Brevidius/MyWepp

Informatieveiligheidsbeleid

Publieke beleidsverklaring | Oktober 2026

MyWepp ondersteunt cliënten, naasten en zorgprofessionals met digitale toepassingen voor communicatie, instructie, begeleiding en dagelijks overzicht (dagstructuur). Aangevuld met op ontspanning gerichte content en functies. Daarbij verwerken wij informatie die persoonlijk en soms gevoelig is. Een zorgvuldige en veilige omgang met deze informatie is daarom een essentieel onderdeel van onze dienstverlening.

Onze uitgangspunten

MyWepp streeft naar passende bescherming van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie. Alleen bevoegde personen krijgen toegang tot gegevens die zij voor hun werkzaamheden/begeleiding nodig hebben. Wij houden rekening met privacy en informatiebeveiliging bij de ontwikkeling, inrichting en het beheer van onze diensten.

Beveiliging in de praktijk

Wij richten organisatorische en technische maatregelen in op basis van risico's. Daarbij gaat het onder meer om toegangsbeheer en authenticatie, passende autorisaties, beveiligde gegevensoverdracht, beheer van systemen en updates, back-ups, monitoring en het zorgvuldig omgaan met gegevens gedurende de gehele levenscyclus. De concrete inrichting wordt periodiek beoordeeld en waar nodig aangepast.

Medewerkers en leveranciers van Brevidius/MyWepp

Medewerkers en externe betrokkenen hebben een verantwoordelijkheid voor veilig werken en vertrouwelijke omgang met informatie. Met leveranciers en andere partijen die namens MyWepp gegevens verwerken, maken wij passende afspraken over beveiliging, geheimhouding en privacy. Toegang tot systemen en gegevens wordt afgestemd op rollen en taken.

Incidenten, risico's en continuïteit

MyWepp besteedt structureel aandacht aan het herkennen, beoordelen en beperken van informatiebeveiligingsrisico's. Vermoedelijke beveiligingsincidenten worden gemeld, onderzocht en waar nodig opgevolgd. Bij incidenten met persoonsgegevens handelen wij overeenkomstig de toepasselijke meldverplichtingen. Wij treffen passende maatregelen om de continuïteit en het herstel van onze dienstverlening te ondersteunen.

Wet- en regelgeving en certificering

Wij houden rekening met de Algemene verordening gegevensbescherming (AVG) en relevante eisen voor informatiebeveiliging in de zorg. Dat is vastgelegd in ons ISMS, dat de basis is voor onze certificering voor ISO 27001 en NEN 7510. Wij evalueren ons beleid en onze maatregelen periodiek en verbeteren deze op basis van risico's, ervaringen en ontwikkelingen in wetgeving en technologie.

Verantwoordelijkheid en contact

De directie van MyWepp is verantwoordelijk voor de uitgangspunten van dit beleid. Iedereen die voor of namens MyWepp werkt, draagt bij aan de uitvoering ervan. Vragen over privacy of informatiebeveiliging kunnen via de gebruikelijke contactkanalen van MyWepp worden gesteld.

Deze verklaring beschrijft de algemene uitgangspunten. Nadere afspraken met klanten worden waar van toepassing vastgelegd in overeenkomsten en bijbehorende privacy- en beveiligingsdocumentatie.