

Datalek gemeld? Leren is wat telt!

Deze toolkit bevat uitleg, tips en hulpmiddelen
om direct mee te starten



Inleiding

Datalekken kunnen grote gevolgen hebben voor patiënten/cliënten en zorgorganisaties. Daarom is het belangrijk dat medewerkers een datalek direct herkennen en melden. Zo blijft de schade beperkt, leren organisaties van incidenten en voorkomen zij dat vergelijkbare datalekken opnieuw plaatsvinden. Op die manier werken zorgorganisaties continu aan informatieveiligheid. Patiënten/cliënten moeten erop kunnen vertrouwen dat hun gegevens veilig zijn. Ook medewerkers verwachten dat zorgvuldig met hun persoonsgegevens wordt omgegaan. Toch worden niet alle datalekken gemeld. Dat heeft meerdere oorzaken:

- Medewerkers herkennen een datalek niet.
- Medewerkers weten niet waarom het belangrijk is om een datalek te melden.
- Medewerkers weten niet waar en hoe ze een datalek moeten melden.

Deze toolkit biedt praktische hulpmiddelen om organisaties en teams in de zorg te ondersteunen bij het melden van datalekken. De hulpmiddelen helpen bij het vergroten van bewustwording, het herkennen van datalekken en het vergroten van kennis over waarom, waar en hoe je een datalek meldt.

De toolkit is ontwikkeld voor CISO's, FG's, privacy officers, informatieadviseurs, ICT en andere professionals die zich bezighouden met informatiebeveiliging en privacy in de zorg. Zij kunnen de hulpmiddelen inzetten om binnen hun organisatie het melden van datalekken onder de aandacht te brengen en medewerkers te stimuleren datalekken tijdig te herkennen en melden.

De hulpmiddelen in deze toolkit zijn ontwikkeld binnen het programma Informatieveilig gedrag in de zorg (IVGZ), in samenwerking met professionals uit het werkveld. Hun praktijkervaring, kennis en expertise zijn vertaald naar praktische hulpmiddelen die direct toepasbaar zijn binnen zorgorganisaties.

Alle hulpmiddelen uit deze toolkit zijn ook afzonderlijk te downloaden via [de website](#) van het programma Informatieveilig gedrag in de zorg.

Samen zorgen we voor goede, veilige en betrouwbare zorg.



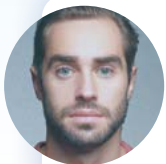
Waarom aan de slag met het melden van datalekken?

Een datalek kan iedereen overkomen. Het verschil maak je door te herkennen dat er mogelijk iets mis is en dit direct te melden volgens de intern geldende procedure. Hoe sneller een melding wordt gedaan, hoe sneller de organisatie kan onderzoeken wat er is gebeurd, de gevolgen kan beperken en maatregelen kan nemen.

Hoe kan het misgaan?



Wij verzamelden medicijndoosjes in een open inleverbak bij de balie. De stickers met namen, geboortedata en medicatiegegevens waren nog goed leesbaar. Een bezoeker maakte er foto's van en deelde deze op sociale media om 'aan te tonen hoe slordig we met gegevens omgaan'.



Tijdens het begeleiden van een training in de oefenzaal werd ik even weggeroepen. Mijn computer stond nog aan, met het dossier van een van de cliënten op het scherm. Andere cliënten zagen persoonlijke informatie zoals diagnose en behandelplan. Een van hen diende een klacht in bij de praktijkgenaar.

Zelf aan de slag met bewustwording?

Onderstaande voorbeelden zijn ook als posters te downloaden. Gebruik ze binnen je organisatie om het gesprek over mogelijke datalekken op gang te brengen. Bespreek met collega's of zij deze situaties zouden herkennen als een mogelijk datalek en wat zij vervolgens zouden doen. Je hoeft niet zeker te weten dat het een datalek is. Bij twijfel: meld het.

Wat kunnen de gevolgen zijn?



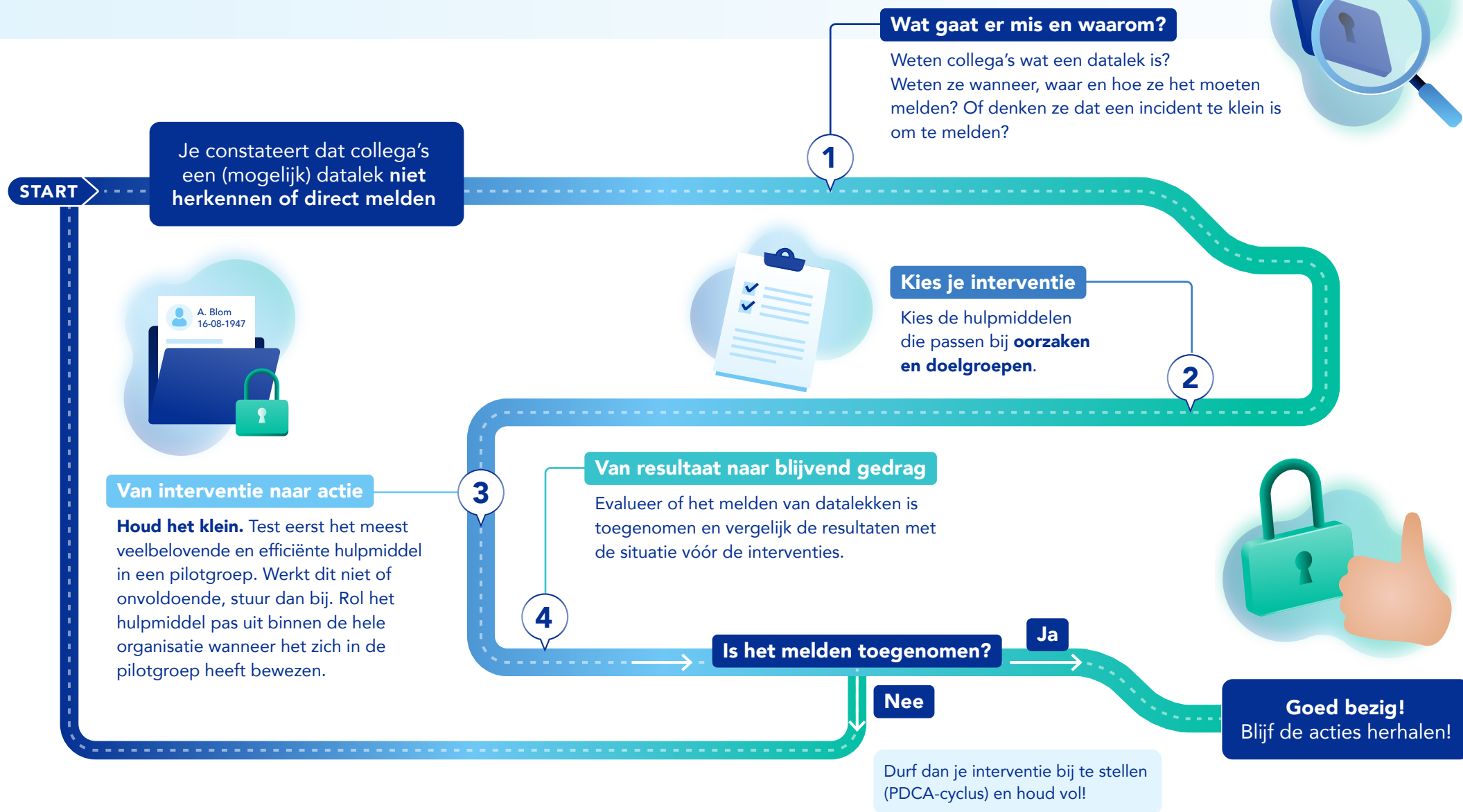
Ik liet mijn werktelefoon even op tafel liggen in de huiskamer. Bij terugkomst was de telefoon verdwenen, waarschijnlijk meegenomen door een cliënt. Op de telefoon stonden onbeveiligde contactgegevens van cliënten en collega's. Het datalek moest gemeld worden en leidde tot zorgen bij familieleden.



Tijdens de zorgverlening aan een cliënt liet ik per ongeluk mijn werktablet open op bed liggen, waarop het zorgplan van een andere cliënt zichtbaar was. Een familielid dat op bezoek was, las onbedoeld deze vertrouwelijke gegevens en sprak mij hierop aan. Dit leidde tot wantrouwen bij de familie.



Stappenplan Melden datalek



1. Wat gaat er mis en waarom?

Je ziet dat collega's een mogelijk datalek niet altijd herkennen of direct melden. Voordat je verbeteracties kiest, is het belangrijk om te begrijpen waar dit gedrag vandaan komt. Breng daarom met een nulmeting de situatie in jouw organisatie in kaart. Gebruik de **Compacte Wegwijzer** om te bepalen welke onderwerpen je in de nulmeting onderzoekt.

Ga in gesprek met minimaal vijf collega's en vraag wat hen tegenhoudt om een mogelijk datalek te melden. Gebruik bij je onderzoek het overzicht van de **Meest voorkomende gedragsoorzaken** op de volgende pagina ter inspiratie. Bespreek herkenbare situaties uit de praktijk en onderzoek welke vragen of twijfels zij hebben.

Bekijk daarnaast bestaande meldingen en het meldproces. Welke soorten datalekken komen voor? Hoe snel worden ze gemeld? Is het meldproces laagdrempelig en weten collega's waar en hoe zij een mogelijk datalek kunnen melden?

Heb je de belangrijkste oorzaken in beeld?

Ga dan verder met **stap 2**.

Zo ontdek je waar het misgaat



Kleinere zorgorganisaties

- Bespreek tijdens een werkoverleg wat collega's onder een datalek verstaan.
- Bespreek herkenbare voorbeelden en vraag wanneer collega's wel of niet zouden melden.
- Vraag collega's wat hen tegenhoudt als zij twijfelen over een melding.
- Loop samen het huidige meldproces door. Is duidelijk waar en hoe je meldt en is dit makkelijk genoeg?
- Bespreek ook situaties waarin een mogelijk datalek snel en goed werd gemeld. Wat hielp daarbij?

Grotere zorgorganisaties

- Analyseer meldingen en kijk naar patronen tussen afdelingen, locaties of soorten incidenten.
- Onderzoek hoe snel mogelijke datalekken worden gemeld en waar en waarom vertraging ontstaat.
- Vergelijk afdelingen of locaties. Weten collega's wat een datalek is en welke meldroute zij moeten volgen?
- Onderzoek of het meldformulier en de meldprocedure duidelijk, makkelijk vindbaar en eenvoudig te gebruiken zijn.
- Gebruik signalen van de Functionaris Gegevensbescherming, privacy officer, informatieveiligheidsprofessional of servicedesk om terugkerende knelpunten te herkennen.
- Betrek collega's uit de praktijk om te onderzoeken wat het melden makkelijker of juist moeilijker maakt.



Meest voorkomende gedragsoorzaken

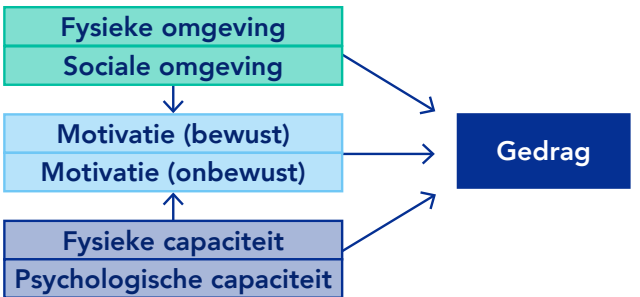
Dit overzicht geeft voorbeelden van veelvoorkomende gedragsoorzaken van het niet melden van datalekken. Gebruik het om te verkennen welke oorzaken binnen jouw organisatie of team een rol kunnen spelen. De oorzaken zijn ingedeeld volgens het **COM-B model**. Rechtsboven vind je een schematische weergave van het model en een verwijzing naar meer informatie.

Gebruik het overzicht als inspiratie voor je eigen onderzoek. Herken je bepaalde oorzaken? Bespreek dan met collega's of deze inderdaad een rol spelen en onderzoek of er andere oorzaken zijn. Zo krijg je zicht op wat het gedrag veroorzaakt en kun je in de volgende stap een passende interventie kiezen.

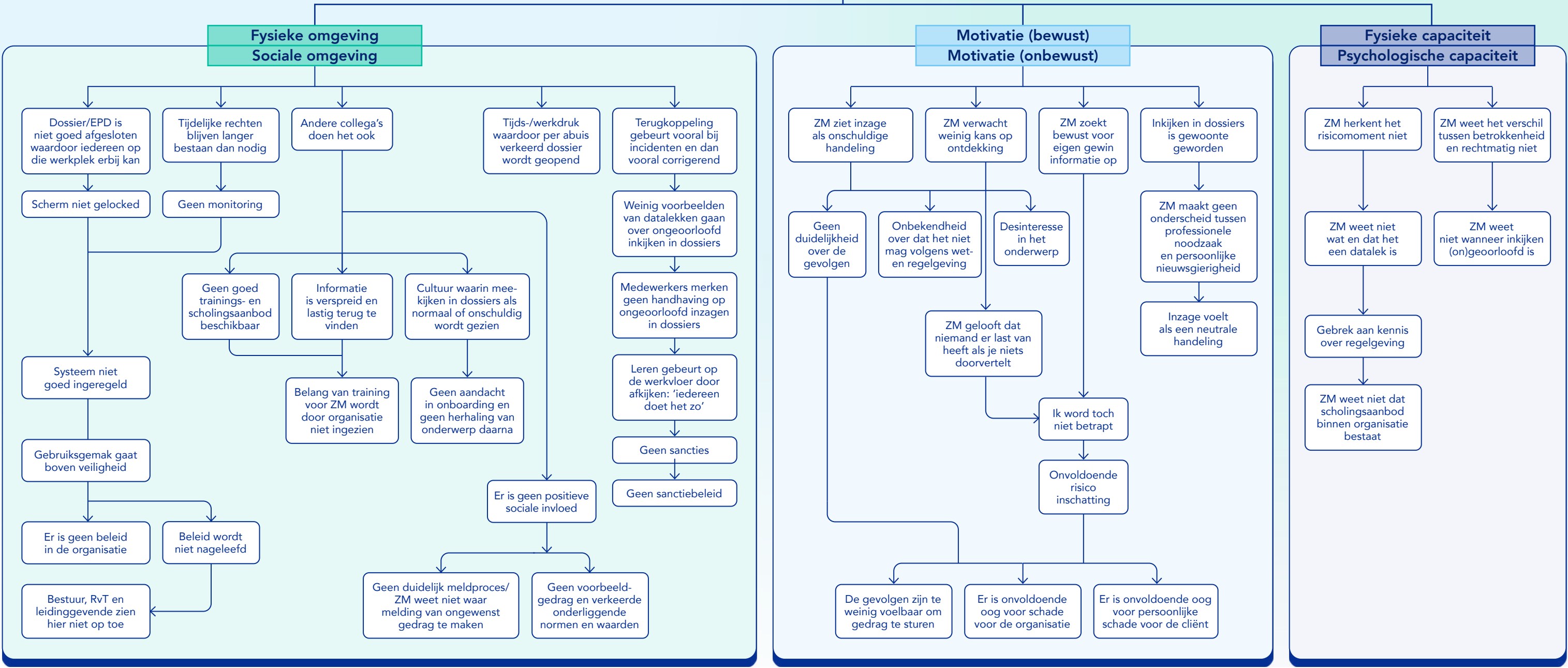
Probleem (risico) Zorgmedewerker meldt een (mogelijk) datalek niet.
Doelgroep Zorgmedewerkers (ZM): zorgprofessionals en andere werknemers binnen een zorgorganisatie.

Doelgedrag Zorgmedewerker meldt een (mogelijk) datalek volgens de geldende meldprocedure.

COM-B model Lees meer in [stap 3 uit De Wegwijzer](#)



● [Hulpmiddel melden datalek](#)



2. Kies je interventie

Je weet nu waarom collega's mogelijke datalekken niet altijd herkennen of direct melden. Bepaal welke acties nodig zijn om ervoor te zorgen dat collega's mogelijke datalekken herkennen en direct melden.

Kies vervolgens welke middelen uit de toolkit passen bij jouw doelgroep en situatie. Op de [overzichtspagina](#) vind je alle hulpmiddelen uit de toolkit, met per hulpmiddel het doel en een voorbeeld van hoe je het kunt inzetten.

[Bekijk hier](#) de tips voor het kiezen van een passend hulpmiddel.

Twijfel je over de aanpak?

Bespreek de mogelijkheden met elkaar en maak samen een keuze. Blijf de voortgang volgen en stel het actieplan bij als dat nodig is. Is het actieplan klaar? Ga dan verder met [stap 3](#).

Zo kies je wat je gaat doen



Kleinere zorgorganisaties

- ➔ Kies één of twee verbeterpunten die aansluiten bij de belangrijkste oorzaken die je hebt gevonden in stap 1.
- ➔ Vraag jezelf bij iedere actie af: welk probleem lossen we hiermee op en waarom verwachten we dat dit werkt?
- ➔ Weten collega's onvoldoende wat een datalek is? Kies dan een actie die helpt bij het herkennen van mogelijke datalekken.
- ➔ Is vooral onduidelijk waar en hoe collega's moeten melden? Maak de meldroute dan eenvoudiger en beter vindbaar.
- ➔ Vinden collega's melden veel gedoe? Kijk dan hoe je het meldformulier korter en makkelijker kunt maken.
- ➔ Vraag een paar collega's of de gekozen oplossing duidelijk en werkbaar is.

Grotere zorgorganisaties

- ➔ Stel een kernteam samen. Vraag onder andere de collega's van privacy, informatiebeveiliging, ICT en communicatie. Betrek ook zorgmedewerkers bij het kiezen van interventies.
- ➔ Koppel iedere actie aan een oorzaak uit stap 1.
- ➔ Bepaal welke acties organisatiebreed nodig zijn en waar een andere aanpak nodig is voor bepaalde afdelingen, functies of locaties.
- ➔ Kijk niet alleen naar voorlichting. Onderzoek ook of het meldproces, het meldformulier of systemen aangepast kunnen worden om melden makkelijker te maken.
- ➔ Maak afspraken over wie meldingen ontvangt en beoordeelt en hoe opvolging en terugkoppeling plaatsvinden.
- ➔ Vergelijk mogelijke acties op verwacht effect en haalbaarheid.
- ➔ Bepaal vooraf hoe je gaat meten of mogelijke datalekken beter en sneller worden gemeld.



Tips bij het kiezen van hulpmiddelen

Kies wat past bij het knelpunt

Sluit aan bij de oorzaken uit stap 1. Herkennen collega's mogelijke datalekken onvoldoende? Kies dan bijvoorbeeld de [animatievideo](#) of (maak) een eigen video. Of gebruik de poster [Voorbeelden van een datalek](#). Zit het knelpunt vooral in de beoordeling en afhandeling van meldingen? Gebruik dan het [Voorbeeldproces Melden datalek](#) om collega's hierin te ondersteunen.

Sluit aan bij wat collega's nodig hebben

Kijk wat collega's al weten en waar zij nog over twijfelen. Gebruik bijvoorbeeld het [Voorbeeldproces Melden datalek](#) om herkenbare situaties te bespreken. Stem de uitleg af op hun kennis en maak duidelijk dat zij bij twijfel een mogelijk datalek kunnen melden.

Maak melden makkelijk en zorg voor goede opvolging

Is het melden zelf een drempel? Gebruik het [Template vragenformulier melden mogelijk datalek](#) om het meldformulier kort en eenvoudig te houden.



3. Van interventie naar actie

Je hebt gekozen welke acties en middelen passen bij de oorzaken voor het niet, niet goed of niet tijdig melden van mogelijke datalekken. Bepaal nu hoe je deze in de praktijk gaat uitvoeren. Maak een eenvoudig actieplan: wat ga je doen, voor wie, wanneer en wie is daarbij betrokken?

Denk ook na over hoe je collega's bereikt. Welk communicatiekanaal past bij de doelgroep? Is een combinatie van kanalen nodig? Welke toon past bij de boodschap en wat is een goed moment?

Voer de acties uit en houd in de gaten hoe ze in de praktijk werken. Vraag collega's naar hun ervaringen en kijk of zij mogelijke datalekken beter herkennen en sneller melden.

Werkt een actie niet zoals verwacht?

Onderzoek waar dit aan ligt en stel je aanpak bij. Ga daarna door naar [stap 4](#).

Zo breng je acties in de praktijk



Kleinere zorgorganisaties

- Spreek per actie af wie deze uitvoert en wanneer.
- Bespreek de infographic, animatievideo of praktijksituaties tijdens bestaande momenten, zoals een werkoverleg.
- Zorg dat de meldroute makkelijk te vinden is, bijvoorbeeld via intranet of een vaste plek in een systeem.
- Houd het meldformulier kort en eenvoudig.
- Oefen samen met herkenbare situaties en laat collega's bepalen wanneer zij een melding zouden maken.
- Vraag tijdens de uitvoering of melden makkelijk gaat en waar collega's nog tegenaan lopen.
- Koppel na een melding terug wat ermee is gedaan, zodat collega's zien wat hun melding oplevert.

Grotere zorgorganisaties

- Leg per actie vast wat er moet gebeuren, wie verantwoordelijk is en wanneer de actie wordt uitgevoerd.
- Test grotere veranderingen eerst bij een afdeling of pilotgroep en gebruik de ervaringen voordat je verder uitrolt.
- Voer acties waar nodig gefaseerd uit per afdeling, locatie of doelgroep.
- Integreer de meldroute waar mogelijk in bestaande systemen en maak deze makkelijk bereikbaar.
- Laat beschikbare gegevens waar mogelijk automatisch invullen om melden makkelijker te maken.
- Gebruik verschillende praktijksituaties om collega's te trainen in het herkennen en melden van mogelijke datalekken.
- Gebruik het voorbeeldproces om meldingen op een eenduidige manier te beoordelen en af te handelen.
- Zorg voor duidelijke terugkoppeling naar melders.



4. Van resultaat naar blijvend gedrag

Bekijk wat de acties hebben opgeleverd. Herhaal de nulmeting die je in stap 1 hebt gedaan. Herkennen collega's mogelijke datalekken beter? Weten zij waar en hoe ze moeten melden? Worden mogelijke datalekken sneller gemeld? En verloopt de opvolging zoals afgesproken?

Vergelijk de resultaten met de situatie vóór de acties. Kijk ook naar de ervaringen van collega's en naar de meldingen zelf. Welke patronen zie je?

Gebruik deze inzichten om je aanpak bij te stellen. Misschien is extra aandacht nodig voor bepaalde soorten datalekken, afdelingen of functies. Of blijkt dat het meldformulier of de meldroute nog eenvoudiger kan.

Zorg er tot slot voor dat het herkennen en melden van mogelijke datalekken onderdeel blijft van de dagelijkse praktijk. Houd de meldroute makkelijk vindbaar, bespreek regelmatig situaties uit de praktijk en laat collega's zien wat er met meldingen gebeurt. Leg ook vast wie verantwoordelijk is voor het meldproces en het actueel houden van afspraken en hulpmiddelen.

Wil je uitgebreider aan de slag met het veranderen en verankeren van informatieveilig gedrag?

De [Compacte Wegwijzer](#) helpt je gedrag te onderzoeken, passende interventies te kiezen en uit te voeren. Wil je meer verdieping? Gebruik dan de [Uitgebreide Wegwijzer](#). Je kunt ook onze [Masterclass](#) volgen. Daarin ondersteunen we je stap voor stap bij het toepassen van de aanpak.

Zie de [volgende pagina](#) voor tips om blijvend resultaat te behalen.



4. Van resultaat naar blijvend gedrag



Zo zorg je voor blijvend resultaat

Kleinere zorgorganisaties

- Bespreek of collega's mogelijke datalekken beter herkennen en sneller melden. Kijk niet alleen naar hoeveel meldingen er zijn, maar ook naar hoe het melden in de praktijk gaat.
- Vraag collega's of zij nog steeds weten waar en hoe zij een mogelijk datalek moeten melden.
- Evaluer of de meldroute en het meldformulier nog duidelijk en makkelijk te gebruiken zijn.
- Deel leerpunten uit meldingen zonder individuele collega's centraal te stellen.
- Koppel terug welke verbeteringen naar aanleiding van meldingen zijn doorgevoerd.
- Spreek af wie verantwoordelijk blijft voor het meldproces en het actueel houden van afspraken en hulpmiddelen.

Grotere zorgorganisaties

- Kijk niet alleen naar het aantal meldingen. Onderzoek ook of collega's mogelijke datalekken beter herkennen, sneller melden en weten hoe zij moeten melden.
- Analyseer de meldingen zelf. Welke soorten mogelijke datalekken worden gemeld, hoe snel gebeurt dit en welke oorzaken en patronen zie je?
- Vergelijk waar mogelijk de resultaten met de situatie vóór de acties en tussen afdelingen of locaties.
- Evaluer het hele meldproces: van herkennen en melden tot beoordeling, opvolging en terugkoppeling.
- Gebruik terugkerende oorzaken van datalekken om gerichte verbetermaatregelen te nemen.
- Zorg voor terugkoppeling naar melders en deel relevante leerpunten binnen de organisatie.
- Beleg het beheer van het meldproces, afspraken en hulpmiddelen bij een vaste functie of afdeling.
- Neem het herkennen en melden van mogelijke datalekken op in bestaande momenten, zoals onboarding, scholing en werkoverleggen.



Hulpmiddelen in deze toolkit

Hieronder vind je een overzicht van de hulpmiddelen in deze toolkit, met het doel van ieder hulpmiddel en een praktisch voorbeeld van hoe je het kunt inzetten. Welk hulpmiddel je kiest, hangt af van het probleem dat je in stap 1 binnen jouw organisatie hebt vastgesteld. Weten medewerkers bijvoorbeeld niet wat een datalek is? Zet dan de animatievideo in.

Voorbeeldproces medewerker

Pagina 13 ➔

Doel

Collega's helpen om mogelijke datalekken te herkennen en duidelijk maken wat zij moeten doen als er iets misgaat.

Voorbeeld

Loop het meldproces samen met een team door en bespreek herkenbare voorbeelden van mogelijke datalekken uit de dagelijkse praktijk.

Voorbeeldproces expert IV

Pagina 16 ➔

Doel

Experts informatieveiligheid ondersteunen bij het beoordelen, opvolgen en afhandelen van meldingen van mogelijke datalekken.

Voorbeeld

Gebruik het voorbeeldproces om de eigen werkwijze te vergelijken en afspraken te maken over beoordeling, maatregelen, terugkoppeling en leren van meldingen.

Template vragenformulier

Pagina 17 ➔

Doel

Experts informatieveiligheid helpen een meldformulier te maken waarmee collega's eenvoudig datalekken melden en de juiste informatie aanleveren.

Voorbeeld

Gebruik het template om een bestaand digitaal meldformulier of ticketsysteem te verbeteren en kies alleen de vragen die passen bij jouw organisatie en meldproces.

Animatievideo

Bekijk de animatie ➔

Doel

Collega's bewust maken van het belang van snel melden en laten zien waarom melden helpt om schade te beperken en herhaling te voorkomen.

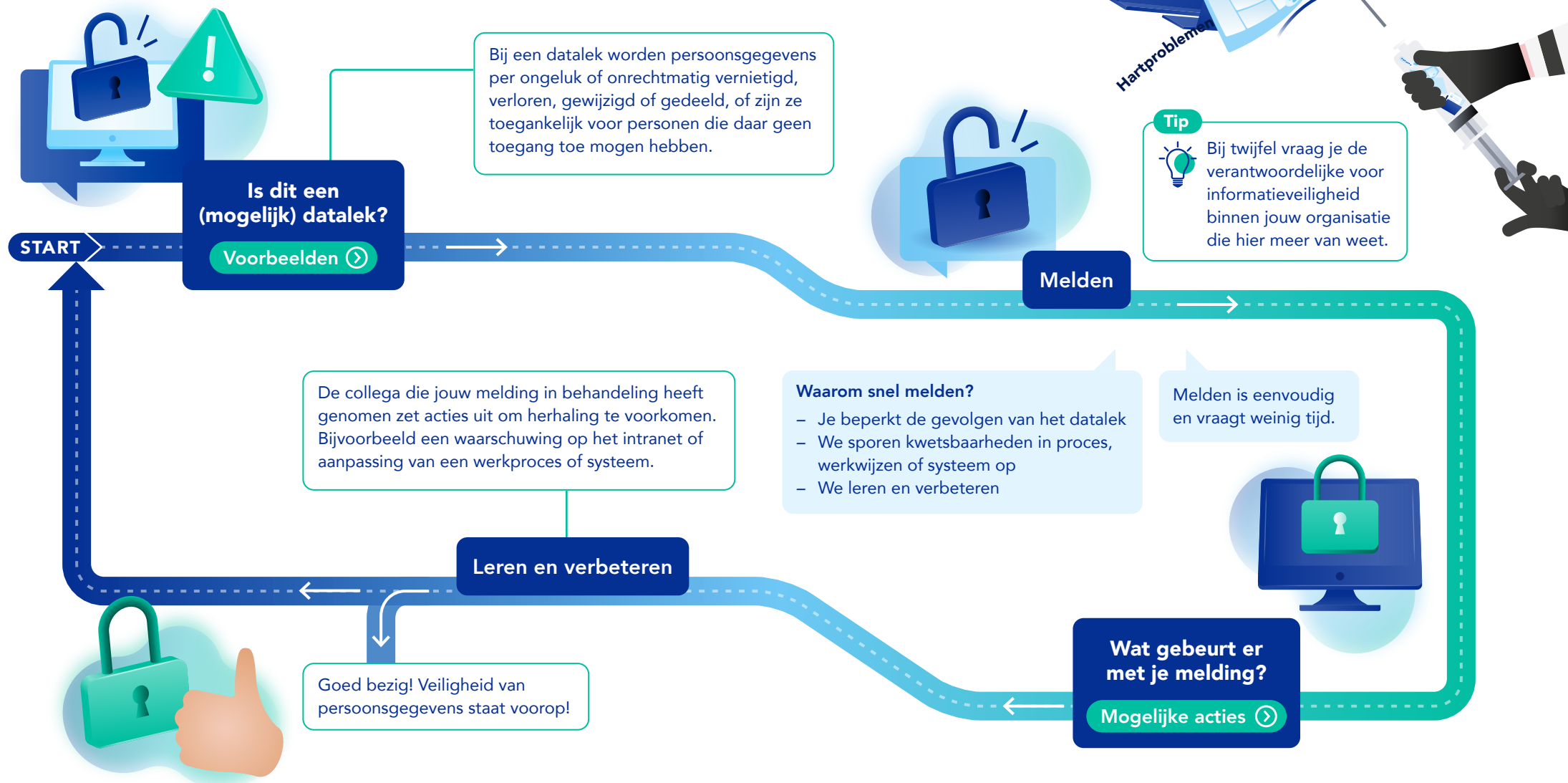
Voorbeeld

Laat de animatievideo zien tijdens een werkoverleg en bespreek daarna welke situaties collega's zouden melden en waar zij nog over twijfelen.

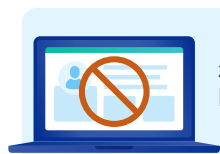


Voorbeeldproces voor medewerkers

Datalek gemeld? Leren is wat telt!



Voorbeelden van een datalek voor medewerkers



Het dossier inzien zonder dat er een behandelrelatie is.



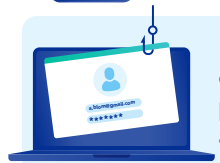
Niet-versnipperde baxterzakjes met alle patiënt- of cliëntgegevens in een open prullenbak.



Medische persoonsgegevens delen via WhatsApp of een andere tool die hier niet voor bedoeld is.



Patiënt- of cliëntgegevens toevoegen aan het verkeerde dossier.



Phishing e-mails openen, op de link klikken en persoonsgegevens achterlaten.



Werktelefoon, laptop, tablet of usb-stick kwijtraken.



E-mail met externe adressen in de cc in plaats van bcc terwijl de geadresseerden elkaars adres niet horen te weten.



Sollicitatiebrieven weggooien bij het oud papier.



Patiënt- of medewerkersgegevens bij de printer laten liggen.



Gegevens over een patiënt/ cliënt op een (wegwerp) handschoen schrijven.



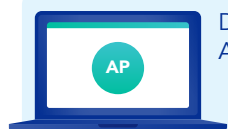
Over een patiënt/cliënt praten op een plek waar anderen kunnen meeluisteren.



Privacygevoelige gegevens invoeren in een niet goedgekeurde AI-tool.



Mogelijke acties na melden datalek voor de expert informatieveiligheid



Datalek melden bij de Autoriteit Persoonsgegevens.



Patiënt/cliënt of medewerker van wie persoonsgegevens zijn gelekt informeren.



Maatregelen nemen om werkwijze, proces of systeem te verbeteren om datalek in de toekomst te voorkomen.



Analyseren en evalueren van (bijna) datalekken. Ook van verschillende ogenschijnlijk kleine incidenten wordt geleerd en kunnen acties worden genomen om een datalek in de toekomst te voorkomen.

Tip



Z-CERT kan je organisatie ondersteunen met technische, operationele en actuele informatie om beter te beschermen tegen cyberdreigingen.



Herstelacties uitvoeren.



Terugkoppeling aan de melder van het datalek en eventueel betrokken collega's.



Het registreren van een datalek in een datalekregister van de eigen organisatie is wettelijk verplicht. Noot: deze registratie is niet bedoeld voor sancties of dossieropbouw.



Voer een onderzoekend gesprek om te leren van het datalek.
In de toolkit Bewuste dossierinzage lees je hoe je dit gesprek op een open en veilige manier voert.

Tip



NEN kan helpen met duidelijke kaders, beveiligingseisen en processen voor het signaleren, melden en zorgvuldig afhandelen van datalekken.

Verwijzingen

Wil je datalekken voorkomen?

Ontdek praktische tips en voorbeelden in onze toolkit

[Veilig omgaan met gegevens.](#)

Weet je niet zeker wanneer je een dossier mag inzien?

In onze toolkit [Bewuste dossierinzage](#) vind je de uitleg, voorbeelden en praktische handvatten.

Wil je veilig communiceren binnen jouw organisatie?

Bekijk onze toolkit [Veilig communiceren](#) en ga direct aan de slag met praktische tips en afspraken.

Wil je AI-chatbots veilig gebruiken?

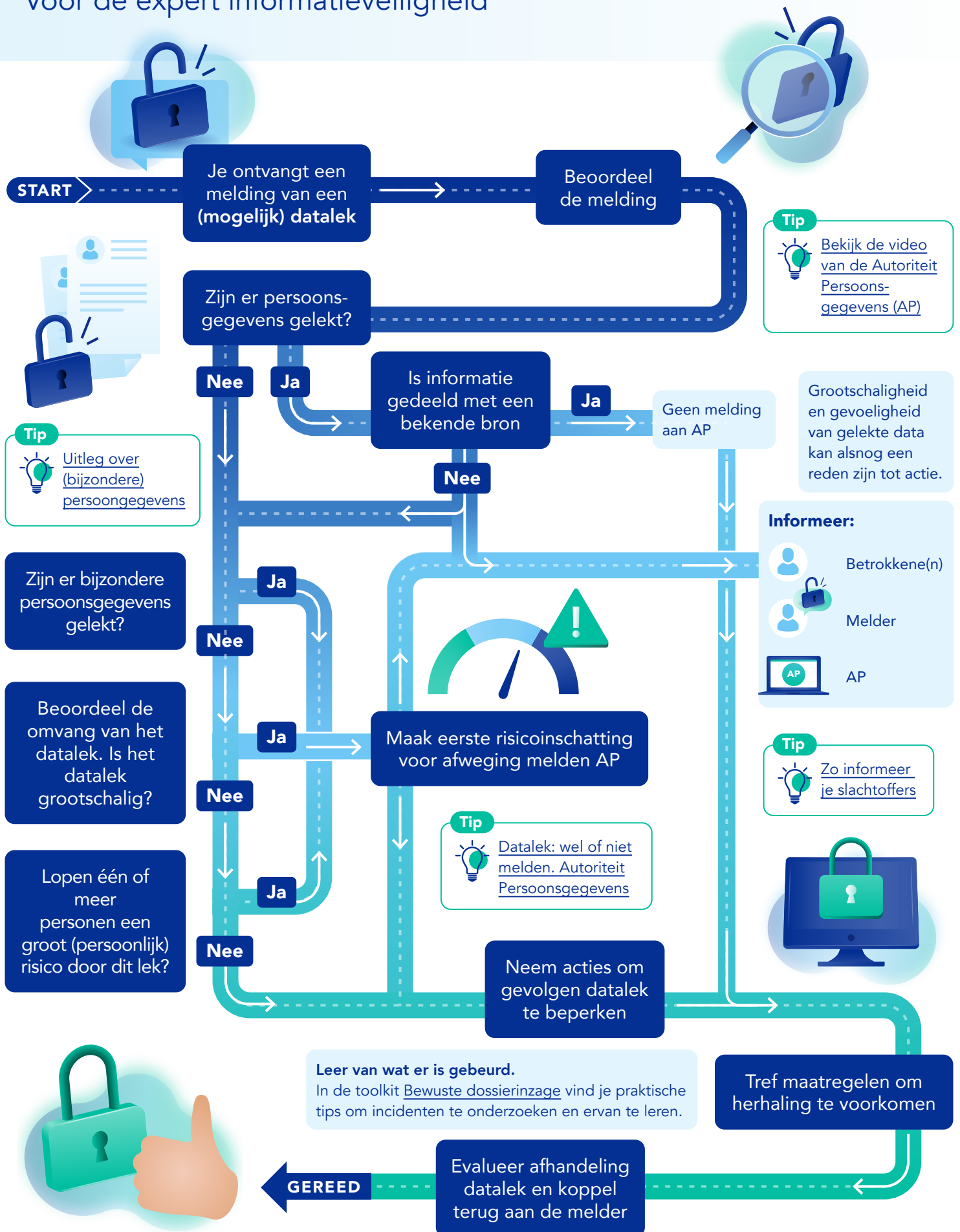
Ontdek hoe je verantwoord met AI werkt en welke gegevens je wel en niet mag delen in onze toolkit

[Veilig gebruik van AI-chatbots.](#)



Voorbeeldproces Melden datalek

Voor de expert informatieveiligheid



Template vragenformulier melden (mogelijk) datalek

Gebruik van dit template

Dit template is een hulpmiddel voor de expert informatieveiligheid. De vragen in dit formulier zijn bedoeld als input om zelf een (digitaal) meldformulier te maken. Kies de vragen die jij passend vindt bij jouw organisatie, meldproces en medewerkers.

Waarom deze vragen?

Zorgmedewerkers kunnen via dit formulier snel en eenvoudig een (mogelijk) datalek melden. En de expert informatieveiligheid ontvangt voldoende en relevante gegevens om met de melding aan de slag te gaan.

Uitgangspunt is dat de gegevens van de melder (naam, emailadres, telefoonnummer) door de digitale melding automatisch gegenereerd zijn. Dit wordt dus niet uitgevraagd.

Je kunt dit meldformulier met vragen beschikbaar stellen aan medewerkers op een passende manier in jouw organisatie. Bijvoorbeeld als digitaal formulier op intranet of via een ticketsysteem.

[Download het formulier hier.](#)

Template vragenformulier
Melden (mogelijk) datalek

Neem de volgende vragen minimaal op in het formulier
Melden (mogelijk) datalek:

Hoe is het (mogelijk) datalek ontstaan?

Wat is er gebeurd?

Datum (mogelijk) datalek:

Datum waarop (mogelijk) datalek is ontstaan:

Wat is de oorzaak van het (mogelijk) datalek?

☐ Niet-verenigende bantzakjes met alle patiëntgegevens in een open prullenbak

☐ Medische persoonsgegevens gedeeld via WhatsApp en nu getoond te hebben vergeten te verwijderen

☐ Patiëntgegevens toegevoegd aan het verkeerde dossier

☐ Phishing e-mails geopend, op de link geklikt en persoonsgegevens achtergelaten

☐ Werkstation, laptop, tablet of usb-stick kwijtgeraakt

☐ E-mail met medische persoonsgegevens met externe adressen in de cc in plaats van de bcc

☐ Sollicitatiebrieven weggegooid bij het oud papier

☐ Patiënt- of medewerkersgegevens bij de printer laten liggen

☐ Gegevens over een patiënt op een (wegwerp) handschoen geschreven

☐ Anders, namelijk...

Welke persoonsgegevens of van welke groepen personen zijn persoonsgegevens gelekt?

☐ Patiënt(en)

☐ Medewerker(s)

☐ Derden, namelijk:

Anders namelijk:

Welke bijzondere persoonsgegevens zijn er gelekt?

☐ persoonsgegevens waaruit iemands etnische afkomst blijkt;

☐ persoonsgegevens waaruit iemands politieke overtuiging blijkt;

☐ persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken;

☐ persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt;

☐ gegevens over iemands gezondheid;

☐ genetische gegevens;

☐ biometrische gegevens (bedoeld voor de unieke identificatie van een persoon)

Zijn er andere organisaties bij betrokken?

☐ Ja

☐ Nee

Onderstaande vragen zijn optioneel. Je verzamelt er extra informatie mee. Realiseer je wel dat deze lastiger zijn in te vullen door de melder. Maak hierin je eigen afweging.

Hoeverveel persoonsgegevens zijn gelekt?

- 
- ➔ Zorg dat je volledig bent in het uitvragen van gegevens die je nodig hebt, zodat er geen extra gesprek of extra vragenlijst nodig is.
 - ➔ Stel korte vragen. Het invullen moet voor de melder weinig tijd kosten, maximaal drie minuten, en makkelijk zijn.
 - ➔ Gebruikt je organisatie een ticketsysteem voor het melden van (mogelijke) datalekken? Vraag dan het ticketnummer uit op het formulier.
 - ➔ Betrek ICT bij het inrichten van het meldformulier. Onderzoek samen welke gegevens al in het systeem beschikbaar zijn en automatisch kunnen worden opgehaald. Zo hoeft de melder minder gegevens zelf in te vullen en wordt de kans op fouten kleiner.
 - ➔ Werk zoveel mogelijk met gesloten vragen of meerkeuzevragen (bijv. ja/nee, een lijst met aan te vinken van voorbeelden van datalekken).

Colofon

De toolkit Melden datalek is een uitgave van het programma Informatieveilig gedrag in de zorg (IVGZ).

Het programma Informatieveilig gedrag in de zorg wordt uitgevoerd door stichting ECP | Platform voor de Informatiesamenleving in opdracht van het ministerie van VWS. De brancheorganisaties ActiZ, de Nederlandse ggz, NFU, NHG (mede namens LHV en INEEN), NVZ, UMCNL en VGN zijn bij het programma betrokken.

Versie 2, september 2026 © Informatieveilig gedrag in de zorg

Auteurs

Bettine Pluut, Informatieveilig gedrag in de zorg
Mariët de Waal, Informatieveilig gedrag in de zorg
Maud Madsen, Informatieveilig gedrag in de zorg
Sebastiaan Stam, Informatieveilig gedrag in de zorg
Sophie Jellema, Informatieveilig gedrag in de zorg

Communicatie

Demi van Spronssen, ECP | Platform voor de Informatiesamenleving

In samenwerking met de werkgroep Melden datalek

Hiske de Vries	Senior beleidsadviseur, RAV Haaglanden
Pieter Jan Visser	CISO, Zonnehuisgroep Amstelland
Monica Bassie	Privacy Officer, Jong JGZ
Spencer Burger	Information Security Officer, Antoni van Leeuwenhoek
Lisanne Reurings	Privacy Officer, Antoni van Leeuwenhoek
Bianca Bogers	Information security officer, GGZ Westelijk Noord Brabant
Sharon van den Hemel	Privacy Officer, Korian
Petra Waelepoel	Ervaringsdeskundige patiëntenzorg
Hilde van Ras	Beleidsadviseur, Laverhof
Marije Kraan	Communicatieadviseur, Zozijn
Agnes Verbruggen	Security Officer, Kempenhaeghe
Danique Arendonk-de Ruijter	Beleidsadviseur Kwaliteit & Veiligheid, Dé Provinciale Kraamzorg Lunavi Kraamzorg

Meelezers revisie 2026

Anton Vos, Information Security Officer, Pro Persona — Boris van Moorsel, Informatieadviseur, Mesdag — Claudia Benning, Beleidsmedewerker kwaliteit & Functionaris Gegevensbescherming, DrieGasthuizenGroep — Eric Consten, Senior Privacy Officer, Ipse de Bruggen — Janneke Brandwijk, Informatieadviseur Cybersecurity, Pieter van Foreest