AVG toelichting

De **Algemene Verordening Gegevensbescherming (AVG)**, ook wel de nieuwe privacywetgeving, is per 25 mei 2018 rechtstreeks van toepassing voor alle bedrijven die persoonsgegevens verwerken in alle lidstaten van de Europese Unie. De AVG, de opvolger van de Wet bescherming persoonsgegevens (WBP) in Nederland, raakt ons allemaal: cliënten, patiënten en medewerkers van (zorg)instellingen. De AVG is van toepassing op elke organisatie die persoonsgegevens verwerkt. Niet naleven van de AVG kan leiden tot forse boetes (tot 20 miljoen of 4% van de jaaromzet), opgelegd door de **Autoriteit Persoonsgegevens (AP)**.
Het doel van de AVG is om twee belangen te waarborgen. Enerzijds de bescherming van natuurlijke personen i.v.m. de verwerking van hun (deels of geheel geautomatiseerde) gegevens, anderzijds het vrije verkeer van persoonsgegevens binnen de EU door harmonisatie van regelgeving. Een organisatie mag niet zomaar persoonsgegevens verwerken, maar moet hiervoor een rechtsgrondslag hebben.
DFZS valt onder de AVG, omdat wij (bijzondere) persoonsgegevens verwerken van zowel patiënten/cliënten (zoals medische en strafrechtelijke gegevens) als medewerkers (denk aan adressen en financiële gegevens). DFZS heeft verschillende grondslagen voor de verwerking van deze gegevens, zoals het vragen van toestemming en/of het aangaan van een vrijwillige overeenkomst (patiënt/cliënt of medewerker meldt zichzelf aan om in zorg of dienst te komen) of een wettelijke verplichting voortvloeiend uit een straf- of civielrechtelijke maatregel die ons 'dwingt' tot gegevensverwerking.
Zorgspecifieke privacyregels blijven naast de AVG van kracht, zoals die volgen uit de Wet Geneeskundige Behandelovereenkomst (WGBO), Bijzondere Opnemingen in Psychiatrische Ziekenhuizen (BOPZ), Beginselenwet verpleging ter beschikking gestelden (Bvt), Wet kwaliteit, klachten en geschillen zorg (Wkkgz), Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG) en de Zorgverzekeringswet (Zwv). De AVG brengt geen veranderingen met zich mee voor het medisch beroepsgeheim.

Hoofdbeginselen AVG:
Op grond van de AVG moet elke verwerking van persoonsgegevens voldoen aan het volgende:

- De verwerking van persoonsgegevens moet **rechtmatig, behoorlijk en transparant** zijn. Er moet een toestemming, contract, overeenkomst, wettelijke plicht of aanmerkelijk belang ten grondslag liggen aan de noodzaak tot verwerking.
- De verwerking moet gebonden zijn aan specifieke verzameldoelen (**doelbinding**). Het verzamelen dient een doel te hebben passend bij de grondslag hierboven. Denk aan het kunnen uitbetalen van salaris of dossiervorming voor het uitvoeren van een behandeling.
- De persoonsgegevens moeten **toereikend zijn en beperkt** tot wat noodzakelijk is. Er mag niet meer data worden verzameld dan nodig is voor het doel.
- De gegevens moeten **correct en juist** zijn.
- De gegevens (digitaal en op papier) mogen **niet langer worden bewaard** dan nodig met inachtneming van andere wettelijke bewaartermijnen die van toepassing kunnen zijn (bijv. dossiers onder WGBO 15 jaar, BOPZ 15 jaar en Tbs waarschijnlijk 10 jaar, maar regelgeving volgt).
- Gegevens moeten **goed beveiligd zijn** en vertrouwelijk blijven. Passende maatregelen in relatie tot het risiconiveau van de persoonsgegevens moeten worden genomen, zoals het gebruik van wachtwoorden, autorisaties, beveiligde mail, afgesloten kasten met dossiers etc.

Gestelde eisen:
De AVG stelt een aantal eisen waaraan voldaan moet worden. De eisen luiden als volgt:

1) Organisaties dienen een **verwerkingsregister** op te stellen waarin zij hun belangrijkste en meest risicovolle verwerkingsactiviteiten identificeren, beschrijven wie er verantwoordelijk voor zijn en onder welke wettelijke grondslag deze verwerkingen mogen plaatsvinden. Risico's voor grootschalige verwerkingen moeten in kaart worden gebracht en evt. beheersmaatregelen beschreven.

2) Het opstellen van v**erwerkersovereenkomsten** met alle organisaties/bedrijven die in opdracht persoonsgegevens verwerken. Zij worden daarmee verplicht aan alle AVG-eisen te voldoen. Denk aan de leverancier van een Elektronisch Patienten Dossier (EPD) of een kantoor voor de salarisadministratie.
3) Grotere (zorg)organisaties dienen een **Functionaris Gegevensbescherming** (FG) aan te wijzen en in te schrijven bij de AP. Deze houdt de organisatie scherp op de bescherming van persoonsgegevens.
4) Organisaties dienen een **privacy- of beveiligingsbeleid** op te stellen en passende maatregelen te nemen voor beveiliging van gegevens. Dit past meestal bij een certificering (ISO 27001 of NEN 7510) op het gebied van informatiebeveiliging.
5) Organisaties moeten een **datalekmeldpunt** inrichten, tijdig melden bij de Autoriteit Persoonsgegevens en de gedupeerden inlichten.
6) **Privacy by design**; nieuwe verwerkingen, dienen meteen conform de AVG worden ingericht.
7) Organisaties moeten intern de **bewustwording** vergroten van de noodzaak tot bescherming van privacygevoelige gegevens.

Om aan deze eisen te voldoen heeft DFZS een verwerkingsregister opgesteld en een risico-inschatting gemaakt voor de meest belangrijke verwerkingen, de verwerkersovereenkomsten met derden aangepast middels een addendum op de bestaande contracten, een Functionaris Gegevens-bescherming aangesteld, een privacyreglement en een informatiebeveiligingsbeleid opgesteld, een datalekmeldpunt ingericht, het nieuwe EPD als voorbeeld voor privacy-by-design genomen en het belang van privacy (opnieuw) onder de aandacht van de medewerkers gebracht.

Wat zijn de rechten van diegenen wiens gegevens worden verwerkt?
De AVG heeft niet alleen een aantal eisen voor organisaties gesteld, ook is in kaart gebracht wat het recht van een ieder is. Hieronder een overzicht:

8) Het **recht op informatie** over de verwerkingen; waar worden de gegevens voor gebruikt en wat zijn de rechten?
9) Het **recht op inzage en een afschrift** (1^{e} kopie is kosteloos) van de eigen gegevens (rekening houdend met de verschillende specifieke wetten). Ook een digitaal afschrift (indien mogelijk) is een recht van betrokkene.
10) Het **recht op correctie**; feitelijke onjuistheden mogen worden gecorrigeerd (daaronder valt niet het oneens zijn met het behandelplan, diagnostiek of ontkenning van het delict etc.). Ook mag er **bezwaar** worden gemaakt tegen bepaalde gegevens in een dossier.
11) Het **recht op verwijdering van gegevens** (tenzij nodig voor derden of klachtafhandeling) na afloop van wettelijke termijnen (BOPZ 15 jaar en Tbs 10 jaar).
12) Het recht om niet onderworpen te worden aan **geautomatiseerde besluitvorming**; niet van toepassing bij DFZS.

Om aan deze rechten te voldoen heeft DFZS de bestaande privacyverklaring op de website aangepast met een uitgebreide toelichting voor zowel opgenomen patiënten met een maatregel als poliklinische (deels) vrijwillige cliënten, waarin wordt uitgelegd wat er wordt verzameld, waarom en welke rechten patiënten/cliënten hebben als het gaat om hun privacy. De privacyverklaring en toelichtingen zijn voor iedereen via de website te downloaden en worden ook bij opname en intake uitgedeeld.