GDPR & BEELDBELLEN

Herwig Claeys

WAT IS DE GDPR?

De General Data Protection Regulation (GDPR) of de Algemene Verordening Gegevensbescherming (AVG) is een geheel van regels om de persoonsgegevens van Europese burgers beter te beschermen.

Persoonsgegevens zijn 'alle informatie over een natuurlijk persoon waardoor deze direct of indirect kan geïdentificeerd worden'. Dat zijn gegevens zoals o.a. naam, identificatienummer, locatiegegevens, telefoonnummers, e-mailadressen en vele andere indicatoren.

De belangrijkste pijlers van de GDPR zijn:

- Er moet **toestemming gevraagd worden** om persoonsgegevens te verzamelen en te gebruiken, en dit op een begrijpelijke manier.
- Er moet **uitgelegd worden waarom** de gegevens verzameld worden (samen met het voorgaande betekent dit 'informed consent') en er mogen niet meer gegevens verzameld worden dan nodig om een bepaalde service te bieden.
- **Opgeslagen data moeten kunnen opgevraagd, aangepast en verwijderd worden**. Wat verwijderen betreft zijn er enkele uitzonderingen, bijvoorbeeld bij medische gegevens.
- Een **meldplicht bij datalekken**. De toezichthoudende autoriteit moet hierover binnen de 72 uur geïnformeerd worden. De betrokkenen eveneens wanneer 'hun rechten en vrijheden' in het gedrang kunnen komen (zie ook verder).

Sommige persoonsgegevens hebben door hun aard een gevoelig karakter en worden daardoor als **'bijzondere categorieën van persoonsgegevens'** beschouwd. In dat geval gaat het over: ras of etnische afkomst, seksueel gedrag of seksuele voorkeur, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens of gegevens over gezondheid.

Gegevens over iemands **gezondheid** (in de brede zin van het woord) zijn gevoelige persoonsgegevens en moeten met de grootste omzichtigheid behandeld worden. Zowel de sectoren Welzijn als Gezondheidszorg dienen hier dus rekening mee te houden.

BEELDBELLEN: RECHTEN VAN DE GEBRUIKER

- **'Informed consent'**:
  - Alle privacyregels in de privacyverklaring (zie verder) moeten vooraf op een duidelijke wijze gecommuniceerd worden en de gebruiker moet expliciet akkoord gaan, via een schriftelijke verklaring of door het aanvinken van een checkbox op een website. Deze laatste optie moet via privacy-by-design op 'uit' staan zodat de gebruikers zelf de keuze kunnen maken.
  - Indien beeldbellen niet via aanmelding op een website verloopt en wanneer er geen voorafgaandelijke schriftelijke toestemming gegeven is, dan moet de gebruiker zijn 'informed consent' kunnen geven via de beeldbelapplicatie, vooraleer het contact begint.
  - Doel(en) van de gegevensverwerking moet(en) duidelijk omschreven worden. Enkel het minimum aantal persoonsgegevens die nodig zijn om het beeldbellen mogelijk te maken, mag opgevraagd worden.
  - Wanneer gegevens over het beeldbellen of gesprekken worden opgeslagen, dan moet de gebruiker hier eveneens over geïnformeerd worden en zijn toestemming geven.
- **De gebruiker heeft het recht alle opgeslagen data van de beeldbelcontacten op te vragen, aan te passen en te laten verwijderen** en moet hier eveneens over geïnformeerd worden. Een uitzondering waarbij data niet moeten verwijderd worden, is bijvoorbeeld wanneer het medische gegevens betreft of wanneer er over het verzamelen van gegevens wettelijke verplichtingen van kracht zijn.
- De gebruiker moet weten hoe en tegenover wie hij eventuele **klachten** kan formuleren.
- De gebruiker moet geïnformeerd worden wanneer zich een **datalek** heeft voorgedaan, tenminste wanneer de 'rechten en vrijheden van betrokkene' hierdoor in het gedrang kunnen komen (zie ook verder).

BEELDBELAPPLICATIES

Volgens de GDPR kunnen er verschillende partijen betrokken zijn:

- **De gegevensverantwoordelijke**: dit is doorgaans de directie of raad van bestuur van een organisatie die het beeldbellen wil aanbieden aan gebruikers/cliënten. Zij zijn de eindverantwoordelijken voor alle data die over cliënten verzameld worden door hun medewerkers en de onderstaande partijen.
- **De gegevensverwerker**: de persoon, firma of organisatie die in opdracht van de gegevensverantwoordelijke gegevens verwerkt.
- **Subverwerkers**: onderaannemers van gegevensverwerkers.

Er zijn twee mogelijkheden: ofwel wordt er beroep gedaan op een externe beeldbelaanbieder, ofwel wordt de beelbelapplicatie op de eigen servers gehost.

EXTERN

De firma/organisatie die de beelbelapplicatie aanbiedt via eigen servers (gegevensverwerker) moet kunnen verklaren dat ze 'GDPR compliant' is, na verzoek van de opdrachtgever (gegevensverantwoordelijke).

'GDPR compliant' wil zeggen:

- De nodige technische en organisatorische beveiligingsmaatregelen hebben genomen (beveiligde server, dataversleuteling, beveiligingscertificaat, enz.).

- Data bewaren op Europese servers, zonder 'omweg' via andere locaties.
- Zich ertoe verplichten datalekken onmiddellijk (binnen 72 uur) te melden aan de opdrachtgever. De gegevensverantwoordelijke moet op zijn beurt het controlerend overheidsorgaan ('Gegevensbeschermingsautoriteit') op de hoogte brengen. De gebruikers/cliënten moeten ook geïnformeerd worden wanneer 'hun rechten en vrijheden' in het gedrang kunnen komen. Dus niet wanneer het datalek geen betrekking had op hen, of wanneer hun gegevens geëncrypteerd (versleuteld) waren.
- Bijstand kunnen bieden i.v.m. de rechten van de gebruikers (bijvoorbeeld data aanleveren na opvraging, verbeteren, anonimiseren, pseudonimiseren of verwijderen).
- Eventuele subverwerkers mogen enkel ingezet worden na toestemming van de opdrachtgever (gegevensverantwoordelijke). Subverwerkers moeten aan dezelfde voorwaarden voldoen als de gegevensverwerker.
- Informatieverstrekking over alle verplichtingen tegenover de opdrachtgever (gegevensverantwoordelijke). Deze laatste heeft ook het recht op inspectie.

Het verklaren van 'GDPR compliant' te zijn, gebeurt via een schriftelijke overeenkomst. Hiervoor kunnen standaardovereenkomsten gebruikt worden (zoals bijv. die van Zorgnet of van Whitewire). Meer info op:

- https://www.zorgneticuro.be/nieuws/boek-gegevensbescherming-de-zorg-een-praktische-gids-bij-de-gdpr
- https://whitewire.be/templates/

INTERN

Een organisatie kan een beeldbelapplicatie zelf op de eigen server(s) zetten. In dat geval is ze zelf verantwoordelijk om ervoor te zorgen 'GDPR compliant' te zijn.

WAT BEVAT DE PUBLIEKE PRIVACYVERKLARING?

Een publieke privacyverklaring op een website of in de beeldbelapplicatie zelf, moet de **volgende elementen bevatten**:

- Wie de gegevensverantwoordelijke en de gegevensverwerkers zijn.
- Welke gegevens gevraagd worden.
- Wat het doel is van de gegevensverwerking.
- Waar de gegevens bewaard worden.
- Welke beveiligingsmaatregelen genomen worden.
- Hoe lang de gegevens bewaard worden.
- Wat de rechten zijn van de gebruiker/cliënt wat betreft opvragen, aanpassen en verwijderen van data.
- Met wie contact kan opgenomen worden voor vragen of klachten.

Het bovenstaande dient 'transparant' en in begrijpelijke taal verwoord te zijn. Het is dus niet nodig om de beveiliging in detail en in technische termen uit te leggen.

Wat contactmogelijkheden betreft, kunnen gegevensverantwoordelijke, projectverantwoordelijke, Data Protection Officer of DPO (indien die er is), en de Gegevensbeschermingsautoriteit vermeld worden.

WELKE DATA OPSLAAN?

In het geval van beeldbellen kan het mogelijk zijn dat bepaalde data moeten worden opgeslagen. Dit is **afhankelijk van de manier waarop een beeldbelapplicatie wordt ingezet**.

- Voor een vrij (open) beeldbelcontact hoeft mogelijk niets te worden opgeslagen.
- Voor het regelmatig beeldbellen met gekende cliënten op afspraak, kan dit wel noodzakelijk zijn. Zoals bijvoorbeeld: naam, e-mailadres, gebruikersnaam en wachtwoord.

Soms is het interessant om enkel niet-persoonsgebonden gegevens op te slaan, zoals bijvoorbeeld de postcode of het tijdstip van inbellen, maar dan zonder verdere persoonlijke gegevens.

Aandachtspunt hierbij zijn eventuele **logfiles** die worden opgeslagen wanneer er contact tot stand komt tussen hulpverlener en gebruiker/cliënt. Wanneer deze logfiles IP-adressen bevatten, dan zijn dat persoonsgegevens.

Er kan voor gekozen worden om de inhoud van de beeldbelcontacten zelf op te slaan. Bijvoorbeeld om deze achteraf te analyseren of te bespreken in een teamvergadering. In dat geval moet er met twee zaken rekening gehouden worden: 1/ het opslaan van beeldbelgesprekken vraagt zeer veel opslagruimte (en is dus duur), 2/ de beveiligingsrisico's zijn veel groter.
Vanuit GDPR standpunt gezien geldt het principe: hoe minder er opgeslagen wordt, hoe beter.

HOE LANG MOGEN GEGEVENS BEWAARD WORDEN?

De algemene regel is dat gegevens slechts voor **de kortst mogelijk tijd** mogen worden opgeslagen. Namelijk zo lang als nodig is om een bepaalde dienst te kunnen leveren waarover een overeenkomst bestaat.

Het is ten zeerste aanbevolen om de bewaartijd **te verantwoorden** in de algemene privacyverklaring van de organisatie. In ieder geval moet er een termijn op gezet worden.

Het valt het te verantwoorden om een termijn te laten ingaan vanaf de laatste keer dat een gebruiker/cliënt gebruik gemaakt heeft van een online dienst. Bijvoorbeeld de termijn van 6 maanden of 1 jaar begint te lopen na het laatste beeldbelcontact. Dit kan verantwoord worden omdat hierdoor kan voorkomen worden dat een gebruiker/cliënt telkens opnieuw een account moet aanmaken wanneer hij/zij tijdens deze periode terug contact wil opnemen.

Voor sommige gegevens is er een wettelijke bewaartermijn voorzien. Zo moeten medische gegevens gedurende 30 jaar bewaard worden. Bepaalde diensten, zoals bijvoorbeeld Centra Geestelijke Gezondheidszorg, vallen onder deze wettelijke verplichting. Het valt echter te betwijfelen dat de Gegevensbeschermingsautoriteit zal accepteren dat gegevens van CGG cliënten 30 jaar bewaard worden, wanneer ze verzameld werden via een beeldbelapplicatie die publiek toegankelijk is (grotere kans op hacking). In dat geval worden ze best na een vastgelegde periode minstens gepseudonimiseerd (zie ook verder).

AANDACHTSGEBIEDEN

KINDEREN

Met betrekking tot rechtstreeks aangeboden online diensten bepaalt de GDPR dat kinderen enkel geldig hun toestemming kunnen geven als zij **minstens 16 jaar oud zijn** (tenzij de lidstaat een lagere leeftijd bij wet voorzien heeft). Als het kind jonger dan 16 is, moet toestemming gegeven worden door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt.

Volgens de GDPR moeten verwerkingsverantwoordelijken 'redelijke inspanningen' leveren om de leeftijd van het kind te achterhalen en daaraan aangepaste taal gebruiken.

WETENSCHAPPELIJK ONDERZOEK EN STATISTISCHE VERWERKING

De GDPR voorziet voor wetenschappelijk onderzoek, bij wijze van uitzondering, dat het doel van de gegevensverwerking meer algemeen kan omschreven worden. Vaak is immers vooraf niet duidelijk voor welke doeleinden wetenschappelijk onderzoek (of statistische verwerking) zal uitgevoerd worden.

Wanneer in verband met wetenschappelijk onderzoek (of statistische verwerking) gegevens gebruikt worden of langer moeten bewaard worden dan vastgelegd in de bewaartermijn, dan moet dit gebeuren op een manier die het onmogelijk maakt om betrokkenen te identificeren. De data moeten dan geanonimiseerd of minstens gepseudonimiseerd worden.

- **Anonimiseren**: Alle persoonsgegevens worden verwijderd en vervangen door een code. Het is achteraf niet meer mogelijk om te achterhalen van wie de gegevens zijn.
- **Pseudonimiseren**: Hierbij worden gegevens getransformeerd in een dataset die niet meer direct herleidbaar is tot een persoon. De persoonsgegevens worden verwijderd en vervangen door een code. De persoonsgegevens zelf worden opgeslagen op een andere plaats. Via een sleutel kunnen later eventueel code en persoonsgegevens terug aan elkaar gekoppeld worden.

Dit document is één van de ondersteunende tools van het SIMBA-project.
Simba staat voor 'Succesvol IMplementeren van Beeldbellen in Ambulante hulp en zorg'.
Dit technologietransferproject wordt gerealiseerd door
UC Leuven Limburg MOVING MINDS — artevelde hogeschool — met de steun van AGENTSCHAP INNOVEREN & ONDERNEMEN
Dit document en andere hulpmiddelen voor het implementeren van beeldbellen
kan je vinden op: http://elearning-onlinehulp.be/simba/

Versie: 10 oktober 2018