twijfels over zijn of vraagstukken waar nog geen eerdere ervaring mee is.

Conclusie afhandeling datalek door SVMN

- Vanaf het begin dat SVMN op de hoogte is van het datalek heeft SVMN een juiste inschatting gemaakt dat dit incident verder gaat dan sec een datelek. SVMN oordeelde juist door dit incident als een crisis te bestempelen vanwege de grote impact op cliënten en een inbreuk op haar bestaansgrond als betrouwbare zorginstelling. SVMN heeft terecht vastgesteld dat deze brede impact vraagt om het optreden en maatregelen van haar Crisisteam.
- Voor de duiding van het datalek dient gezegd te worden dat het om een bijzonder datalek gaat. Bijzonder in de zin dat klokkenluiders voor een lange periode geprobeerd hebben om een statement te maken richting de maatschappij. Er is gericht gezocht naar gaten in het systeem van zorginstellingen om daarmee toegang te krijgen tot persoonsgevoelige cliëntgegevens.
- Het heeft SVMN veel tijd gekost heeft om erachter te komen wat er precies is gebeurd. Dit kwam doordat de expertise bij SVMN ontbreekt om digitaal te rechercheren en daardoor afhankelijk was van het onderzoek door een extern bureau. Wij vinden dat van SVMN niet verwacht mag worden dat zij de expertise en capaciteit in huis heeft om digitaal te rechercheren. Dat het onderzoeksproces langer duurde dan gewenst, past in lijn der verwachtingen.
- Het datalek is vakkundig afgehandeld door het datalek snel te dichten, een onderzoek in te stellen en externe technische en juridische expertise in te schakelen. Er is tijdig en conform de richtlijnen meerdere meldingen van het datalek gedaan bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens vindt dat zij voldoende op de hoogte is en bij ongewijzigde ontwikkelingen hoeft SVMN geen aanvullende meldingen meer te doen.
- SVMN is verantwoordelijk is voor het ontstaan van het datalek (ook al komt dat door een opeenstappeling van factoren) en de gevolgen voor cliënten die gedupeerd zijn. SVMN is en blijft verantwoordelijk voor goed beheer van persoonsgevoelige informatie.
- SVMN heeft geprobeerd zoveel als mogelijk alle betrokkenen te achterhalen en te informeren, maar is hierin niet geslaagd aangezien er geen toegang meer is tot contactgegevens van ex-cliënten. Het pleit voor SVMN dat zij snel externe expertise ingeschakeld hebben om vast te stellen hoe ver zij moet gaan om ook getroffen ex-cliënten te achterhalen en individueel te informeren. Wij verwachten van SVMN dat zij in dit verband ook haar opdrachtgevers (de gemeenten) betrekt bij deze overweging. Dit heeft zij niet gedaan. Daarnaast had SVMN een second opinion kunnen uitvoeren op het juridische advies. Dit had SVMN geholpen in haar verdere onderbouwing van de vervolgstappen op basis van het eerste juridische advies. Bij tegenstrijdige adviezen had SVMN dit bijvoorbeeld kunnen voorleggen aan haar Cliëntenraad en de gemeenten om daarover een gezamenlijk standpunt in te nemen. SVMN had hiertoe het initiatief kunnen nemen.

Conclusie huidige status informatiebeveiliging bij SVMN

- Beleid. Het beleid over informatiebeveiliging SVMN is momenteel aanwezig. Het beleid is echter te generiek van aard en vraagt om een duidelijke vertaling naar de context van SVMN, haar bestaansgrond en risico's. SVMN dient meer gebruik te maken van de potentie van het beleid door operationalisering daarvan zodat medewerkers beter geëquipeerd zijn voor dagelijkse uitdagingen rondom informatieveiligheid.
- Organisatie. In opzet is er een duidelijke rol- en taakverdeling voor informatiebeveiliging. SVMN levert merkbare inspanningen om informatiebeveiliging te implementeren en uit te voeren (de werking). Dit doet SVMN door beheersmaatregelen, processen en procedures in te richten. Er zijn nog wel nieuwe actoren (bijv. de Stuurgroep Informatieveiligheid) die nog duidelijker gepositioneerd moeten worden binnen informatiebeveiliging. Er wordt veel aandacht besteed aan het ontwikkelen van bewustwording onder medewerkers. Informatiebeveiliging kan robuuster worden door ook rekening te houden met nieuwe (ICT) ontwikkelingen en risico's.
- Risicobeheer. Het risicobeheer van SVMN is in de basis goed. Zeker met de aangescherpte risicobeoordeling van 2019. Het helpt SVMN om een basisniveau van informatiebeveiliging te definiëren in een basisset van technische maatregelen. Nu blijft het lastig om per situatie (risico, project, etc) vast te stellen of de juiste maatregelen zijn genomen en of dit voldoende is.
- Beveiligingsincidenten. De procedure voor het melden van veiligheidsincidenten is goed. Binnen SVMN is een hoge meldingsbereidheid, mede door de bewustwordingscampagnes. SVMN heeft goed zicht op het aantal informatiebeveiligingsincidenten. Wanneer SVMN naast de analyse van de aantallen een strategische analyse uitvoert over alle meldingen, stelt haar dat in staat om overkoepelende verbeteracties door te voeren.
- Toetsing. Er vindt geen structurel toetsing plaats binnen SVMN. Toetsing binnen SVMN heeft eerder het karakter van reflectie en interne afstemming dan controle op effectiviteit van maatregelen (leveren de maatregelen op wat ze moeten beogen?).

Bovenstaande kwalificaties horen bij een organisatie als SVMN die enkele jaren bezig is met informatiebeveiliging. SVMN heeft duidelijke stappen genomen en staat nu op het punt om informatiebeveiliging door te ontwikkelen.

Aanbevelingen voor balans werkbaarheid en informatiebeveiliging

1. Stel aanvullende specifieke uitgangspunten op voor het handelen van professionals die nodig zijn om een veilige, betrouwbare en passende werking van het gebruik van persoonsgevoelige gegevens te waarborgen. De betrokken medewerkers kunnen met de uitgangspunten vanuit hun hun eigen verantwoordelijkheid werken.
2. Verstevig het risicobeheer voor informatiebeveiliging door een duidelijker onderscheid tussen risico's die moeten worden aangepakt en de aanvaardbare risico's (de risicoacceptatie). Wees als SVMN transparant over aanvaardbare risico's, bijv. omdat het soms in het belang is van acute zorg en daarmee in het belang van de cliënten. Aanvaardbare risico's kunnen er ook zijn omdat dit de ketensamenwerking versterkt.
3. Versterk de borging van informatiebeveiliging door ook aandacht te besteden aan mogelijke verbeteringen (beleid, organisatie, risicobeheer). De winst zit in het zoeken naar geschikte technische maatregelen om risico's te voorkomen (privacy by design en privacy by default in reguliere én in acute situaties). Communiceer dit ook duidelijk naar de medewerkers en leg hierover als bestuur van SVMN verantwoording af aan Raad van Toezicht.
4. Betrek cliënten bij de doorontwikkeling van informatieveiligheid. Cliënten kunnen een belangrijke bijdrage leveren aan de normen en uitgangspunten voor het gebruik van persoonsgevoelige clientgegevens. Betrek bijvoorbeeld Clientenraad bij de bovengenoemde aanbevelingen.

5. Betrek opdrachtgevers van SVMN bij de doorontwikkeling van informatieveiligheid. Wees transparant in de keuzes die SVMN gaat maken bij de doorontwikkeling van informatieveiligheid. Leg ook duidelijk uit dat daadwerkelijke incidenten rond persoonsgevoelige gegevens -ondanks alle inspanningen- nooit volledig uit te sluiten zijn. Geef daarbij wel aan hoe het crisismanagement van SVMN ervoor zorgt dat SVMN effectief, tijdig en conform de verwachtingen van de buitenwereld handelen tijdens een crisisfase.
6. Organiseer crisisoefeningen over de brede impact van een omvangrijk datalek. Wees aantoonbaar voorbereid op grote en ongewenste incidenten rond persoonsgevoelige informatie. Organiseer jaarlijks een crisisoefening waarin de crisisvaardigheden voor de top risico's van SVMN ontwikkeld worden.

2 Inleiding

2.1 Achtergrond

Op dinsdag 9 april 2019 is Samen Veilig Midden-Nederland (hierna: SVMN) door RTL Nieuws geïnformeerd over een omvangrijk datalek binnen SVMN. Het datalek is ontstaan door het gebruik van oude emailadressen met een oude domeinnaam ('bjzutrecht.nl'). SVMN heeft vanaf 9 april direct maatregelen genomen. Het datalek bij SVMN heeft geleid tot veel impact op cliënten, politieke en maatschappelijke aandacht en vragen onder medewerkers van SVMN.

SVMN in het kort

SVMN komt in beeld als er zorgen zijn over de veiligheid van een kind of als er sprake is van geweld in de huiselijke sfeer. De medewerkers werken samen met cliënt, gezin, netwerk en lokale hulpverlening aan een oplossing. SVMN werkt met gebiedsgerichte teams die werkzaam zijn in de directe omgeving van de cliënt. De medewerkers werken aan de hand van de werkwijze Samenwerken aan Veiligheid (SAVE). De gebiedsgerichte SAVE-teams werken samen met de lokale teams. Daarnaast maakt Veilig Thuis Utrecht onderdeel uit van SVMN. Veilig Thuis is het advies- en meldpunt voor geweld in de huiselijke sfeer.

De medewerkers van SVMN bezoeken ongeveer 8.000 gezinnen op jaarbasis en werken voor 32 gemeenten in de provincies Utrecht en Flevoland. 580 medewerker werken vanuit vijf locaties: het hoofdkantoor in Utrecht en de regiokantoren in Nieuwegein, Amersfoort, Veenendaal en Almere.

2.2 Opdracht, doel en scope

Naar aanleiding van het datalek bij SVMN heeft de gemeente Utrecht mede namens de overige Utrechtse regio's een onafhankelijk onderzoek uitgevoerd naar hoe SVMN met de persoonsgegevens en privacy van betrokken kinderen en gezinnen is omgegaan. De gemeente Utrecht en SVMN tonen zich bewust van het belang van informatiebeveiliging en willen mede daarom maximaal inzicht in de afhandeling van het datalek door SVMN, de feitelijke situatie van informatiebeveiliging en gerichte aanbevelingen.

Het onderzoek heeft betrekking op de volgende thema's:
- De afhandeling van het datalek;
- De organisatie van informatiebeveiliging;
- De inrichting van informatiebeveiliging;
- Het risicobeheer van informatiebeveiliging;
- Het incidentenbeheersysteem;
- De toetsing op informatiebeveiliging.

De gemeente Utrecht heeft COT Instituut voor Veiligheids- en Crisismanagement (hierna: COT) gevraagd dit onderzoek uit te voeren. Dit onderzoek is gericht op het inzichtelijk maken van ervaringen, verklaringen, uitdagingen en lessen, zowel in relatie tot zaken die goed zijn verlopen alsook zaken waar vragen of twijfels over zijn of vraagstukken waar nog geen eerdere ervaring mee is.

2.3 Onderzoeksaanpak en verantwoording

Het onderzoek is uitgevoerd in de periode van mei tot en met augustus 2019. Wij zijn het onderzoek gestart met een documentenanalyse. De onderzoekers hebben de beschikking gekregen over relevante documenten, procedures, logboeken, interne evaluaties, verslagen en mailwisselingen. Zie bijlage A voor de lijst van alle ontvangen documenten.

Door middel van interviews met respondenten is aanvullende informatie verzameld. Ook is een lessenbijeenkomst op 1 juli georganiseerd. Tijdens de lessenbijeenkomst heeft het COT haar overkoepelende observaties gepresenteerd. De deelnemers hebben hun ervaringen en leerpunten gedeeld. Dit is mede input voor dit rapport en de aanbevelingen. Zie bijlage B voor een overzicht van de respondentenlijst.

Voor dit onderzoek hebben we gebruik gemaakt van verschillende referentiekaders:

- Voor de beoordeling van de afhandeling van het datalek (hoofdstuk 4) hebben we gebruik gemaakt van de richtlijnen die gelden voor meldplicht datalekken zoals vastgelegd door Autoriteit Persoonsgegevens (zie paragraaf 3.4).
- Voor de beoordeling van de status van informatiebeveiliging van SVMN (hoofdstuk 5) hebben we gebruik gemaakt van de uitgangspunten van NEN 7510, norm voor informatiebeveiliging in de zorg (zie paragraag 3.2).
- Voor de aanbevelingen hebben we gebruik gemaakt van de uitkomsten van de lessenbijeenkomst met de relevante betrokkenen.

2.4 Leeswijzer

In hoofdstuk 3 geven wij een korte achtergrondbeschrijving van (de normen voor) informatiebeveiliging, privacy en AVG en de stappen die horen bij afhandeling van een datalek. Hoofdstuk 4 bevat de bevindingen en conclusie over de afhandeling van het datalek door SVMN. Hoofdstuk 5 bevat de bevindingen en conclusie over de huidige status van informatiebeveiliging van SVMN. In hoofdstuk 6 schetsen wij aanbevelingen voor de verdere doorontwikkeling van informatiebeveiliging in relatie tot de werkbaarheid door professionals van SVMN.

2.5 Dankzegging

Bijzondere dank zijn wij verschuldigd aan het projectteam van SVMN (Directeur Servicecentrum, Functionaris Gegevensbescherming en beleidsmedewerker) voor de medewerking bij het verkrijgen van toegang tot relevante bronnen en personen, het organiseren van de interviews, lessenbijeenkomst en het ondersteunen tijdens het onderzoeksproces. De respondenten willen wij danken voor de getoonde openheid en de bereidwillige medewerking. Tijdens de interviews toonden respondenten ook persoonlijk de behoefte te leren van deze crisis.

Wij zijn ook dank verschuldigd aan de begeleidingsgroep van dit onderzoek (Strategisch adviseur Maatschappelijke Ontwikkeling gemeente Utrecht, Privacy and Security Officer gemeente Utrecht, Senior beleidsmedewerker/ projectleider MO gemeente Utrecht en teammanager/ plaatsvervangend afdelingsmanager Sociaal Domein gemeente Amersfoort) voor haar betrokkenheid en review.

3 Achtergrond en context

3.1 Inleiding

Informatiebeveiliging, privacy en datalekken zijn complexe begrippen. In dit hoofdstuk worden op hoofdlijnen deze begrippen beschreven. In hoofdstuk 4 en 5 gaan we in op hoe dit bij SVMN is geregeld.

3.2 Informatiebeveiliging in de zorgsector

Informatiebeveiliging gaat in de kern over verantwoord huisvaderschap voor de gevoelige en vertrouwelijke informatie in de organisatie. Informatiebeveiliging is daarom geen eenmalig project, maar een proces in de organisatie. Zorginstellingen dienen de risico's af te dekken die een zeer aanzienlijke schade kunnen opleveren, als deze zouden optreden. Het is belangrijk om juist deze risico's te onderkennen en maatregelen te treffen om ze te voorkomen. Deze verplichting voor de zorginstellingen bestaat uit het feit dat bij het leveren van verantwoorde zorg de patiëntgegevens op adequate wijze moeten worden beveiligd.

De norm NEN 7510 is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland. De norm is gebaseerd op de Code voor Informatiebeveiliging. NEN 7510 geeft zorginstellingen de mogelijkheid een set van maatregelen te hanteren, die in balans is met de risico's die zij lopen. Net als bij de ISO-kwaliteitssystemen wordt het normatieve denken vervangen door een invalshoek op basis van 'fit for purpose'. Niet de beveiligingsnorm of de baseline staat centraal. Centraal staan het bedrijfsrisico en de inschatting van het management of het een al dan niet een acceptabel risico betreft. Het management moet hiervoor uiteraard met daadwerkelijke relevante informatie gevoed worden. En dan gaat het niet alleen om informatie over informatiebeveiliging of over absolute controle, maar om informatie over risicoduiding en bedrijfsrisicobeheersing.

3.3 Privacy en datalekken persoonsgevoelige informatie

Privacy gaat erover dat mensen controle en regie houden over hun gegevens. Om de privacy van mensen te beschermen, zijn er privacyregels en wetten waar organisaties en bedrijven aan moeten voldoen en waar toezicht op wordt gehouden. Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) ingetreden. Deze privacywet zorgt onder andere voor versterking en uitbreiding van privacyrechten en meer verantwoordelijkheden voor organisaties. De AVG bevat regels voor het verwerken van persoonsgegevens, waarbij de nadruk ligt op geautomatiseerd verwerken van persoonsgegevens. De Autoriteit Persoonsgegevens is de toezichthouder op verwerking van persoonsgegevens en de naleving van de AVG.

Zodra er een inbreuk in verband met persoonsgegevens plaatsvindt, is er sprake van een datalek. Een datalek is het gevolg van een beveiligingsprobleem. Een datalek kan worden gedefiniëerd als "een beveiligingsincident waarbij persoonsgegevens in handen van onbevoegden zijn gekomen, voor onbevoegden toegankelijk waren, of 'zijn verloren'.

De Autoriteit Persoonsgegevens definieert een datalek als "toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van de organisatie of zonder dat dit wettelijk is toegestaan"[1]. Een datalek moet zo snel mogelijk en binnen 72 uur na

[1] De wet biedt verschillende algemene en bijzondere uitzonderingsgronden op het verwerkingsverbod op persoonsgegevens (bij rechtsvordering, een zwaarwegend algemeen belang, etc.) . Voor uitgebreide toelichting op

vaststelling gemeld worden bij de Autoriteit Persoonsgegevens tenzij het onwaarschijnlijk is dat er een risico is voor de betrokken personen.

3.4 Maatregelen bij datalekken

Een datalek kan grote schade veroorzaken aan de persoonlijke levenssfeer van betrokken. Daarnaast kan het impact hebben op het imago en de continuïteit van de eigen organisatie. Het is bij een dergelijk incident belangrijk adequaat te handelen. Een organisatie dient de volgende stappen en maatregelen te ondernemen bij datalek (of een vermoeden ervan):

1. **Vaststellen of er daadwerkelijk sprake is van een datalek?** Er is sprake van een datalek wanneer persoonsgegevens:
    a. al dan niet met opzet zijn gestolen of zijn kwijtgeraakt. Denk daarbij bijvoorbeeld aan verlies van een mobiele schijf of USB-drive met privacygevoelige data op straat of in de trein. Maar bijvoorbeeld ook persoonsgegevens die verloren gaan door brand is een datalek;
    b. op een onrechtmatige manier zijn verwerkt. Bijvoorbeeld wanneer gevoelige data is opgeslagen zonder medeweten of toestemming van de betrokkene;
    c. gegevens worden ingezien en/of bewerkt door niet-bevoegd personeel;
    d. data langer dan de afgesproken periode zijn bewaard, tenzij de betrokkene daar expliciet toestemming voor gegeven heeft;
    e. langer zijn bewaard dan nuttig voor het beoogde doel, tenzij de betrokkene daar expliciet toestemming voor gegeven heeft.
2. **Maatregelen nemen om het actieve datalek te stoppen**. In sommige gevallen is er sprake van een ‘actief’ datalek, bijvoorbeeld wanneer een hacker of onbevoegde medewerker mogelijk nog toegang tot de data heeft en nog altijd nieuwe gegevens kan buitmaken. Hackers blijven soms weken, maanden of zelfs jaren onopgemerkt in het netwerk en kunnen gedurende die tijd ongestoord data stelen.
3. **Zoveel mogelijk informatie verzamelen over het datalek**. Niet alleen over de aard van het lek zelf, zoals hoeveel en welke gegevens precies gelekt zijn. Maar vooral ook wat daar precies aan voorafging en hoe het lek heeft kunnen plaatsvinden.
4. **Datalek melden bij Autoriteit Persoonsgegevens**. Wij kennen sinds 1 januari 2016 in Nederland de Meldplicht Datalekken. Je bent verplicht melding te maken als het datalek zich heeft voorgedaan en mogelijke gevolgen heeft voor betrokkenen.
5. **Het informeren van het datalek bij betrokkenen/gedupeerden**. Sinds 1 januari 2016 zijn organisaties niet alleen verplicht ernstige datalekken te melden bij de Autoriteit Persoonsgegevens, maar ook in sommige gevallen bij de betrokkenen. Dat zijn in dit geval de mensen wier gegevens zijn gelekt. Organisaties zijn dit verplicht wanneer een lek mogelijk schadelijk is voor de ‘persoonlijke levenssfeer’ van de betrokkenen. Schade is hier een breed begrip: het gaat om mogelijke schade aan bijvoorbeeld het imago, de privacy, of financiële schade.
6. **Maatregelen nemen om het datalek in de toekomst te voorkomen.** Aanscherpen van securitymaatregelen, vergroten awareness, invoeren van aanvullende ICT-technische maatregelen, verbeteren van registratiesystemen, etc.

---

de uitzonderingsgronden: zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf

4 Bevindingen en conclusie afhandeling datalek 9 april 2019

4.1 Inleiding

Dit hoofdstuk behandelt het onderwerp '*afhandeling datalek 9 april door SVMN*'. Wij starten eerst met de specifieke bevindingen van het optreden door SVMN die horen bij de afhandeling van een datalek. Wij beantwoorden de zes maatregelen zoals beschreven in paragraaf 3.4. In paragraaf 4.3 komt de conclusie over de afhandeling door SVMN aan bod.

4.2 Bevindingen over afhandeling datalek SVMN 9 april 2019

4.2.1 Hoe is vastgesteld dat er daadwerkelijk sprake is geweest van een datalek?

SVMN is op maandagavond 8 april door RTL Nieuws ingelicht dat cliëntendata in handen van klokkenluiders zijn terechtgekomen. Twee journalisten van RTL Nieuws overleggen als bewijs een drietal kopieën van registratiegegevens van aanvragen voor crisisplaatsingen. Uit de inhoud van de kopieën van registratiegegevens en de herkenbaarheid ervan, stelt SVMN op dat moment vast dat er sprake is van een datalek. Volgens RTL Nieuws hebben de klokkenluiders de domeinnaam 'bjzutrecht.nl' geclaimd. Aan deze domeinnaam is een catch-all mailbox (een mailbox waarin alle berichten komen die naar …@bjzutrecht.nl worden gestuurd) gehangen, waardoor enkele duizenden berichten zouden zijn ontvangen. Een groot deel van deze berichten bevat inhoudelijke cliëntinformatie vanuit de 'Crisistool', welke als platte tekst in het mailbericht stonden. Dit systeem stuurt bij elke mutatie (ook een verwijdering van een dossier) verschillende in het heden en verleden bij deze zaak betrokken medewerkers een mail met daarin alle dossierinformatie over de betreffende cliënt van dat moment. Het ontvangen van deze mail was optioneel, dit kon door de medewerker ingesteld worden. Deze applicatie is vormgegeven in een Microsoft SharePoint-omgeving en wordt gebruikt door meerdere zorgaanbieders voor crisisplaatsingen in de gehele provincie Utrecht. Ook zijn er voicemailberichten (als MP3 bestand) in deze mailbox terecht gekomen.

Activeren Crisisteam SVMN dinsdagochtend 9 april

SVMN vindt het op dat moment aannemelijk dat ook andersoortige berichten zijn ontvangen, omdat cliënten en relaties mogelijk nog emailadressen gebruiken die eindigen op '@bjzutrecht.nl'. Nadat op dinsdagochtend 9 april Hoofd Informatiemanagement van SVMN de Functionaris Gegevensbescherming voorziet van een schets van de situatie is het Crisisteam van SVMN geactiveerd. SVMN heeft besloten om haar Crisisteam te activeren, omdat de impact veel breder is dan puur het melden van het datalek bij de Autoriteit Persoonsgegevens. Volgens SVMN is het datalek mogelijk geweest door een opeenstapeling van factoren (zie 4.5).

4.2.2 Welke maatregelen zijn genomen om het actieve datalek te stoppen?

Het Crisisteam van SVMN is direct op dinsdagochtend 9 april geactiveerd. Het datalek is gedicht op 9 april door de domeinnaam '@bjzutrecht.nl' weer in eigen handen te krijgen. Een mail die naar dit adres wordt gestuurd, wordt vervolgens ontvangen in een mailbox die alleen benaderd kan worden door SVMN. Ook is er op de mailserver van SVMN aangegeven dat er vanaf het interne netwerk geen mail gestuurd mag worden naar e-mailadressen die eindigen op 'bjzutrecht.nl' en 'bjzflevo.nl'. Daarnaast is op 9 april de Crisistool van Veilig Thuis Utrecht onmiddellijk stilgelegd.

Deze Crisistool wordt als een belangrijke bron van de cliëntgegevens die in het datalek zijn aangetroffen gezien. De dagelijkse procesgang vindt daarna voortgang met een nieuwe werkwijze.

4.2.3 Welke informatie is verzameld over het datalek?

SVMN start direct een intern onderzoek. SVMN heeft dit gedaan om te achterhalen hoe de domeinnaam in handen heeft kunnen komen van een derde partij, welke besluitvorming daaraan ten grondslag heeft gelegen, hoe de consequenties zijn gewogen en wie de opdracht heeft gegeven. Ook is in opdracht van SVMN door extern bureau Fox-IT aanvullend onderzoek gedaan. Fox-IT heeft onderzocht of er:

- (digitale) sporen aanwezig zijn waaruit aannemelijk wordt dat alle e-mail gericht aan het domein bjzutrecht.nl alleen bij SVMN aankomt,
- (digitale) sporen aanwezig zijn waaruit blijkt of SVMN nog systemen heeft die naar het domein e-mail versturen,
- (digitale) sporen aanwezig zijn waaruit blijkt hoe de telefooncentrale naar het domein heeft kunnen e-mailen,
- (digitale) sporen aanwezig zijn waaruit blijkt welke cliëngegevens gelekt zijn,
- (digitale) sporen aanwezig zijn waaruit blijkt wie de e-mails gestuurd aan bjzutrecht.nl onbevoegd heeft ontvangen in de periode oktober 2018 tot en met begin april 2019 door het registreren van het bjzutrecht.nl domein.

Uitkomsten Fox-IT onderzoek

Uit het Fox-IT onderzoek is gebleken dat extracten uit cliëntgegevens naar een e-mailadres op het bjzutrecht.nl-domein zijn gestuurd bij wijziging in het dossier of verwijdering ervan per e-mail. Op zo'n moment wordt een extract uit een cliëntdossier in zijn volledigheid verstuurd naar het desbetreffende e-mailadres. SVMN heeft in 2018 een groot aantal dossiers verwijderd en deze acties hebben als resultaat dat al deze dossiers in afzonderlijke e-mails zijn verstuurd naar het bjzutrecht.nl-domein en daardoor in handen zijn gekomen van de onbekenden.[2] Ook was er een tweede applicatie die e-mails stuurde naar het oude e-maildomein, een voice-over-IP telefooncentrale. Op het moment dat een gebruiker van de centrale een voicemailbericht ontvangt, wordt dit voicemailbericht per e-mail doorgestuurd naar het e-mailadres van de gebruiker.

Analyse oorzaak

Na afronding van het interne onderzoek door SVMN en het onderzoek door Fox-IT, concludeert SVMN dat door medewerkers SVMN in het kader van het datalek geen fouten zijn gemaakt, maar dat de externe ICT-partij die voor de ICT-dienstverlening is ingehuurd, het hoofd Informatiemanagement hierover niet geconsulteerd heeft. [3] SVMN heeft het beheer van haar ICT-voorziening voor een groot gedeelte uitbesteed aan een gecontracteerde ICT-dienstverlener. De operationalisering van het informatiebeveiligingsbeleid in zowel technische maatregelen als ook processen en procedures vormen hierin een belangrijk onderdeel, in het bijzonder wanneer processen en procedures SVMN-overschrijdend zijn. ICT-taken kunnen uiteraard gedelegeerd worden. Echter, de verantwoordelijkheid blijft bij de afdeling Informatiemanagement die het contract is aangegaan. De afdeling Informatiemanagement is de liason en beheert het contract met deze ICT-dienstverlener waarin zowel technische als organisatorische afspraken geborgd zijn. Alle ICT-gerelateerde vragen van SVMN medewerkers verlopen via een daarvoor ingerichte ICT servicedesk.

De medewerker Communicatie van SVMN die verantwoordelijk is voor websites en zich ook bezighield met domeinnamen, overzag de gevolgen van het afstoten van domeinnamen niet maar heeft daarover advies gevraagd bij de ICT servicedesk. Hier is aldus SVMN, de vraag te vluchtig als operationeel beantwoord, waarbij ook niet is gerealiseerd dat het niet gewenst is dat een andere afdeling dan

[2] Fox-IT, Cornelia rapportage, 2019.

[3] Dit standpunt van SVMN vraagt om een toelichting hoe het beheer van ICT-voorzieningen bij SVMN is ingericht.

Informatiemanagement domeinnamen afstoot.[4] Verder past het standpunt van SVMN niet bij het beheer van ICT-voorzieningen. Vragen van SVMN medewerkers verlopen via een daarvoor ingerichte ICT servicedesk.

Dat er nog een aantal oude '@bjzutrecht' mailadressen in omloop zijn gebleven, is veroorzaakt door het feit dat bij het overgaan van BJZ Utrecht' naar 'Samen Veilig' de mailserver zowel de mail van @bjzutrecht.nl als @samen-veilig.nl ontving, en medewerkers twee mailadressen hadden. De mail kon daardoor op twee mailadressen mail ontvangen worden. Door SVMN werd verondersteld dat de domeinnaam '@bjzutrecht' in eigen beheer was. Ook was het niet bekend dat de Crisistool die SVMN gebruikt bij alle mutaties een mail verstuurde met informatie naar alle betrokkenen en dat hiervoor nog '@bjzutrecht' adressen in de adreslijst stonden. Het gevoel onder SVMN heerst dat zij dit wel hadden moeten weten, maar niet goed waren geïnformeerd of geadviseerd door de Applicatie Ontwikkelaar. Er zijn het afgelopen jaar wel aanpassingen voor informatieveiligheid doorgevoerd in het gebruik van de Crisistool. Zo werden vanaf medio 2018 alleen initialen gebruikt i.p.v. volledige cliëntnamen en is er in november 2018 gestart met een opschoningsproces. Dit opschoningsproces heeft tot gevolg gehad dat een grote hoeveelheid signaleringsmails (nl. van verwijdering) is gecreëerd.

SVMN heeft aangegeven dat elf gebruikers een e-mailadres hadden geconfigureerd op het domein, waardoor e-mails met voicemailberichten voor deze gebruikers in handen is gekomen van de onbevoegden.

Inschakelen van externe juridische expertise

SVMN heeft ICTRecht Privacy B.V. ingeschakeld voor juridisch advies. De vraag die daarin centraal staat, is in hoeverre SVMN wettelijk verplicht is de 'slachtoffers' (betrokkenen) van het datalek individueel te informeren. De behoefte aan juridisch advies naar de wettelijke verplichtingen van SVMN ontstaat nadat SVMN (op basis van Fox-IT onderzoek) vaststelt dat vervolginspanningen disproportioneel zouden zijn. Onder de onevenredige inspanning wordt namelijk gezien de grote omvang en gedetailleerdheid van het werk dat nodig is om betrokkenen en contactgegevens op individueel niveau te identificeren en vervolgens op individueel te kunnen informeren. Het advies van ICTRecht Privacy is dat SVMN kan volstaan met een algemene mededeling en identificatie van individuele betrokkenen niet noodzakelijk is. Dit vereist namelijk een onevenredige inspanning van SVMN. ICTRecht Privacy oordeelt dat door middel van de algemene mededelingen betrokkenen beschikken over alle aanwezige informatie waaruit blijkt dat eventuele gevolgen voor hen ten aanzien van het datalek zeer beperkt zijn.[5]

4.2.4 Is het datalek gemeld bij de Autoriteit Persoonsgegevens?

SVMN heeft het datalek op 9 april om 17:40 uur formeel gemeld bij de Autoriteit Persoonsgegevens nadat eerder begin van de middag de Autoriteit Persoonsgegevens door SVMN reeds telefonisch op de hoogte is gesteld van de situatie en media-aandacht. In het geval van een datalek is bij SVMN de afspraak dat de Functionaris Gegevensbescherming afstemt met directeur Servicecentrum. Respondenten hebben aangegeven dat dinsdagmiddag 9 april de beleidsmedewerkers, Hoofd Informatiemanagement, bestuurder en directeur Servicecentrum in het Crisisteam bij elkaar zijn gekomen, waarbij de Functionaris Gegevensbescherming heeft aangegeven dat dit binnen de wettelijke richtlijnen gemeld moest worden bij de Autoriteit Persoonsgegevens.

[4] SVMN, memo domeinnaam, 2019

[5] ICTRecht Privacy B.V., C. Advies informeren van betrokkenen def 26062019, 2019.

Overwegingen melden datalek bij Autoriteit Persoonsgegevens
Het besluit om de melding te maken is genomen vanwege de omvang, de mogelijke gevolgen voor cliënten, de moedwilligheid van het datalek en de media-aandacht die er al bij betrokken was. Zodoende is in het begin van de middag van 9 april naar de Autoriteit Persoonsgegevens gebeld om haar in te lichten dat er eind van de middag 9 april een melding komt. De aanpassing op de melding van 9 april is gedaan op 19 april. SVMN had gehoopt dat de er sneller aanvullende informatie beschikbaar zou zijn om een tweede aangepaste melding te doen. Ten slotte is er een derde keer een aangepaste melding gedaan waarin de nieuwe bekende informatie zoals de aard en strekking van persoonsgegevens die gelekt zijn verduidelijkt zijn. De Functionaris Gegevensbescherming heeft in die periode regelmatig contact met de Autoriteit Persoonsgegevens. Na de derde melding heeft de Autoriteit Persoonsgegevens aangegeven geen aangepaste meldingen meer te hoeven ontvangen en dat eerst het resultaat van het Fox-IT rapport kan worden afgewacht voor een volgende melding. SVMN heeft de laatste melding gestuurd op basis van haar eindrapportage. Inmiddels is de situatie dat Autoriteit Persoonsgegevens deze zaak gesloten heeft en vanuit SVMN geen verdere meldingen te hoeven worden gedaan.

4.2.5 Hoe en wanneer zijn betrokkenen en gedupeerden geïnformeerd?

Naar aanleiding van het datalek heeft SVMN zich ook gefocust op communicatie naar betrokken doelgroepen. De communicatie richt zich op cliënten en (indien mogelijk) getroffen (oud)cliënten, medewerkers, ketenpartners en zorgaanbieders, opdrachtgevers en het brede publiek. Dit hebben zij door middel van de volgende verschillende platforms uitgevoerd.

Crisistelefoon
SVMN heeft veel (oud-cliënten) aan de telefoon gehad met de vraag of hun persoonlijke gegevens onderdeel waren van het datalek. Via dit crisistelefoonnummer hebben medewerkers namens de organisatie excuses aangeboden en uitgelegd dat er onderzoeken worden gedaan om te achterhalen welke en wiens gegevens in handen van onbevoegden zijn geraakt. Zij hebben via deze weg voor meer verduidelijking kunnen zorgen over de situatie, en tot slot de cliënten toegezegd hun persoonlijk te informeren als er meer informatie beschikbaar was, indien zij daar behoefte aan hadden.

Crisismail
Via de mail werden dezelfde vragen behandeld en informatie verstrekt aan (oud)cliënten als via de telefonische weg.

Website
Tevens werden er voor het brede publiek berichten geplaatst op de website van SVMN met het laatste nieuws over de stand van zaken. In de maand april hebben zij drie berichten geplaatst, en in mei nog eens vier. Deze omvatten een bericht op 10 april over het datalek en dat deze is gedicht, op 16 april een update met de stand van zaken op dat moment, en op 25 april een bericht over de bijeenkomst voor ketenpartners, zorgaanbieders, wijkteams en gemeenten die wordt georganiseerd. Op 6 mei plaatst SVMN een stuk over het werken aan professionaliteit en betrouwbaarheid, 7 mei over het speciale telefoonnummer en e-mailadres dat nog steeds beschikbaar is voor vragen over het datalek, 14 mei over het aan de slag gaan met verbinden en vertrouwen, en tot slot op 28 mei nog een update over het datalek. Op de website is er ook een sectie met veelgestelde vragen en antwoorden daarop opgesteld.

Social media
SVMN heeft ook LinkedIn gebruikt als platform om updates te plaatsen.

Brief
SVMN verzekert in een brief aan cliënten dat hun gegevens die in handen van onbevoegden zijn geraakt, gewist zijn. Ex-cliënten die ook mogelijk gedupeerden zijn, hebben ze niet direct kunnen bereiken aangezien zij hun gegevens niet meer hebben omdat dit niet meer mag. Ook informeren ze cliënten dat ze voor vragen terecht kunnen bij de organisatie via telefoon en e-mail.

Communicatie naar medewerkers
Medewerkers van SVMN zijn periodiek geïnformeerd via berichten op intranet en door hun leidinggevenden. Tevens zijn hun vragen beantwoord door middel van fysieke gesprekken en mailcontact en konden zij aanschuiven bij bijeenkomsten met de directie om te reflecteren op het datalek.

Communicatie naar ketenpartners en zorgaanbieders
Ketenpartners en zorgaanbieders kunnen voor informatie en updates de websites raadplegen. Daarnaast is er op 16 april 2019 een bijeenkomst geweest met contactpersonen van de crisisplaatsingen van zorgaanbieders (vanwege het aanzienlijke aandeel van Crisistool in het datalek). Een nieuwsbrief met informatie over het datalek naar ketenpartners en andere abonnees is verstuurd op 22 april. Op 25 april 2019 zijn ketenpartners, zorgaanbieders en lokale teams uitgenodigd voor een gezamenlijk overleg over de impact van het datalek op het vertrouwen en de bereidheid om te melden. Op 4 juli is nog een bijeenkomst georganiseerd door Samen Veilig voor ketenpartners en zorgaanbieders. Tijdens deze bijeenkomst worden ketenpartners en zorgaanbieders geïnformeerd over de huidige situatie, de inspanningen rondom het datalek, en wat de bevindingen tot nu toe opleveren voor de partners in de keten.

Communicatie naar opdrachtgevers
SVMN heeft diverse gesprekken gehad met Raad van Toezicht van SVMN, wethouders en ambtenaren. Ook wordt er via de mail contact gehouden met andere opdrachtgevers.

4.2.6 Welke maatregelen zijn genomen om het datalek in de toekomst te voorkomen?

Technische maatregelen
- Na het datalek van 9 april is het protocol van SVMN voor afhandeling datalek verder aangescherpt en aangevuld met een set van handelingen. Deze handelingen zijn meer gericht op een datalek van deze omvang. In deze nieuwe meldroute staat meer informatie over datalekken en meerdere stappen in hoe medewerkers moeten handelen bij het vinden van een groot datalek als deze.
- Sinds het datalek kunnen en mogen wijzigingen aan domeinnamen alleen door het Hoofd Informatiemanagement worden aangegeven bij de organisatie die de domeinnamen voor SVMN registreert. De domeinnamen die door SVMN geregistreerd zijn, worden door Z-CERT gemonitord.
- Aan het domein ‘bjzutrecht.nl’ is een catch-all mailbox gehangen. Gedurende één jaar zal alle binnenkomende mail worden geanalyseerd en de personen die mailen naar dit adres worden op de hoogte gebracht van het gebruiken van een foutief emailadres. Daarna ontvangen verzenders van de mail naar dit adres een melding dat de mail onbestelbaar is.
- SVMN heeft Zivver als tool om mailcorrespondentie te beveiligen sinds 2018. SVMN heeft de instellingen hiervan aangepast (privacy by default). Zo staat Zivver standaard aan voor alle medewerkers in plaats van dat medewerkers dit zelf moeten doen.

Overige maatregelen

- Er is een app voor privacykennis en een bewustwordingscampagne voor medewerkers opgesteld.
- De afdeling Informatiemanagement heeft een Cyber Security Specialist aangesteld die extra controle uitvoert en helpt de kwaliteit van digitale gegevensbescherming te ontwikkelen.
- Naast de Functionaris Gegevensbescherming wordt er ook een Privacy Officer aangesteld ter (operationele) ondersteuning van de werkzaamheden rondom informatieveiligheid.
- Het onderwerp informatieveiligheid wordt meer verwerkt in overleggen en agenda's. Het is binnen de tactisch en strategisch managementoverleggen van SVMN een vast onderwerp. Ook stemt de directie jaarlijks met de Stuurgroep Informatieveiligheid, de Functionaris Gegevensbescherming en het hoofd Informatiemanagement de strategische koers af rondom informatieveiligheid en legt de Stuurgroep jaarlijks verantwoording af aan de directie.
- Om bewustwording van medewerkers te vergroten is een bewustwordingscampagne door Functionaris Gegevensbescherming uitgevoerd. Door de (regio)managers zijn gesprekken gevoerd met medewerkers om de onderwerpen meer onder de aandacht te brengen.

4.3 Conclusie over afhandeling datalek door SVMN

- Vanaf het begin dat SVMN op de hoogte is van het datalek heeft SVMN een juiste inschatting gemaakt dat dit incident verder gaat dan sec een datelek. SVMN oordeelde juist door dit incident als een crisis te bestempelen vanwege de grote impact op cliënten en een inbreuk op haar bestaansgrond als betrouwbare zorginstelling. SVMN heeft terecht vastgesteld dat deze brede impact vraagt om het optreden en maatregelen van haar Crisisteam.
- Voor de duiding van het datalek dient gezegd te worden dat het om een bijzonder datalek gaat. Bijzonder in de zin dat klokkenluiders voor een lange periode geprobeerd hebben om een statement te maken richting de maatschappij. Er is gericht gezocht naar gaten in het systeem van zorginstellingen om daarmee toegang te krijgen tot persoonsgevoelige cliëntgegevens[6].
- Het heeft SVMN veel tijd gekost heeft om erachter te komen wat er precies is gebeurd. Dit kwam doordat de expertise bij SVMN ontbreekt om digitaal te rechercheren en daardoor afhankelijk was van het onderzoek door een extern bureau. Wij vinden dat van SVMN niet verwacht mag worden dat zij de expertise en capaciteit in huis heeft om digitaal te rechercheren. Dat het onderzoeksproces langer duurde dan gewenst, past in lijn der verwachtingen.
- Het datalek is vakkundig afgehandeld door het datalek snel te dichten, een onderzoek in te stellen en externe technische en juridische expertise in te schakelen. Er is tijdig en conform de richtlijnen meerdere meldingen van het datalek gedaan bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens vindt dat zij voldoende op de hoogte is en bij ongewijzigde ontwikkelingen hoeft SVMN geen aanvullende meldingen meer te doen.
- SVMN is verantwoordelijk is voor het ontstaan van het datalek (ook al komt dat door een opeenstappeling van factoren) en de gevolgen voor cliënten die gedupeerd zijn. SVMN is en blijft verantwoordelijk voor goed beheer van persoonsgevoelige informatie.
- SVMN heeft geprobeerd zoveel als mogelijk alle betrokkenen te achterhalen en te informeren, maar is hierin niet geslaagd aangezien er geen toegang meer is tot contactgegevens van ex-cliënten. Het pleit voor SVMN dat zij snel externe expertise ingeschakeld hebben om vast te stellen hoe ver zij moet gaan om ook getroffen ex-cliënten te achterhalen en individueel te informeren. Wij verwachten van SVMN dat zij in dit verband ook haar opdrachtgevers (de gemeenten) betrekt bij

[6] De klokkenluiders willen waarschuwen voor de gevaren van verlopen websitedomeinen binnen de zorgsector. Volgens hen zijn er nog tientallen soortgelijke organisaties waarvan hun oude domeinnaam ook is verlopen, en door kwaadwillenden is over te nemen. Bron: https://www.rtlnieuws.nl/tech/artikel/4672826/jeugdzorg-datalek-dossiers-kinderen-utrecht-email

deze overweging. Dit heeft zij niet gedaan. Daarnaast had SVMN een second opinion kunnen uitvoeren op het juridische advies. Dit had SVMN geholpen in haar verdere onderbouwing van de vervolgstappen op basis van het eerste juridische advies. Bij tegenstrijdige adviezen had SVMN dit bijvoorbeeld kunnen voorleggen aan haar Cliëntenraad en de gemeenten om daarover een gezamenlijk standpunt in te nemen. SVMN had hiertoe het initiatief kunnen nemen.

5 Bevindingen en conclusie informatiebeveiliging bij SVMN

5.1 Inleiding

Dit hoofdstuk behandelt het onderwerp 'informatiebeveiliging bij SVMN'. Wij starten met de bevindingen van de volgende specifieke thema's: beleid, organisatie, risicobeheer, beveiligingsincidenten en toetsing. Voor de uitwerking van deze thema's hebben wij gebruik gemaakt van de daarbij behorende onderzoeksvragen (zie bijlage C). Vervolgens beschrijven wij in paragraaf 5.7 de conclusie over de huidige status van informatiebeveiliging bij SVMN.

5.2 Beleid

SVMN heeft sinds 1 januari 2017 een Informatiebeveiligingsbeleid. Het Informatiebeveiligingsbeleid is vastgesteld door de Directie van SVMN. De doelstellingen en uitgangspunten zijn beschreven, evenals verantwoordelijkheden en bevoegdheden. In het Informatiebeveiligingsbeleid is het Information Security Management System (ISMS) uitgewerkt. Het ISMS is nodig om de borging van informatiebeveiliging te waarborgen, bijvoorbeeld door een Plan-Do-Check-Act cyclus. Plan (maak een plan met de resultaten die je wilt bereiken), Do (voer het plan uit), Check (vergelijk de resultaten met wat je had willen bereiken), Act (bij afwijking: neem maatregelen/stuur bij om de resultaten alsnog te bereiken). Door het volgen van deze cyclus vindt een periodieke toets en eventuele verbetering van de informatiebeveiliging plaats. Op deze manier kan ook jaarlijks bijgehouden worden of de maatregelen het gewenste effect hebben en waar aanpassing/aanvulling nodig is. De fase waarin SVMN zich momenteel bevindt voor Informatiebeveiliging kenmerkt zich voornamelijk door aandacht voor planvorming (Plan).

Het Informatiebeveiligingsbeleid en het privacybeleid vinden hun basis in de periodieke afhankelijkheids- en risicobeoordeling. Privacy is bij SVMN onderdeel van informatieveiligheid. Diverse privacy gerelateerde procedures en processen zijn beschreven bij SVMN. Wanneer SVMN gebruik maakt van externe ICT-leveranciers wordt gewerkt met gecertificeerde leveranciers.

Wij zijn van mening dat het SVMN zou helpen om het informatiebeveiligingsbeleid door te vertalen naar een basisniveau van informatiebeveiliging. Deze basisset van concrete technische maatregelen kan vervolgens worden geïmplementeerd en/of doorvertaald in contracten met derden (bijv. leveranciers).

5.3 Organisatie

De Directie van SVMN heeft voor informatiebeveiliging een duidelijke organisatiestructuur vastgesteld met delegatie van eenduidige en passende verantwoordelijkheden en bevoegdheden. Sinds 2018 bestaat er een Stuurgroep Informatieveiligheid met diverse functionarissen uit de SVMN-organisatie, waarbij zowel het primaire proces (Jeugdbescherming, Jeugdreclassering en Veilig Thuis), privacy als informatieveiligheid vertegenwoordigd zijn. In de Stuurgroep Informatieveiligheid komen de volgende onderwerpen aan bod: archief, registratie, dossiermanagement en risico- en afhankelijkheidsanalyse. In de Stuurgroep Informatieveiligheid komen de verschillende invalshoeken voor deze onderwerpen aan bod en worden keuzes gemaakt over wie bepaalde onderwerpen oppakt. SVMN heeft de ambitie om de positie en rol van de Stuurgroep Informatieveiligheid verder uit te werken en te verduidelijken, zeker in relatie tot andere actoren binnen informatiebeveiliging (Directie, Functionaris Gegevensbescherming, Hoofd Informatiemanagement).

De rollen van de verschillende actoren voor informatiebeveiliging zijn uitgewerkt en beschreven. Wij schetsen hieronder op hoofdlijnen de uitgewerkte rollen voor informatiebeveiliging:

- De Directie van SVMN draagt de integrale verantwoordelijkheid voor het beleid en het ISMS.
- De beleidsmedewerkers Kwaliteit zorgen ervoor dat het beveiligingsbeleid en het ISMS aansluit op het kwaliteitsbeleid van SVMN.
- De Security Officer zorgt voor het opstellen van effectief en efficiënt beleid en de uitvoering van de onderdelen van het ISMS.
- De dagelijkse verantwoordelijkheid berust bij de leidinggevenden: managers primair proces en afdelingshoofden Servicecentrum (Informatiemanagement, Facilitair en P&O etc.), die voortdurend toezicht op naleving van de vastgestelde procedures en richtlijnen uitoefenen en de risico's beoordelen waarmee hun afdeling /regio wordt geconfronteerd.
- De proces/systeemeigenaren (leden van het middenkader) hebben naast hun integrale verantwoordelijkheid als manager een specifieke verantwoordelijkheid voor de controle en uitvoering van de in Service Level Agreements/ Verwerkerovereenkomsten behorende bij het systeem waar zij eigenaar van zijn. Dit gebeurt in samenspraak met de afdeling ICT.
- De Functionaris Gegevensbescherming controleert namens de Directie de periodieke rapportages over de stand van de (integrale) beveiliging op onjuistheden van materieel belang en geeft een evaluatie van het algehele beeld van de informatiebeveiliging.

De aandacht voor bewustwording binnen SVMN in de afgelopen jaren is hoog. Bijv. door periodiek bewustwordingscampagnes te houden en het intern delen van de gedragsregels. Via verschillende kanalen, waaronder Intranet, wordt duidelijk gemaakt hoe en in welke vorm veilig moet worden omgegaan met persoonsgevoelige informatie. Na de invoering van de Algemene Verordening Gegevensbescherming (AVG) zijn specifiek hierover inhoudelijke presentaties gegeven voor de medewerkers.

Innovatie en ontwikkeling houdt in dat een organisatie de mogelijkheden onderzoekt van nieuwe technologie en deze toepast in haar bedrijfsvoering. De innovatie en ontwikkeling van ICT is niet beschreven in het Informatiebeveiligingsbeleid. Wel wordt in een presentatie over de AVG aan de medewerkers aangegeven wat een Privacy Impact Assessment bij nieuwe systemen inhoudt. Het gaat hier om het tijdig betrekken van de Functionaris Gegevensbescherming zodat het principe 'privacy by design & default' kan worden toegepast.

Privacy by design betekent gegevensbescherming door ontwerp. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy door gebruik te maken van privacy-verhogende maatregelen, zowel technisch als organisatorisch. Bijv. door afspraken te maken om alleen met geanonimiseerde gegevens te werken (of een deel van de persoonsgegevens), omdat (alle) persoonsgegevens niet echt nodig zijn voor dienst/product.

Privacy by default kan gezien worden als onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn. Er moet bijvoorbeeld voor gezorgd worden dat persoonsgegevens nooit standaard openbaar zichtbaar zijn.

ICT-middelen doorlopen een levenscyclus, van ingebruikname, beheer tot en met uitfaseren. De maatregelen die horen bij de verschillende stadia van de levenscyclus van ICT-middelen worden bij SVMN nergens expliciet beschreven. Wel zijn vanuit het perspectief van de AVG de risico's en inzichten voor SVMN benoemd in een presentatie. Daarbij is aandacht voor Privacy Impact Assessment en het principe 'privacy by design & default'. Afspraken voor het uitfaseren van ICT-middelen hebben we niet vastgesteld. Een maatregel voor het uitfaseren van een ICT-middel geldt bijvoorbeeld bij

gegevensdragers (smartphone, USB-sticks, harde schijven) waarbij er duidelijke afspraken zijn om het risico van overgebleven data op de gegevensdragers te voorkomen (bijv. vernietigen, data wissen etc.)

5.4 Risicobeheer

SVMN heeft een goed beeld van haar belangrijkste risico's voor informatieveiligheid. SVMN heeft een methode en werkwijze voor het uitvoeren van risicobeoordelingen vastgelegd. De intentie van SVMN is dat de risicobeoordeling haar helpt om maatregelen te prioriteren en in te spelen op grote veranderingen. SVMN kent twee soorten risicobeoordelingen: de *periodieke* integrale risicobeoordeling, waarbij afhankelijkheid en risico's worden bepaald voor alle bedrijfsmiddelen en de *specifieke* risicobeoordeling met als doel de risico's van een verandering in kaart te brengen en om hiervoor maatregelen te bepalen. SVMN heeft in haar risicobeoordeling risicogebieden vastgesteld. Voorbeelden (niet uitputtend) van de vastgestelde risicogebieden zijn: ongeautoriseerde toegang tot gevoelige informatie, niet voldoen aan wetgeving, ongeautoriseerde veranderingen door beheerders en gebruikers, kwaadaardige software, risico's verbonden aan mobiele computers, gebruikersfouten en hardware/systeemfouten.

Het risicobeheer binnen SVMN is vormgegeven door de uitvoering van bovengenoemde risicobeoordelingen, waarbij de risicogebieden zijn aangereikt door Jeugdzorg Nederland. Deze is opgesteld aan de hand van de Baseline informatiebeveiliging Rijksdienst (BIR) en met behulp van praktijkervaring van het privacy en security bureau genaamd *'Informatiebeveiliging doe je zo'*. De Functionaris Gegevensbescherming van SVMN is verantwoordelijk voor het organiseren van de risicobeoordelingen. Binnen de organisatie zijn 27 medewerkers betrokken geweest bij de risicobeoordelingen. Zij zijn gevraagd om informatie te geven en deel te nemen om de gezamenlijke uitkomsten van de interne sessies af te stemmen. De risico's worden door Functionaris Gegevensbescherming, Hoofd Informatiemanagement, Hoofd Personeelszaken, Directielid en de Stuurgroep Informatieveiligheid gescoord naar kans en impact. Bij de impact wordt rekening gehouden met schade voor de cliënt en schade voor SVMN. De Stuurgroep Informatieveiligheid stelt vervolgens de uiteindelijke prioritering vast (wat gaan we het eerst oppakken?). Het is niet duidelijk wat de criteria zijn voor de prioritering. De gescoorde risico's worden voorgelegd aan de Directie.

De risicobeoordeling laat een duidelijk beeld zien waar de risico-acceptatie van SVMN zich bevindt. De risico's krijgen een score op basis van kans x impact. De risico's met een lage score worden geaccepteerd en met een hele hoge score worden risico's niet geaccepteerd. Voor de risico's met een score daartussen wordt een behandelplan opgesteld en dit wordt opgenomen in een plan van aanpak. De voorgestelde acties zijn kennis, gedrag, technische en procesverbeteringen om risico's te mitigeren. Het is niet voor alle risico's vast te stellen hoe de voorgestelde verbeteracties daadwerkelijk het risico mitigeren naar een voor SVMN acceptabel niveau. Dit blijft een subjectieve exercitie. Het is niet bij alle geïdentificeerde risico's duidelijk welke maatregelen moeten leiden tot het verminderen of wegnemen van het risico. Dit is vooral bij risico's waarbij gedragsverandering geen rol speelt. De verbeteracties uit de risicobeoordeling 2017 zijn vooral gericht op gedragsverandering. Uit de inzage die wij hebben gehad in de conceptversie van de risicobeoordeling 2019 kunnen wij opmaken dat de risicobeoordeling een duidelijke verbetering is ten opzichte van 2017. Dit blijkt uit een duidelijkere rol van de Stuurgroep hierbij en een meer gedegen analyse- en afwegingsproces.

SVMN besteedt regelmatig aandacht aan de bewustwording onder medewerkers. De aandacht voor bewustwording binnen SVMN wordt naast het delen van de gedragsregels ingevuld door periodieke bewustwordingscampagnes te houden. Via verschillende kanalen, waaronder het Intranet, wordt duidelijk gemaakt hoe veilig moet worden omgegaan met informatie, in welke vorm dan ook. Ook na de invoering van de AVG zijn inhoudelijke presentaties gegeven voor de medewerkers. Medewerkers zijn

zich bewust van de privacywetgeving en melden mogelijke privacy overtredingen actief. Er is sprake van een hoge meldingsbereidheid (zie paragraaf 5.5).

SVMN heeft maatregelen gedefinieerd om de privacy van de cliënten, medewerkers en overige belanghebbenden aantoonbaar te garanderen. SVMN heeft conform het Informatiebeveiligingsbeleid uitgangspunten voor beheer en onderhoud beschreven. Dit geldt voor de eindverantwoordelijkheid voor werkzaamheden die zijn uitbesteed aan derden. Bij de inkoop van informatiesystemen hanteert SVMN het uitgangspunt dat alleen gebruik gemaakt wordt van *'proven technology'.* De reden voor dit uitgangspunt is dat SVMN te klein is om goed te kunnen omgaan met de risico's van nieuwe en onbekende technieken. Het uitgangspunt voor dataopslag is dat gebruik wordt gemaakt van de diensten van grote, gecertificeerde, hostingpartijen. Daarbij hanteert SVMN het uitgangspunt dat opslag van gevoelige informatie op papier zoveel mogelijk moet worden vermeden, vanwege de grote risico's op verlies en uitlekken van informatie.

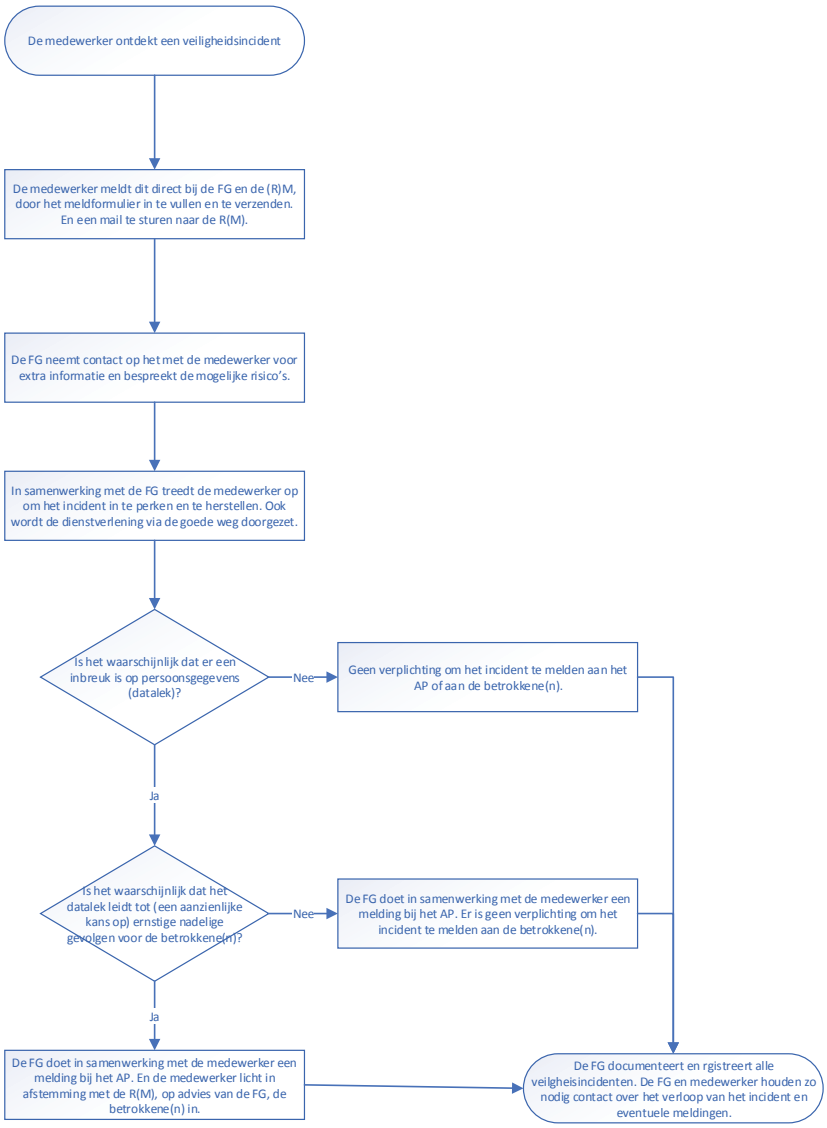
De ICT-functionaliteit en het beheer wordt uitgevoerd door de ICT-afdeling binnen SVMN. De ICT-afdeling is integraal verantwoordelijk voor een adequate beveiliging van de ICT-infrastructuur (i.s.m. de systeemeigenaren). Intern worden afspraken gemaakt over de eisen en beveiligingsmaatregelen. De afspraken worden op verschillende niveaus gemaakt en vastgelegd in werkinstructies. SVMN maakt in Service Level Agreements (SLA) & Bewerkersovereenkomsten afspraken met externe ICT-dienstverleners over de te treffen beveiligingsmaatregelen (de zogenaamde basisvoorzieningen).

De controle op de naleving en juiste implementatie van de afgesproken basis beveiligingsmaatregelen berust bij het Hoofd Informatiemanagment & de Proces/Systeem-eigenaren. SVMN dient minimaal tweejaarlijks een controle uit te (laten) voeren op de naleving van de SLA's. Zowel geconstateerde afwijkingen die de interne ICT organisatie van SVMN betreffen als de afwijkingen die externe ICT dienstverleners betreffen, worden door het Hoofd Informatiemanagement/ de Proces/Systeem eigenaren aan de Directie gerapporteerd (en ter informatie tevens aan de Security Officer gestuurd). Tijdens de afhankelijkheidsanalyse van de verschillende informatiesystemen wordt beoordeeld of de gestelde eisen afgesproken in de SLA's nog afdoende zijn. Deze eisen worden indien nodig teruggekoppeld naar de leveranciers om verbeteringen te laten doorvoeren.

SVMN heeft zoals hierboven beschreven zowel technische als organisatorische maatregelen genomen om de privacy in relatie tot partners te garanderen. Het kan echter voorkomen dat in acute situaties in het belang van de cliënt niet conform deze maatregelen informatie wordt gedeeld met partners. Aangezien acute zorg een belangrijk onderdeel is van SVMN, mag je van SVMN verwachten dat zij ook voor acute situaties maatregelen hebben op basis van privacy by default.

5.5 Beveiligingsincidenten

SVMN beschikt over een procedure 'Meldroute datalek' met instructies voor medewerkers hoe de meldroute bij een veiligheidsincident moet plaatsvinden. Hierbij is ook rekening gehouden wanneer het persoonsgegevens betreft en mogelijk de Autoriteit Persoonsgegevens en gedupeerden geïnformeerd moeten worden. Hieronder is het stroomschema uit de betreffende procedure weergegeven:



SVMN houdt sinds 2016 een overzicht bij van incidenten en/of datalekken. SVMN analyseert de meldingen en classificeert of het beveiligingslekken en datalekken zijn geweest. Daar waar er conform de richtlijnen van de AVG sprake is van een meldingsplicht bij Autoriteit Persoonsgegevens wordt dit ook gedaan. Van de 66 gemelde incidenten in 2018, is in 14 gevallen melding gedaan bij de Autoriteit Persoonsgegevens. SVMN heeft op dit moment nog geen inzicht in de meldingen van 2019. SVMN verwacht dat 2019 in lijn zal zijn met 2018 met een lichte stijging. Het gaat hier bijvoorbeeld om informatie verkeerd geadresseerd, verloren/gestolen van beveiligde en versleutelde laptops en telefoons of kwijtgeraakte poststukken/papieren documenten. Deze worden besproken in het Middenkaderoverleg. Uit de vergaderstukken blijkt een volledige registratie, evaluatie en aanbevelingen per gemeld incident. De meeste aanbevelingen zijn in de sfeer van gedragsveranderingen en daarvan is vast te stellen dat deze zijn doorgevoerd binnen SVMN (bijv. diverse bewustzijncampagnes onder de medewerkers). Daarnaast zijn technische aanpassingen doorgevoerd, zoals het voorkomen van opslaan van wachtwoorden en het uitrollen van de technische oplossing Zivver voor het veilig mailen. Wat nog ontbreekt is de strategische analyse van alle gemelde veiligheidsincidenten. Wat heeft SVMN kunnen

leren en wat kunnen ze verbeteren? Zijn er trends intern en extern? Moeten bepaalde maatregelen verder opgeschroefd worden of juist geschrapt? Dit past ook in het verder toepassen van de PDCA-cyclus.

Welke risico's SVMN loopt in geval van incident is niet duidelijk. De meldingen laten enkel een beeld zien over de informatieveiligheid en geeft geen beeld van verstoringen of onderbrekingen die de beschikbaar en of continuïteit van de dienstverlening beïnvloeden. SVMN beschikt over een afhankelijkheidsanalyse voor alle informatiesystemen die tijdens de tweejaarlijkse risicobeoordeling opnieuw wordt beoordeeld. Deze analyse geeft per informatiesysteem een classificatie voor beschikbaarheid, integriteit, vertrouwelijkheid en belang. Hoe de classificatie wordt doorvertaald naar technische maatregelen en of eisen aan leverende partijen is niet beschreven.

Juist door de georganiseerde interne bewustwordingscampagnes over de privacywetgeving zijn medewerkers bij SVMN in de afgelopen jaren meer gaan melden. Deze trend zet zich volgens SVMN ook in 2019 door. Daarbij kan gezegd worden dat nu een situatie bestaat waarbij eerder wel dan niet wordt gemeld. Daarnaast worden veel vragen gesteld over security en privacy en mogelijke situaties waarop een datalek van toepassing is. Zoals bepaalde poststukken die geopend binnenkomen of zijn verzonden in een vensterenveloppe waardoor de naam en adresgegevens zichtbaar zijn.

5.6 Toetsen van informatiebeveiliging

Een beoordeling (toetsing) van informatiebeveiliging is nodig om vast te kunnen stellen of een organisatie de goede dingen doet en de dingen goed doet. Tot op heden vindt er geen periodieke toetsing plaats om na te gaan of SVMN in control is op het gebied van informatiebeveiliging (en in relatie tot haar eigen beleid). Dit past bij een lerende organisatie zoals SVMN waarin de aandacht in eerste instantie uit gaat naar Plan en Do. SVMN heeft het besluit genomen haar risicobeoordeling jaarlijks uit te voeren.

Hoewel deze toetsing formeel volgens de PDCA-cyclus niet plaatsvindt wordt er wel intensief gecommuniceerd over het onderwerp informatiebeveiliging tussen de Functionaris Gegevensbescherming en de Directie. De Directie stemt jaarlijks met de Stuurgroep Informatieveiligheid, de Functionaris Gegevensbescherming en het Hoofd Informatiemanagement de strategische koers af voor informatieveiligheid.

5.7 Conclusie over huidige status informatiebeveiliging SVMN

- Beleid
    - Het beleid over informatiebeveiliging SVMN is momenteel aanwezig. Het beleid is echter te generiek van aard en vraagt om een duidelijke vertaling naar de context van SVMN, haar bestaansgrond en risico's.
    - SVMN dient meer gebruik te maken van de potentie van het beleid door operationalisering daarvan zodat medewerkers beter geëquipeerd zijn voor dagelijkse uitdagingen rondom informatieveiligheid.
- Organisatie
    - In opzet is er een duidelijke rol- en taakverdeling voor informatiebeveiliging.
    - SVMN levert duidelijke en merkbare inspanningen om informatiebeveiliging te implementeren en uit te voeren (de werking). Dit doet SVMN door beheersmaatregelen, processen en procedures in te richten.
    - Er zijn nog wel nieuwe actoren (bijv. de Stuurgroep Informatieveiligheid) die nog duidelijker gepositioneerd moeten worden binnen informatiebeveiliging.

- Er wordt veel aandacht besteed aan het ontwikkelen van bewustwording onder medewerkers. Informatiebeveiliging kan robuuster worden door ook rekening te houden met nieuwe (ICT) ontwikkelingen en risico's.

- Risicobeheer
  - Het risicobeheer van SVMN is in de basis goed. Zeker met de aangescherpte risicobeoordeling van 2019.
  - Het helpt SVMN om een basisniveau van informatiebeveiliging te definiëren in een basisset van technische maatregelen. Nu blijft het lastig om per situatie (risico, project, etc) vast te stellen of de juiste maatregelen zijn genomen en of dit voldoende is.
- Beveiligingsincidenten
  - De procedure voor het melden van veiligheidsincidenten is goed. Binnen SVMN is een hoge meldingsbereidheid, mede door de bewustwordingscampagnes.
  - SVMN heeft goed zicht op het aantal informatiebeveiligingsincidenten.
  - Wanneer SVMN naast de analyse van de aantallen een strategische analyse uitvoert over alle meldingen, stelt haar dat in staat om overkoepelende verbeteracties door te voeren.
- Toetsing
  - Er vindt geen structurel toetsing plaats binnen SVMN. Toetsing binnen SVMN heeft eerder het karakter van reflectie en interne afstemming dan controle op effectiviteit van maatregelen (leveren de maatregelen op wat ze moeten beogen?).

Bovenstaande kwalificaties horen bij een organisatie als SVMN die enkele jaren bezig is met informatiebeveiliging. SVMN heeft duidelijke stappen genomen en staat nu op het punt om informatiebeveiliging door te ontwikkelen.

6 Aanbevelingen voor balans werkbaarheid en informatiebeveiliging

Tijdens de lessenbijeenkomst van 1 juli 2019 hebben we uitvoerig stilgestaan bij de voorwaarden voor de balans van informatiebeveiliging in relatie tot werkbaarheid. Wij zijn ook ingegaan op de andere kant van de medaille en dat is het versterken van het crisisvermogen van SVMN. Immers, risico's zijn nooit volledig uit te sluiten en daarom dient ook het crisisvermogen versterkt te worden.

1. **Stel specifieke uitgangspunten op voor het handelen van professionals**. SVMN heeft uitgangspunten vastgesteld voor beheer en onderhoud. Binnen de context van SVMN zijn ook duidelijke uitgangspunten nodig om een veilige, betrouwbare en passende werking van het gebruik van persoonsgevoelige gegevens te waarborgen. De betrokken medewerkers kunnen met de uitgangspunten vanuit hun hun eigen verantwoordelijkheid werken. Dit gaat ook om uitgangspunten die richting geven bij mogelijke dilemma's omtrent persoonsgevoelige gegevens. Indien het niet lukt om binnen de uitgangspunten te handelen, dienen medewerkers dilemma's en uitdagingen voor te leggen aan hun leidinggevenden. Stel deze uitgangspunten op in samenspraak met de medewerkers, de Cliëntenraad, Raad van Toezicht en eventueel ketenpartners. Leg deze uitgangspunten vast in het Informatiebeveiligingsbeleid.

2. **Verstevig het risicobeheer voor informatiebeveiliging**. Maak een duidelijker onderscheid tussen risico's die moeten worden aangepakt en de aanvaardbare risico's (de risicoacceptatie). De inspanningen voor bewustwording onder medewerkers zijn momenteel ruim voldoende. De winst zit in het zoeken naar geschikte technische maatregelen om risico's te voorkomen (privacy by design en privacy by default in reguliere én in acute situaties). Wees transparant over aanvaardbare risico's, bijv. omdat het soms in het belang is van acute zorg en daarmee in het belang van de cliënten. Aanvaardbare risico's kunnen er ook zijn omdat dit de ketensamenwerking versterkt.

3. **Versterk de borging van informatiebeveiliging.** Dit kan door als SVMN periodiek te toetsen of de organisatie op geschikte wijze, adequaat en doeltreffend informatiebeveiliging ter hand neemt. In de beoordeling moet aandacht worden besteed aan mogelijke verbeteringen (beleid, organisatie, risicobeheer). Communiceer dit ook duidelijk naar de medewerkers en leg hierover als bestuur van SVMN verantwoording af aan Raad van Toezicht.

4. **Betrek cliënten bij de doorontwikkeling van informatieveiligheid**. Cliënten kunnen een belangrijke bijdrage leveren aan de normen en uitgangspunten voor het gebruik van persoonsgevoelige clientgegevens. Betrek bijvoorbeeld Clientenraad bij de bovengenoemde aanbevelingen. Naast relevante inhoudelijke input, realiseer je ook draagvlak onder de cliënten.

5. **Betrek opdrachtgevers van SVMN bij de doorontwikkeling van informatieveiligheid**. SVMN had bij dit datalek twee uitdagingen, te weten het adequaat afhandelen ervan maar ook het managen van de verwachtingen van opdrachtgevers. Wees transparant in de keuzes die SVMN gaat maken bij de doorontwikkeling van informatieveiligheid. Leg ook duidelijk uit dat daadwerkelijke incidenten rond persoonsgevoelige gegevens -ondanks alle inspanningen- nooit volledig uit te sluiten zijn. Geef daarbij wel aan hoe het crisismanagement van SVMN ervoor zorgt dat SVMN effectief, tijdig en conform de verwachtingen van de buitenwereld handelen in een crisisfase.

6. **Organiseer crisisoefeningen over de brede impact van een omvangrijk datalek**. Wees aantoonbaar voorbereid op grote en ongewenste incidenten rond persoonsgevoelige informatie. Organiseer jaarlijks een crisisoefening waarin de crisisvaardigheden voor de top risico's van SVMN ontwikkeld worden.

Bijlage A Ontvangen documenten

Ten behoeve van de documentanalyse hebben de onderzoekers de beschikking gekregen over alle voor dit onderzoek relevant documenten. Een lijst van deze documenten is in deze bijlage opgenomen.

Autoriteit Persoonsgegevens, *Ontvangstbevestiging datalek 9 4 2019*, 2019.

Autoriteit Persoonsgegevens, *Ontvangstbevestiging 2 19 4 2019*, 2019.

Autoriteit Persoonsgegevens, *Ontvangstbevestiging 13 5 2019 nr 2*, 2019.

Fox IT, *OFF_Cornelia_QQ-181148_Plan_van_aanpak*, 2019.

Fox IT, *20190611_REP_Cornelia_PR180624_Rapportage_v2.0*, 2019.

Fox IT, *20190611_REP_Cornelia_PR180624_Aanbevelingen_v2.0*, 2019.

Gemeente Utrecht, *2018.04.12 Subsidieregeling*, 2018.

Gemeente Utrecht, *2018.04.12 subsidietenderleidraad*, 2018.

Gemeente Utrecht, *Strategisch Informatiebeveiligingsbeleid Utrecht 2014-2018 v1.1.,* 2018.

Gemeente Utrecht, *Subsidietenderleidraad VT, JB, JR*,. 2018.

Gemeente Utrecht, *Tactische Richtlijnen Informatiebeveiliging Utrecht v1.1*., 2014.

Gemeente Utrecht, *TN172037 - SF02 Aankondiging van een opdracht 20180412181003*, 2018.

ICTRecht Privacy B.V., *C. Advies informeren van betrokkenen def 26062019*, 2019.

Jeugdzorg Nederland, *CONCEPT NIEUW Privreglement GI voor cliënten versie 2.0 juni 2019*, 2018.

Jeugdzorg Nederland, *sv-privacyreglement-gecertificeerde-instelling-,* 2016.

KPMG, *Accountantsverslag 2017 ML 2017 v1*, 2017.

Lloyd's Register, *Bijlage 5 - Kwaliteitsnormen WaaS – TRUE*, 2016.

SVMN, *4.2.1 Brief cliënten - informatie rondom datalek SVMN*, 2019.

SVMN, *Analyse crisistool svmn*, 2019.

SVMN, *Feitenrelaas svmn datalek dd 16 april 2019_vws*, 2019.

SVMN, *Statusoverizcht PVA*, 2019.

SVMN, *memo domeinnaam*, 2019.

SVMN, *Onderzoeksvragen Fox it*, 2019.

SVMN, *plan van aanpak datalek-16042019*, 2019.

SVMN, *Samen Veilig Midden-Nederland Nieuwsbrief Datalek 9 mei 2019*, 2019.

SVMN, *SV_ADV_UN_DRUK_cpdf_DEF*, 2019.

SVMN, *Toelichting update d.d.16-5-19*, 2019.

SVMN, *Toelichting; 26-4 pva*, 2019.

SVMN, *Veranderagenda Samen Veilig Midden-Nederland,* 2019.

SVMN, *Eindrapportage Datalek Samen Veilig*, 2019.

SVMN, *Toelichting update 27-5*, 2019.

SVMN, *Verbeteracties SVMN nav datalek 9 april 2019*, 2019.

SVMN, *1.1 Bevestiging registratie domeinnaam bjzutrecht.nl*, 2019.

SVMN, *1.2 Afsluiten en beveiligen data op Addgroep.sharepoint*, 2019.

SVMN, *2.3 Samenvatting Voicemails*, 2019.

SVMN, *3.1 Gang van zaken afstoten domeinnamen*, 2019.

SVMN, *3.2 Communicatie transitie BJZ naar SAVE*, 2019.

SVMN, *3.3 Rapportage analyse crisistool*, 2019.

SVMN, *4.2.1. Brief cliënten – informatie rondom datalek SVMN*, 2019.

SVMN, *aanvraag-vernietiging-dossier-door-clienten-4.0 maart 2019*, 2019.

SVMN, *Agendabijlage DO samen veilig zivver*, 2018.

SVMN, *Bijlage 2 - Security Structure september 2018*, 2018.

SVMN, *Bijlage 9 - Algemene presentatie ZIVVER - Samen Veilig Midden Nederland*, 2017.

SVMN, *Bijlage 11 - WIJZ Functie-Autorisatiematrix juli 2018*, 2018.

SVMN, *Bijlage 12 - CLAVIS Functie-Autorisatiematrix december 2017*, 2017.

SVMN, *Bijlage 13a - EXACT Functie-Autorisatiematrix september 2018*, 2018.

SVMN, *Bijlage 13b - EXACT Synergy Functie-Autorisatiematrix september 2018,* 2018.

SVMN, *Bijlage 20 - Password Policy*, 2018.

SVMN, *SVMN ICT Strategie 2018*, 2018.

SVMN, *gebruik-brp-door-gi-en-vt-1.0 maart 2019*, 2019.

SVMN, *gebruik-van-bsn-1.0 maart 2019*, 2019.

SVMN, *inzage-in-dossiers-door-clienten-2.0 maart 2019*, 2019.

SVMN, *Privacystatement-Samen-Veilig-versie-GI-31-10-2018*, 2018.

SVMN, *sv-1-dossierbeleid-bij-overgang-client-preventieve-jb-naar-justitieel-en-vice-versa-Dec 2018*, 2018.

SVMN, *sv-format-verwerkersovereenkomst-svmn-Aug 2018*, 2018.

SVMN, *sv-informatiebeveiliging-beleidsdocument-*, 2016.

SVMN, *sv-privacyreglement-bijlage-1-richtlijn-feiten-aanvoeren-*, 2015.

SVMN, *sv-privacyreglement-bijlage-2-handreiking-samenwerken-en-gegevensuitwisseling-*, 2015.

SVMN, *sv-regeling-bruikleen-mobiele-kantoor-en-communicatie-apparatuur-,* 2019.

SVMN, *sv-register-verwerkingsprocessen-svmn-Nov 2017*, 2017.

SVMN, *zivver com*, 2019.

SVMN, *11 juni Agenda Stuurgroep Informatie Veiligheid 4-6*, 2019.

SVMN, *30 april Agenda 30-4 Stuurgroep Informatie Veiligheid*, 2019.

SVMN, *Com Informatieveiligheid in de praktijk deel 1*, 2016.

SVMN, *Com Informatieveiligheid in de praktijk deel 2*, 2016.

SVMN, *Com Informatieveiligheid in de praktijk deel 3*, 2016.

SVMN, *Het hoe en wat van de AVG bij Samen Veilig 25 mei FG*, 2018.

SVMN, *Informatiesystemen SVMN 1-6*, 2019.

SVMN, *INFORMATIEVEILIGHEID gedragsregels com*, 2018.

SVMN, *Presentatie AVG mdw VT 2018*, 2018.

SVMN, *Presentatie AVG mdwGI okt 2018*, 2018.

SVMN, *Samen-Veilig-organogram-per-1-maart-2019*, 2019.

SVMN, *sv-gedragsregels-t-b-v-een-veilige-omgang-met-informatie-Nov 2017*, 2017.

SVMN, *Uit jaarverslag over 2018*, 2018.

SVMN, *Veranderagenda Samen Veilig Midden-Nederland*, 2019.

SVMN, *8a Oplegger MKO; analyse datalekken 2018*, 2019.

SVMN, *8b Jaaroverzicht 2018; Meldingen informatieveiligheid*, 2019.

SVMN, *Accountantsverslag 2018 def SVMN geautomatiseerde gegevensverwerking*, 2018.

SVMN, *Accountantsverslag 2018 def SVMN in beeld*, 2018.

SVMN, *ap 9 - agendabijlage MKO - datalek 2017*, 2018.

SVMN, *ap 9a - overzicht meldingen beveiligingslekken anoniem - 2018-01-03*, 2018.

SVMN, *Com Belang van informatiebeveiliging datalek melding,* 2016.

SVMN, *Com tussentijds ander datalek*, 2017.

SVMN, *nieuwe-meldroute-datalek-april 2019*, 2019.

SVMN, *Planning risicoanalyses 2019*, 2019.

SVMN, *presentatie informatieveiligheid mko def*, 2017.

SVMN, *Risicobeoordeling 2019,* 2019.

SVMN, *risicogebieden die worden onderzocht*, 2019.

SVMN, *tips-medewerkers-bij-datalek-,* 2019.

SVMN, *Verslag risicobeoordeling SVMN 17 2 2017 def*, 2017.

SVMN, *wet datalek ppo 5 7 2016*, 2016.

SVMN, *Risicomanagement en risicobeoordeling Samen Veilig nb 2*, 2019.

SVMN, *Advertentie AD 1.0 def2*, 2019.

SVMN, *FORMAT – agendabijlage Middenkaderoverleg datalek 2017*, 2018.

SVMN, *Instructie meldingsroute Data lekken 1*, 2019.

SVMN, *rapportage 2016 en q1 2017*, 2018.

SVMN, *rapportage management meldingen datalek 2016 2017*, 2018.

SVMN, *SV_ADV_UN_DRUK_cpdf_DEF*, 2019.

Bijlage B Respondentenlijst

Naam	Functie binnen SVMN
[redacted]	Manager Veilig Thuis
[redacted]	Hoofd Informatiemanagement
[redacted]	Bestuurder
[redacted]	Regiomanager SAVE
[redacted]	Bestuurder
[redacted]	Beleidsmedewerker/manager operations Veilig Thuis
[redacted]	Directeur Servicecentrum
[redacted]	Regiomanager SAVE
[redacted]	Functionaris Gegevensbescherming
[redacted]	Jurist
[redacted]	Beleidsmedewerker

Bijlage C Onderzoeksvragen datalek en informatiebeveiliging

Concreet n.a.v. datalek

- Welke maatregelen heeft de organisatie genomen na het datalek van april 2019 en zijn deze voldoende om dergelijke incidenten in de toekomst redelijkerwijs te voorkomen?

Beleid en organisatie

- Hoe is het informatiebeveiligingsbeleid en het privacybeleid vormgegeven binnen de organisatie?
- Hoe wordt concreet invulling gegeven aan de uitvoering van het informatiebeveiligingsbeleid en het privacybeleid?
- Hoe verhoudt het informatiebeveiligings- en privacybeleid en de uitvoering daarvan zich tot de inrichting en het bestuur van de organisatie van SVMN in brede zin en welke wisselwerking is daarin vast te stellen? Bijvoorbeeld:
    - Wie zijn er als verantwoordelijken aangesteld?
    - Is er aandacht voor bewustwording bij alle medewerkers?

Risicobeheer

- Heeft de organisatie in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?
    - Hoe is risicobeheer vormgegeven binnen de organisatie?
    - Welke risico's zijn formeel geaccepteerd en welke niet?
    - Welke maatschappelijke gevolgen kan dit hebben in geval van een incident?
    - Is de privacy van de cliënten, medewerkers en overige belanghebbenden aantoonbaar gegarandeerd?
    - Ook in relatie tot partners van de organisatie?

Beveiligingsincidenten

- Zijn er binnen de organisatie procedures opgesteld voor incidenten?
    - Hoeveel incidenten en/of datalekken zijn er in de afgelopen periode (maand/half jaar) geweest?
    - Van hoeveel datalekken is melding gedaan bij de Autoriteit Persoonsgegevens?
    - Is er een procedure voor het inlichten van betrokkenen bij incidenten?
    - Worden incidenten geregistreerd, geëvalueerd en worden aanbevelingen uit de evaluaties daadwerkelijk doorgevoerd?
    - Welke risico's loopt de organisatie in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt?

Toetsing van informatiebeveiliging

- Vindt er een periodieke toetsing plaats om na te gaan of de organisatie *in control* is op het gebied van informatieveiligheid via peer reviews, audits of self-assessment, in het bijzonder in relatie tot de uitvoering van het beleid en de invulling van de NEN7510?
    - Wat zijn de resultaten van deze toetsing(en)?
    - Hoe wordt invulling gegeven aan de resultaten van deze toetsing(en) in bijvoorbeeld de PDCA-cyclus?
    - Op welke manier wordt hierover gecommuniceerd met het bestuur en eventuele betrokkenen?

Effectiviteit en werkbaarheid

- Hoe kun je er voor zorgen dat de privacy en de security bij de instellingen goed geborgd is maar dat er tegelijkertijd nog open en transparant in de keten wordt samengewerkt en de noodzakelijke cliënt gegevens nog wel voldoende met elkaar gedeeld worden?

Over het COT

Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismanagement. Ons werkterrein strekt zich uit van vraagstukken over security ambities en de vormgeving van lokaal veiligheidsbeleid tot de voorbereiding op crisissituaties. Met onze kennis en kunde helpen we opdrachtgevers in complexe situaties waarbij grote risico's worden gelopen, strategische belangen op het spel staan en vaak vele stakeholders zijn betrokken. Advies, onderzoek, en training en oefening vormen de basis van onze dienstverlening. Het COT is een volledige dochteronderneming van Aon Nederland.

Meer informatie: www.cot.nl of cot@cot.nl

Disclaimer onderzoek

Deze onderzoekrapportage is gebaseerd op informatie die ter beschikking is gesteld, en verkregen, tijdens de periode waarin het onderzoek is uitgevoerd. Nieuwe of aanvullende informatie kan van invloed zijn op de inhoud en de geformuleerde conclusies en aanbevelingen. Het COT beschikt alleen over informatie waar het rechtswege toegang toe heeft. Rapporten worden in beginsel in opdracht van de opdrachtgever gemaakt en niet gepubliceerd. Eén kopie wordt bewaard voor juridische, IT- en wetgeving- en toezichtdoeleinden.

Burgemeester en Wethouders
Postadres Postbus 16200, 3500 CE Utrecht
Telefoon 14 030
www.utrecht.nl

Gemeente Utrecht

Aan de gemeenteraad

Behandeld door	[redacted]	**Datum**	27 september 2019
Doorkiesnummer	[redacted]	**Ons kenmerk**	6875977
E-mail	[redacted]	**Onderwerp**	Onderzoek Gegevensbescherming Samen Veilig Midden Nederland
Bijlage(n)	1	**Beleidsveld**	Jeugd en Jeugdzorg

Geachte leden van de raad,

De gezamenlijke Jeugdregio's in de provincie Utrecht hebben n.a.v. het op 9 april 2019 geconstateerde datalek bij Samen Veilig Midden Nederland (SVMN) opdracht gegeven aan het COT/Aon (instituut voor Veiligheids- en crisismanagement) tot het doen van onderzoek naar gegevensbescherming binnen SVMN.

Bijgaand treft u de rapportage van de onderzoekbureaus aan.

COT en Aon hebben beoordeeld:
a. hoe SVMN is omgegaan met de afhandeling van het datalek
b. hoe de informatiebeveiliging is ingericht binnen de organisatie van SVMN.

Op basis van hun bevindingen hebben de onderzoekers 6 aanbevelingen geformuleerd voor SVMN.

Een volledige weergave van alle conclusies en aanbevelingen vind u in de management samenvatting aan het begin (blz. 3-5) van het rapport.

Het onderzoeksrapport van het COT is gepresenteerd in het bestuurlijk overleg van de Jeugdregio's van 27 september jl.. Over de uitkomsten van het onderzoek en de implementatie van de aanbevelingen worden door de samenwerkende Jeugdregio's -als opdrachtgever- op korte termijn concrete afspraken gemaakt met SVMN.

SVMN heeft constructief meegewerkt aan het onderzoek in goede interactie met het COT.
De uitkomsten geven aan dat SVMN adequaat heeft gehandeld na constatering van het datalek.
De onderzoekers hebben ook vastgesteld dat informatiebeveiliging beleidsmatig en organisatorisch is ingericht binnen SVMN. Zij signaleren dat daarin qua niveau en qua implementatie nog verdere stappen te zetten zijn.
Het COT doet de aanbeveling de aansluiting met de relevante omgeving, zoals cliënten en opdrachtgevers, te versterken. Deze bevinding sluit aan bij de thema's die aan de orde zijn in de veranderagenda van SVMN.

Zoals wij u per brief van 23 mei 2019 hebben aangegeven, zijn er naast deze rapportage met aanbevelingen ook andere ontwikkelingen waar opgaven voor SVMN uit voortvloeien.

Tijdens de raadscommissie Mens & Samenleving van 16 juli 2019 zijn een aantal toezeggingen gedaan omtrent het informeren over de voortgang van de ontwikkelingen van en rondom SVMN.

Burgemeester en Wethouders

Datum 27 september 2019
Ons kenmerk 6875977

Zoals toegezegd zullen wij u in oktober een totaal overzicht sturen van alle ontwikkelopgaven van SVMN. Uit dit overzicht zal tevens blijken welke afspraken de Jeugdregio's als opdrachtgever met SVMN hebben gemaakt om uitvoering te geven aan de aanbevelingen uit de COT rapportage.
Bij het totaaloverzicht zullen wij aangeven hoe wij de ontwikkelingen duiden en hoe wij in samenhang met onze regio collega's de ontwikkelingen sturen en monitoren.

Hoogachtend,
Burgemeester en wethouders van Utrecht,

de secretaris, de burgemeester,