Autorisatiebeleid Stichting Zeeuwse WensAmbulance

Dit autorisatiebeleid beschrijft hoe de Zeeuwse WensAmbulance toegang tot persoonsgegevens reguleert en beveiligt. Het beleid is opgesteld in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en het privacyreglement van de Zeeuwse WensAmbulance.

1. Doelstelling

Het autorisatiebeleid heeft als doel om:

- Ongeautoriseerde toegang tot persoonsgegevens te voorkomen.
- De vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens te waarborgen.
- Toegang tot persoonsgegevens te beperken tot geautoriseerde vrijwilligers en vrijwilligers die deze gegevens nodig hebben voor de uitvoering van hun werkzaamheden.

2. Rollen verantwoordelijkheden

- Aanvragenbeheerder: Ontvangt alle wensaanvragen en zet deze uit naar een persoon die de medische gegevens beoordeelt en een akkoord kan geven.
- Medisch beoordelaar: Heeft toegang tot de medische gegevens van de wensvrager en beslist of de wens uitvoerbaar is.
- Wenscoördinator: Ontvangt de goedgekeurde aanvragen en stuurt de vrijwilligers aan.
- Bestuursleden: Hebben beperkte toegang tot vrijwilligersgegevens en relevante informatie voor beleidsvoering.
- Vrijwilligers bij wensrit: Krijgen alleen op de dag van uitvoering tijdelijk toegang tot de gegevens van de wensvrager die nodig zijn voor de uitvoering van de wens.

3. Autorisatieniveaus

Toegang tot persoonsgegevens wordt geregeld op basis van het ‘need-to-know’ principe. De volgende autorisatieniveaus worden gehanteerd:

- Algemeen toegangsniveau: Basisinformatie over de organisatie en algemene contactgegevens.
- Beperkt toegangsniveau: Bestuursleden en wenscoördinatoren hebben toegang tot vrijwilligersgegevens en planning.
- Uitgebreid toegangsniveau: De medisch beoordelaar heeft toegang tot medische gegevens van wensvragers.
- Tijdelijk toegangsniveau: Vrijwilligers die een rit uitvoeren, ontvangen op de dag van de wens een e-mail met de gegevens van de wensvrager. Het wachtwoord om deze gegevens in te zien wordt separaat toegestuurd. Na de rit wordt deze e-mail verwijderd.

4. Toegangsbeveiliging

- Medische gegevens worden bewaard in een beveiligde map met Two-Factor Authentication (2FA).
- Vrijwilligersgegevens zijn alleen toegankelijk voor bestuursleden en de wenscoördinator, eveneens beveiligd met 2FA.
- Toegangsrechten worden periodiek geëvalueerd en aangepast bij functiewijzigingen of beëindiging van werkzaamheden.
- Inloggegevens en wachtwoorden zijn persoonlijk en mogen niet worden gedeeld.

5. Incidentenbeheer

- Onregelmatigheden worden gemeld aan het bestuur en indien nodig onderzocht.
- Bij een (vermoedelijk) datalek wordt dit direct gemeld aan het bestuur en wordt geregistreerd met daarbij de genomen maatregelen.
- Het bestuur bepaalt of en hoe betrokkenen en de Autoriteit Persoonsgegevens op de hoogte gesteld moeten worden.

6. Evaluatie

Dit beleid wordt minimaal eens per jaar geëvalueerd en aangepast indien nodig, mede op basis van technische ontwikkelingen en wijzigingen in wet- en regelgeving.

Datum publicatie: maart 2025

Laatste evaluatie: maart 2026- geen wijzigingen

Volgende evaluatie: maart 2027