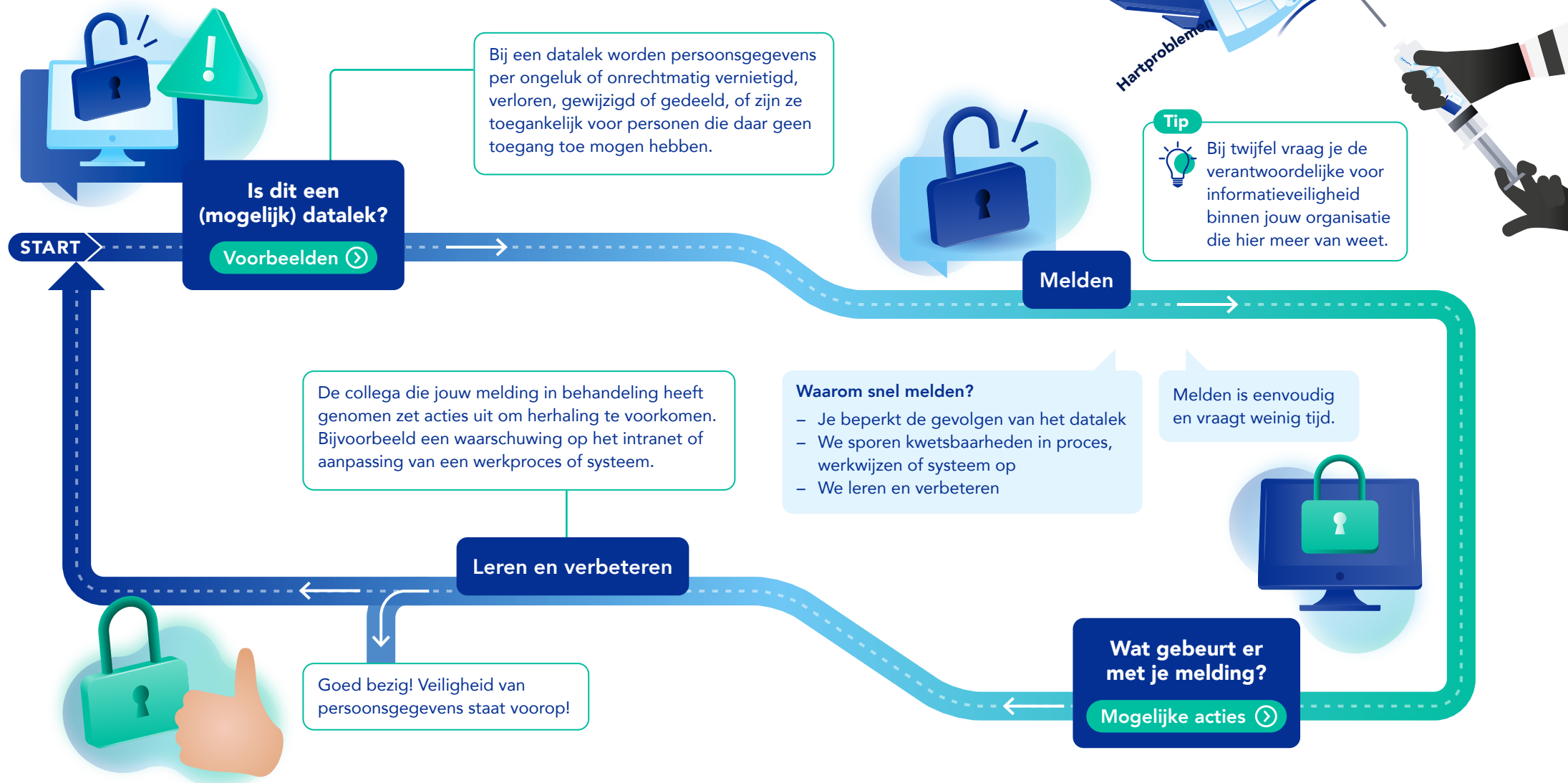


Voorbeeldproces voor medewerkers

Datalek gemeld? Leren is wat telt!



Voorbeelden van een datalek voor medewerkers



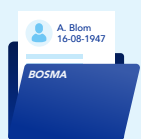
Het dossier inzien zonder dat er een behandelrelatie is.



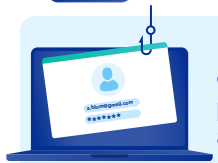
Niet-versnipperde baxterzakjes met alle patiënt- of cliëntgegevens in een open prullenbak.



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.



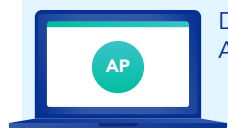
Over een patiënt/cliënt praten op een plek waar anderen kunnen meeluisteren.



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.](#)

