Stap 4: Beveiliging en Organisatie

Bij ‘Stap 1: Inventarisatie Persoonsgegevens’ bent u nagegaan welke persoonsgegevens er binnen uw organisatie (medische instelling) gebruikt worden. Bij ‘Stap 2: Verwerkingsregister en Privacy Policy’ heeft u de inventarisatie uitgebreid met de grondslag, verwerking, bewaartermijn en beveiliging van de persoonsgegevens en heeft u dit vastgelegd in een Verwerkingsregister. Ook heeft u een Privacy Policy opgesteld. Bij ‘Stap 3: Verwerkersovereenkomst’ heeft u verwerkersovereenkomsten opgesteld met derden. In deze vierde stap, ontvangt u informatie om uw beveiliging en organisatie op orde te krijgen.

Als organisatie (medische instelling) zorgt u voor technische en organisatorische beveiligingsmaatregelen om een beveiligingsniveau te bereiken voor de persoonsgegevens die u verwerkt dat past bij het risico. Doordat u medische gegevens van klanten verwerkt, dient u te zorgen voor extra goede maatregelen. Het gaat om gegevens die uit privacy-oogpunt extra aandacht behoeven.

Beveiliging

Toegangsbeveiliging van (digitale) documenten
Om zeker te weten dat alleen geautoriseerde personen de persoonsgegevens kunnen inzien en bewerken, moeten deze altijd beveiligd zijn met een wachtwoord en als het kan ook met een gebruikersnaam. Zo kunt u een Excel-bestand beveiligen met een wachtwoord en een PC voorzien van een gebruikersnaam en een wachtwoord. Zorg er dus voor dat u altijd minimaal één keer een wachtwoord moet weten voordat u de persoonsgegevens kunt inzien of bewerken.

Zorg bij bijzondere persoonsgegevens extra goed voor de toegangsbeveiliging. Hierbij brengt u eerst goed in kaart welke bijzondere persoonsgegevens u heeft en wie er toegang heeft tot deze bijzondere persoonsgegevens. Zorg er minimaal voor dat deze gegevens beveiligd zijn met een gebruikersnaam en een wachtwoord. Ook is het aan te raden om één of meerdere van onderstaande maatregelen ook te treffen:

- wachtwoord regelmatig wijzigen;
- een tweede autorisatiemethode toepassen zoals een extra code via SMS;
- automatische schermblokkering na 3 minuten van inactiviteit;
- afsluiten van ruimtes waar deze gegevens verwerkt worden;
- geen gasten op het WIFI netwerk;

LET OP: Hoe gevoeliger de bijzondere persoonsgegevens zijn, des te beter moeten de maatregelen zijn.

Beveiliging van mobiele telefoons
Als u persoonsgegevens, zoals bijvoorbeeld telefoonnummers, opslaat op een mobiele telefoon, zorg er dan voor dat er altijd een wachtwoord of een codebeveiliging aan staat op deze telefoon. Ook is het beter om een zakelijke mobiele telefoon met persoonsgegevens niet in handen van onbevoegden of kinderen te leggen. Voor u het weet, heeft u te maken met een datalek.

Beveiliging van software
Om systemen zo veilig mogelijk te laten zijn, moet u ze up-to-date houden. Zorg ervoor dat alle software ingesteld is op het automatisch ophalen en uitvoeren van updates. Zorg ook voor goede antivirussoftware. Maak goede afspraken met al uw softwareleveranciers.

U kunt zelf controleren of de website(s) van uw organisatie (medische instelling) veilig zijn via www.internet.nl (Internet.nl is een initiatief van de Internetgemeenschap en de Nederlandse overheid). Voer uw website-adres in op deze site. U krijgt dan onmiddellijk een analyse van de sterke en zwakke punten van de toegangsbeveiliging. Zo kunt u eenvoudig checken of de internetverbinding, e-mail en website wel voldoen aan moderne internetstandaarden.

LET OP: Als u persoonsgegevens verzamelt via de website, moet u in ieder geval https gebruiken. Dat voorkomt dat onbevoegde derden mee kunnen lezen met het verkeer naar de website.

Beveiliging van papieren documenten
Als persoonsgegevens ook vastliggen op papier (denk aan aanmeldingsformulieren), dan moeten die papieren met persoonsgegevens achter slot en grendel zijn opgeslagen. Praktisch: bewaar dus alle papieren met persoonsgegevens in een kast die u steeds op slot doet. Alleen personen die voor hun werk voor de organisatie (medische instelling) daarvoor toestemming hebben, mogen in die kast komen.

Een kast op slot doen is één ding, maar als de sleutels rondslingeren gaat het effect van een beveiligde opslag verloren. Onze tip is vast te leggen dat één persoon namens de organisatie (medische instelling) de sleutel(set) beheert. Zorg er ook voor dat de sleutelkast zelf (waar u alle sleutels van kasten bewaart) niet zichtbaar is van buiten het pand.

Gegevens opslaan buiten de EU
Binnen de EU is het niveau van gegevensbescherming gelijk. Dat komt omdat alle EU-lidstaten moeten voldoen aan de AVG. Als u persoonsgegevens verwerkt buiten de EU, bijvoorbeeld door deze te laten verwerken door een partij buiten de EU of een internationale organisatie, moet u kijken of er een adequaatheidsbesluit van de Europese Commissie bestaat. u moet ook weten en kunnen aantonen dat er passende of geschikte waarborgen zijn, en hoe er een kopie van kan worden

verkregen of waar ze kunnen worden geraadpleegd.

De wetgever is dus extra streng als u persoonsgegevens wilt verwerken/opslaan buiten de EU. Als u dat toch zou willen, dan moet er heel veel geregeld worden bovenop de normale AVG-verplichtingen. Dus check of uw dienstverlener (drukker, verspreider, enz.) de toevertrouwde persoonsgegevens binnen de EU opslaat.

Bij online diensten (zoals Dropbox, WeTransfer enz.) wordt het wat moeilijker. Enige terughoudendheid is vereist. Bij online diensten moet u zelf onderzoeken of deze voldoen aan de eisen. Geef altijd aan dat uw organisatie (medische instelling) domicilie heeft in Nederland (zie de verwerkersovereenkomst). Voor meer informatie: zie de voorwaarden van de dienstenaanbieders.

Als u wilt dat de organisatiedata netjes binnen de EU blijven? Hoe pakt u dat dan aan? Hier een aantal handige stappen:

1. Werk voor dit onderdeel nauw samen met de ICT-afdeling of ICT-partij. Zeker externe partijen krijgen deze vragen steeds vaker en hebben waarschijnlijk al wat antwoorden klaarliggen.
2. Begin met een beschrijving van alle software die uw organisatie (medische instelling) gebruikt, het zogenaamde softwarelandschap.
3. Geef in het landschap aan met welke softwareleveranciers u een verwerkingsovereenkomst heeft. Als het goed is staat in de verwerkersovereenkomst dat jullie data alleen binnen de EU opgeslagen mogen worden.
4. Vraag bij de overgebleven softwareleveranciers na waar de persoonsgegevens opgeslagen worden. Vaak heeft een softwareleverancier daarover al informatie staan op de website.
5. Zorg dat u de informatie bewaart waar de persoonsgegevens zijn opgeslagen. Dit geldt in het bijzonder voor leveranciers waarvan bekend is dat ze een niet-Europese achtergrond hebben.
6. Wees u er ook van bewust dat er sprake kan zijn van een keten van leveranciers. Zorg dat de eigen leverancier garant staat voor de gegevensbescherming door de partners en derden.

Data back-up

Om de persoonsgegevens te beschermen tegen het verlies of diefstal moet u back-ups maken. Het is noodzakelijk om dat regelmatig te doen. Zorg ervoor dat deze back-up veilig wordt opgeborgen.
Automatisch backups maken is de slimste manier om u te beschermen tegen ransomware maar ook tegen verlies, diefstal of brand. Hieronder een aantal do's en don'ts als het gaat om het maken van back-ups:

- Maak zo veel mogelijk automatisch back-ups, zodat u daar geen omkijken naar hebt.
- Maak verschillende back-ups bijvoorbeeld één per dag van de week.
- Zorg ervoor dat back-ups op een ander systeem staan dan waar u een back-up van maakt.
- Als u een back-up maakt op een losse harde schijf zorg er dan voor dat deze versleuteld is.
- Bewaar back-up's altijd in een goed afgesloten kast of ruimte.
- Controleer regelmatig of de back-up goed is. Dit kunt u doen door gegevens terug te lezen vanaf de back-up.

Overige beveiligingsmaatregelen

- Alle persoonsgegevens zijn alleen te bereiken via een inlog, dit kan een wachtwoord op een telefoon zijn of een gebruikersnaam en wachtwoord op een computer.
- Gebruik zoveel mogelijk versleutelde gegevensdragers als u bijzondere persoonsgegevens moet vervoeren. Hiermee zorgt u ervoor dat de persoonsgegevens voor anderen niet leesbaar zijn.
- Gebruik beveiliging op netwerkmappen en waar nodig ook op bestanden op het netwerk.
- Overweeg om meervoudige authenticatie in te voeren (naast een gebruikersnaam en een wachtwoord moet dan ook een code ingevoerd worden, die u bijvoorbeeld via SMS ontvangt).
- Sluit de website/het netwerk af voor landen waarvoor dit niet strikt noodzakelijk is.
  Toelichting: het is mogelijk om internetverkeer naar de organisatie (medische instelling) af te sluiten voor landen waar vandaan veel hackers actief zijn. Werk hierbij van binnen naar buiten, dus alleen openstellen voor landen waarvoor dat stikt noodzakelijk is.
- Als persoonsgegevens via een besloten website te benaderen zijn, moet die beveiligde internetverbinding te herkennen zijn aan het groene slotje (HTTPS).
- Als u bijzondere persoonsgegevens in uw CRM opgeslagen hebt, zorg er dan voor dat deze alleen door de juiste personen (met autorisatie) te zien zijn.
- Laat alle medewerkers een geheimhoudingsverklaring tekenen, zodat men zich bewust is van de risico’s en hun rol daarin.
- Zorg voor een goede back-up procedure met onder andere een regelmatige test van het herstellen van de gegevens.
- Test en evalueer regelmatig de maatregelen en de beveiliging.

Organisatie

Autorisatie medewerkers

Denk goed na over wie binnen de organisatie (medische instelling) bij welke gegevens moet kunnen en beschrijf dat. Door heel bewust medewerkers wel of geen toegang tot persoonsgegevens te geven, beperkt u het risico op datalekken.

Als een medewerker die niets met de persoonsgegevens te maken heeft (voor het uitoefen van de functie) daar toch bij kan, kan er sprake zijn van een datalek. In risicovolle situaties (bijvoorbeeld bij grote hoeveelheden bijzondere persoonsgegevens) moet u dat melden aan de Autoriteit Persoonsgegevens. Voorkom dat. Pas dus goed op met autorisatie en wie welke toegang heeft.

Als medewerker van een organisatie (medische instelling) of andere partijen waarmee uw organisatie (medische instelling) een verwerkersovereenkomst heeft, mag u alleen toegang hebben tot de persoonsgegevens als:

- u voor uw werk bij de organisatie (medische instelling) iets moet doen met de persoonsgegevens;
- u daarvoor toestemming (autorisatie) heeft van het bestuur of directie;
- u een geheimhoudingsverklaring of een arbeidsovereenkomst met geheimhoudingsbeding hebt getekend.

Voorbeeld geheimhoudingsbeding voor in een (nieuwe) arbeidsovereenkomst:

De werknemer is verplicht tot geheimhouding hetgeen hem uit hoofde van zijn functie ter kennis komt, voor zover die verplichting hem uitdrukkelijk is opgelegd dan wel zaken betreft waarvan de werknemer weet of redelijkerwijs kan weten dat kennisneming daarvan door derden het belang van de werkgever kan schaden. Deze geheimhouding omvat eveneens alle gegevens waarvan de werknemer uit hoofde van zijn functie van derden kennis neemt. Deze verplichting geldt ook na beëindiging van het dienstverband behoudens voor zover enig wettelijk voorschrift de werknemer tot mededeling verplicht.

LET OP: Dit is een voorbeeld, u kunt hier geen rechten aan ontlenen. U kunt het aanpassen zodat deze meer geschikt is voor uw situatie. U blijft zelf verantwoordelijk voor de inhoud en toepassing.

Vernietigen persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt. Dus: na beëindiging van een overeenkomst worden de persoonsgegevens van die persoon vernietigd.
Wijs aan wie verantwoordelijk is voor het vernietigen van persoonsgegevens of de controle op de vernietiging.

NB: Verscheuren en weggooien is onvoldoende. Schaf daarom een versnipperaar aan.

Let op: In de financiële administratie mogen (of eigenlijk: moeten!) deze persoonsgegevens nog wel blijven staan, want daar geldt een (wettelijke) bewaarplicht van 7 jaar. Voor een medisch dossier geldt dat deze minimaal 15 jaar moet worden bewaard nadat de behandeling is gestopt.

Hoe lang u gegevens mag bewaren, verschilt per geval. De AVG verplicht in elk geval een aantal zaken te regelen.

- Bepaal hoe lang u persoonsgegevens bewaart. Als dat niet mogelijk is, bepaalt u in elk geval de criteria voor het vaststellen van de bewaartermijn. Leg de bewaartermijn of de criteria vast in een bewaarbeleid (is een onderdeel van de privacy policy);
- Beschrijf de bewaartermijnen per verwerking/doelbinding in de privacy policy;
- Informeer de betrokkenen (de mensen van wie u gegevens verwerkt) over de bewaartermijnen. Dit doet u via de privacy policy en deze kunt u plaatsen op de website van uw organisatie (medische instelling).

Ga bij vernietigen na waar de gegevens van een persoon gebruikt kunnen zijn, zoals:

- de ledenlijst die in een Excel-bestand bewaard wordt op het netwerk;
- een telefoonnummer in een mobiele telefoon;
- mailtjes in een mailbox;
- een los documentje op een laptop;
- een registratie in een CRM-systeem met daaraan veel gekoppelde gegevens;
- en nog veel meer…

We geven graag onderstaande handleiding om dit onderdeel op een structurele manier te kunnen oppakken:

1. Maak een overzicht van alle systemen waarin persoonsgegevens gebruikt worden. Zo'n overzicht wordt ook wel een systeemlandschap genoemd. Let er op dat ook de back-ups in dit verhaal betrokken worden;
2. Zorg voor zo min mogelijk losse lijstjes. Geef op lijstjes aan hoe lang deze 'houdbaar' zijn en hoe deze vernietigd moeten worden;
3. Laat mailboxen automatisch opschonen en laat ook regelmatig oude contacten verwijderen;
4. Spreek af dat u altijd zorgt voor actuele gegevens in het CRM-systeem en dat men daarin moet kijken;
5. Zorg voor een duidelijke procedure voor het opschonen van het CRM. Als een persoon niet verwijderd kan worden, wis dan alle velden van deze persoon en

zet een afgesproken tekst in het veld ‘naam’ zodat u weet dat het om een gewist persoon gaat;
6. Spreek met de derden af (via de verwerkersovereenkomst) dat bestanden voor een eenmalig doel daarna worden verwijderd (bijvoorbeeld het adressenbestand dat aan een drukker wordt aangeboden voor verzending van een mailing);
7. Maak afspraken met uw medewerkers en software leveranciers om de gegevens ook echt daadwerkelijk te (kunnen) verwijderen.

Toestemming bij minderjarigen
Als u persoonsgegevens heeft van personen jonger dan 16 jaar, dan moet u daarvoor altijd schriftelijk een handtekening (op papier!) voor akkoord hebben van de ouder, verzorger of wettelijke vertegenwoordiger.

Publicatie persoonsgegevens op internet
Niemand mag zomaar persoonsgegevens (dus ook geen foto) van een ander op internet publiceren. Dit mag in principe alleen als deze persoon hiervoor toestemming geeft. Mensen hebben ook het recht om hun toestemming later in te trekken. Dat geldt dus ook als mensen deze gegevens zelf al op het internet hebben geplaatst, zoals op Facebook of LinkedIn. Reden om hier streng op te zijn: eenmaal op internet geplaatste gegevens kunnen jaren later nog vindbaar zijn en negatief zijn voor betrokkenen, bijvoorbeeld bij een sollicitatie.

Toestemming voor direct marketing
De wetgever maakt onderscheid tussen gewone direct marketing (bellen en post sturen) en digitale direct marketing (via e-mail, Facebook, LinkedIn of sms). De redenering is dat gewone direct marketing een organisatie geld kost en dus altijd beperkt zal blijven. Digitale marketing is nagenoeg gratis en kan daardoor heel veel toegepast worden, met alle gevolgen van dien. Om deze reden gelden er strengere regels voor digitale direct marketing. Bij gewone direct marketing heef u vooraf geen toestemming nodig van degene die u benadert. Bij digitale direct marketing heeft u wel vooraf toestemming nodig.

Bij het eerste direct marketing contact moet u altijd het volgende duidelijk uitleggen:

- waarom er contact opgenomen is;
- met welke partijen de organisatie (medische instelling) de persoonsgegevens zal delen;
- wat de rechten zijn om bezwaar te maken tegen deze direct marketing.

De betrokkene heeft te allen tijde het recht om bezwaar te maken tegen de verwerking van zijn gegevens voor direct-marketingdoeleinden. Als de betrokkene

een dergelijk bezwaar indient, dan mogen zijn of haar gegevens niet meer voor marketingdoeleinden worden verwerkt.

Datalekken

Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Een datalek is een beveiligingsincident waarbij persoonsgegevens gelekt zijn. Dit kan gaan om een ongeoorloofde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens. Van een datalek is alleen sprake als er persoonsgegevens zijn gelekt!

Enkele voorbeelden van datalekken:

- U raakt een USB-stick met daarop persoonsgegevens kwijt.
- Er is een laptop gestolen met daarop persoonsgegevens.
- Er is door een hacker ingebroken in een databestand of systeem (met daarop persoonsgegevens).
- Er is een mailing verstuurd met alle e-mailadressen in de Aan of CC in plaats van BCC.
- Uit een tas zijn papieren gestolen met daarop persoonsgegevens.
- Door een crash van een harddisk of door brand zijn persoonsgegevens verloren gegaan en er is geen back-up.

In bepaalde gevallen bent u verplicht melding te doen van een datalek bij de Autoriteit Persoonsgegevens. Ook kan het zo zijn dat u de betrokkenen moet informeren over het datalek. Dit zijn de personen van wie u gegevens verwerkt.

Meld u een datalek niet terwijl u dit volgens de wet wel had moeten doen? Dan kan de Autoriteit Persoonsgegevens u een (flinke) boete geven. Ook is het belangrijk dat u alle datalekken vastlegt. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of u aan de meldplicht hebt voldaan.
Als er binnen uw organisatie (medische instelling) een datalek optreedt is het belangrijk dat u de juiste actie onderneemt. U moet direct aan de slag en mogelijk moet u het incident binnen 72 uur melden bij de Autoriteit Persoonsgegevens. In sommige gevallen moet u ook de betrokkenen informeren.

LET OP: Het is belangrijk dat iedereen in uw organisatie (medische instelling) weet wat een datalek is zodat dit op tijd gesignaleerd kan worden. Zorg ervoor dat iedereen weet welke persoon in uw organisatie (medische instelling) het aanspreekpunt is bij (een vermoeden van) een datalek. Maak ook afspraken wie datalekken gaat melden bij de Autoriteit Persoonsgegevens, verkeerde meldingen kunnen voor een hoop problemen zorgen.

Stel een procedure op om actief op zoek te gaan naar mogelijke datalekken. Zo kunt u alle USB-sticks die gebruikt mogen worden voorzien van een nummer. U kunt dan

vaststellen of u er een kwijt bent. Ook kunt u met uw systeembeheerder praten over actieve maatregelen om hack-aanvallen op te sporen.