GDPR toepassen in de praktijk: stappenplan

Stap 1: Bewustwording binnen organisatie: bestuur en medewerkers

Een correcte GDPR-strategie hanteren kan maar werken als alle medewerkers binnen een praktijk zich bewust zijn van de algemene vereisten van de nieuwe regelgeving. Bij 'Tools' worden de materialen vermeld die terug te vinden zijn op onze website.

Bestuur

Om na te gaan welke verplichtingen van toepassing zijn op een praktijk of organisatie, is het belangrijk na te gaan wat de doelstellingen van de organisatie zijn, en in het kader waarvan persoonsgegevens verwerkt worden. Het belangrijkste onderdeel van de nieuwe regelgeving is het duidelijk kunnen verantwoorden waarom bepaalde gegevens verwerkt worden. In de zorgsector zijn er heel vaak wettelijke bepalingen die ingeroepen kunnen worden, ook vallen bepaalde non-profit organisaties met een opdracht vanuit de overheid voor bepaalde verwerkingen onder het algemeen belang. Volgende vragen dien je te stellen:

- Wat doen we als organisatie met persoonsgegevens?
- Hebben we deze persoonsgegevens nodig en waarom?
- Houden we alleen die gegevens bij die noodzakelijk zijn voor de verwerking?

Deze eerste korte inschatting is de eerste aanzet van de verantwoording die in onder andere de verwerkingsregisters en privacyverklaring zal meegegeven worden.

Verder dient het bestuur ook aandacht te hebben voor het informeren van de medewerkers, zodat die op een correcte manier het veiligheidsbeleid van de organisatie of praktijk volgen.

Medewerkers

Fouten in omgaan met persoonsgegevens worden snel gemaakt, en komen vaak voort uit onoplettendheid. Heel eenvoudige maatregelen kunnen genomen worden om problemen te beperken, en een correcte manier van werken te implementeren. Organiseer voor medewerkers tijdens personeelsvergaderingen, of overleg binnen de praktijk een moment waarop de nieuwe regelgeving wordt besproken, en overloop tips om op een correcte manier met persoonsgegevens om te gaan. Laat ook de medewerkers mee na denken over wat de verbeterpunten kunnen zijn in de organisatie.

TOOLS:

- Presentatie GDPR-opleiding, deel I awareness
- Artikel Huisarts Nu

Stap 2: Verwerkingsregister

In een verwerkingsregister dient vastgelegd te worden hoe en waarom persoonsgegevens worden verwerkt. Er moet aangegeven worden wat er wordt gedaan om deze gegevens veilig te verwerken, en met wie deze gegevens gedeeld worden. In de zorgsector draait de kern rond het behandelen van een patiënt en het correct beheren van het patiëntendossier, aspecten waar al veel wettelijke kaders

rond bestaan. Verder worden er mogelijk ook persoonsgegevens verwerkt in het kader van personeelsadministratie en boekhouding, deze dienen ook opgenomen te worden. Een verwerkingsregister bestaat dus over verschillende onderdelen en omvat voor alle persoonsgegevens die verwerkt worden. Let dus goed op van wie u allemaal gegevens bijhoudt of verwerkt.

TOOLS:

- model verwerkingsregister
- checklist verwerkingsregister om het model aan te vullen naar de eigen praktijk

Stap 3: Gegevensbeschermingsbeleid en risico-analyse

In het verwerkingsregister komt een oplijsting van de genomen maatregelen voor de bescherming van persoonsgegevens, of deze staan in een apart document waarnaar er in het register wordt verwezen. Het gaat niet enkel over elektronische gegevens, maar elk type verwerking van persoonsgegevens (vb. papieren klassement, afdrukken van voorschriften,...). Daarnaast zullen er binnen praktijken of organisaties nog verbeterpunten of lacunes worden opgemerkt. Neem hier de juiste stappen om deze te implementeren in de praktijk, en zorg er ook voor dat de medewerkers binnen de organisatie deze ook opvolgen. Het belang en de opvolging van het gegevensbeschermingsbeleid maakt mee onderdeel uit van de bewustwording binnen de organisatie (stap 1), en kan als regelmatig agendapunt geagendeerd en besproken worden: zijn er incidenten geweest? Wat loopt er goed en wat kan er nog beter? Worden de bewaartermijnen opgevolgd?

Zeker op te volgen binnen stap 3:

- Wat is het risico voor de betrokkene als het fout loopt?
- Worden de (papieren en elektronische) gegevens voldoende beveiligd? Worden de bewaartermijnen gerespecteerd?
- Worden de genomen maatregelen opgevolgd?

TOOLS:

- model verwerkingsregister
- checklist verwerkingsregister
- presentatie GDPR-opleiding, deel II en III

Stap 4: Informeren van betrokkenen

De GDPR vraagt dat personen van wie er gegevens verwerkt worden, goed op de hoogte worden gesteld van onder andere de redenen van verwerking, de rechtsgronden waarop er verwerkt wordt, met wie er informatie wordt gedeeld,… Een privacyverklaring die ter beschikking wordt gesteld van de betrokkene zorgt ervoor dat aan deze vereiste wordt voldaan. Er zijn wel verschillende soorten betrokkenen: personeel of medewerkers worden op een andere manier geïnformeerd dan patiënten. Het verwerkingsregister kan helpen om op te lijsten welke informatie de betrokkenen dienen te krijgen.

TOOLS:

- Inhoud Privacyverklaring
- Model privacyverklaring voor patiënten
- Model privacyverklaring voor medewerkers
- Model privacyverklaring voor leden van kring/LMN

Stap 5: Verwerkers

Er zijn heel wat bedrijven en organisaties waarmee wordt samengewerkt en die persoonsgegevens verwerken voor een praktijk of organisatie, kijk bijvoorbeeld naar een elektronisch patiëntendossier of een HR-tool. Als deze organisaties volledig in opdracht werken van de praktijk of organisatie, betreft het verwerkers, en dient er een verwerkingsovereenkomst te worden afgesloten. Andere, die ook zelf een opdracht en verantwoordelijkheid hebben (vb. ziekenhuizen, andere praktijken, mutualiteiten) zijn zelf ook verwerkingsverantwoordelijken en met hen is geen overeenkomst nodig. Als een verwerker zelf een overeenkomst bezorgt, dient er ook nagegaan te worden of deze overeenkomst conform de wettelijke verplichtingen is. Hiervoor zijn heel wat modellen en hulpmiddelen beschikbaar.

TOOLS:

- Voorbeelden verwerkersovereenkomsten
- Checklist Whitewire verwerkersovereenkomsten

Stap 6: Rechten van de betrokkene

De GDPR stipuleert heel wat rechten voor de betrokkenen waarover persoonsgegevens worden verwerkt. Deze bestaan niet los van de gangbare wettelijke kaders. Sociale zekerheidsrecht, arbeidsrecht, de wet op patiëntenrechten,… blijven van toepassing. Ook is het een misvatting dat elk recht binnen de GDPR zomaar van toepassing is. Een betrokkene kan bijvoorbeeld niet vragen om gegevens te wissen wanneer u als organisatie of praktijk hier een wettelijke verplichting rond heeft. Ga na welke rechten van toepassing zijn, en informeer hierover in de privacyverklaring. Als een betrokkene zijn recht op inzage wil uitoefenen, dient hiervoor binnen een gepaste termijn op te worden gereageerd (1 maand, verlengbaar met 1 maand, maar termijn voor patiëntendossiers is korter binnen wet patiëntenrechten). Bespreek bijvoorbeeld met uw softwarepakket hoe op dergelijke vragen kan ingegaan worden, en zorg er intern voor dat dergelijke vragen niet blijven liggen maar snel behandeld kunnen worden.

Zorg voor een procedure zodat er binnen de correcte termijn op de vraag kan ingegaan worden, en wie de communicatie rond dit soort vragen opneemt. Intern overleg zal zeker nodig zijn om gepast op de vragen van betrokkenen te kunnen antwoorden.

Rechten die vaak van toepassing zijn:

- Recht op informatie: dit wordt gevat in de privacyverklaring
- Recht op inzage: let op de termijn waarbinnen gereageerd dient te worden (korter bij patiëntengegevens : wet patiëntenrechten)
- Recht op correctie of aanpassing van gegevens
- Recht op wissing of recht op vergetelheid: enkel indien er geen geldige rechtsgrond is, meer specifiek:
    - Toestemming was rechtsgrond en deze is ingetrokken
    - Gerechtvaardigd belang was rechtsgrond en is weggevallen na terecht bezwaar betrokkene
- Recht op intrekken toestemming: enkel bij toestemming als rechtsgrond
- Recht op bezwaar: enkel bij gerechtvaardigd belang als rechtsgrond

TOOLS:

- Inhoud Privacyverklaring

- Model privacyverklaring voor patiënten
- Model privacyverklaring voor medewerkers
- Verwerkingsregister (voor het bepalen van de rechtsgronden en bijhorende rechten)

Stap 7: Incidentenregister en procedure datalek

Als er inbreuken gebeuren op de beveiliging van persoonsgegevens, dient er snel gehandeld te worden. Eerst en vooral moet worden nagegaan of het incident gemeld dient te worden aan de Gegevensbeschermingsautoriteit (voormalige Privacy commissie) of zelfs ook aan de betrokkene. In elk geval dient elke organisatie dit ook intern te registreren. Dit om bij controles aan te geven dat de juiste procedures zijn gevolgd, en om na te gaan of problemen uit het verleden voldoende zijn aangepakt om te vermijden in de toekomst.

Als een lek gemeld moet worden, dient dit binnen de 72u te gebeuren. Bekijk wie hiervoor binnen de organisatie het aanspreekpunt is bij problemen, en ook hoe er tijdig gemeld kan worden indien deze persoon niet beschikbaar is. Leg deze procedure ook vast.

TOOLS:

- Flowchart Datalekken
- Register datalekken
- https://www.gegevensbeschermingsautoriteit.be/melding-van-gegevenslekken