Dataverkeerbeleid Zorgcentrum Het Leefhuis.

1. Doel van het beleid.

Het doel van dit dataverkeerbeleid is om de bescherming van persoonsgegevens te waarborgen door te reguleren hoe en onder welke voorwaarden gegevens tussen de zorginstelling, haar medewerkers, externe partijen en softwaresystemen worden gedeeld en overgedragen. Het beleid is van toepassing op alle vormen van gegevensoverdracht binnen de zorginstelling, inclusief maar niet beperkt tot e-mail, applicaties, opslag en netwerken.

2. Algemeen beleid voor dataverkeer.

De zorginstelling maakt gebruik van verschillende softwareprogramma's en systemen voor het verwerken van persoonsgegevens, zoals onder andere Carefriend, Yorganizr, NAS, Zivver, Siilo, en Colabaris. Dit dataverkeerbeleid geldt voor alle uitwisselingen van gegevens die plaatsvinden via deze systemen.

3. Soorten gegevens die gedeeld kunnen worden.

Gegevens die gedeeld worden binnen de zorginstelling kunnen onder andere bestaan uit:

- Persoonsgegevens van deelnemers (naam, adres, geboortedatum, zorgvraag, enz.).
- Gegevens over medische behandeling en/of begeleiding, voortgang, medicatie en zorgverlening.
- Gegevens met betrekking tot zorgplan en begeleidingsdoelen.
- Administratieve gegevens zoals facturering, declaraties, en planning.
- Beveiligde e-mails en/of berichten (bijvoorbeeld via Zivver) met vertrouwelijke informatie.

4. Beveiliging van dataverkeer

Alle gegevens die overgedragen of ontvangen worden via digitale kanalen dienen te voldoen aan de wettelijke eisen van de AVG en het dataverkeerbeleid. Specifieke maatregelen omvatten:

- Versleuteling van persoonsgegevens tijdens overdracht, met gebruik van versleutelde e-mail (Zivver) en versleuteling van databases en bestanden.
- Gebruik van beveiligde netwerken en VPN's voor interne communicatie.
- Authenticatieprotocollen voor toegang tot gegevens (bijvoorbeeld multi-factor authenticatie).
- Toegang wordt strikt beperkt tot geautoriseerde medewerkers en partijen op basis van functiebehoeften.

5. Maatregelen bij datalekken

In het geval van een datalek moet het dataverkeerbeleid de volgende maatregelen bevatten:

- Directe meldingen bij de verantwoordelijke voor gegevensbescherming (DPO).
- Beoordeling van de aard en ernst van het datalek.
- Melding aan de Autoriteit Persoonsgegevens indien het datalek een hoog risico voor de betrokkenen met zich meebrengt.
- Informatie en instructies aan betrokkenen (bijvoorbeeld de deelnemers van de zorginstelling).
- Correctieve maatregelen om herhaling te voorkomen (bijvoorbeeld een aanpassing van systemen of processen).

6. Gegevensdoorgiften naar derden

Wanneer gegevens gedeeld worden met externe partijen (zoals gemeenten, softwareleveranciers, of andere zorginstellingen), moet dit plaatsvinden op een manier die voldoet aan de vereisten van de AVG:

- Er moeten duidelijke afspraken worden gemaakt met de externe partijen, die worden vastgelegd in verwerkersovereenkomsten.
- Alle gegevens die doorgestuurd worden, worden volgens de wettelijke richtlijnen beveiligd.
- Voor doorgifte van persoonsgegevens buiten de EU is toestemming nodig van de betrokkenen en moeten aanvullende maatregelen worden getroffen, zoals het afsluiten van modelovereenkomsten.

7. Specifieke software en gegevensuitwisseling

Specifieke Software en Gegevensuitwisseling - Zorginstelling

Software/Applicatie	Wat is het?	Soorten Gegevens	Gegevensverkeer	Beveiligingsmaatregelen	Deelnemers	Bewaartermijn
Carefriend	Rapportagesysteem voor zorgdossiers en (voortgang)rapportages.	- Naam, geboortedatum, zorgbehoefte, begeleidingsplan, doelen, starterspakket, indicatiegegevens, medicatie, voortgang, risicogedrag, risicobeschrijvingen, MIC/MIM-meldingen.	Gegevensuitwisseling tussen zorginstelling en zorgverleners.	- Versleuteling van data. - Authenticatie via multi-factor. - Beveiligde opslag. - Periodieke audits van toegangsrechten.	Deelnemers, zorgverleners	15 jaar na laatste zorgcontact
Yorganizr	Software voor de planning van zzp'ers.	- Initialen van deelnemers, zorgvorm, begeleidingsbehoeftes, adres (indien vervoer door de zorginstelling vorm wordt gegeven), planning van zzp'ers.	Gegevensuitwisseling tussen zorginstelling, zzp'ers en medewerkers over zorgplanning.	- Versleuteling van gegevens. - Toegang op rol gebaseerd niveau. - Regelmatige audits van toegang. - Beveiligde verbindingen.	Deelnemers, zzp'ers, zorgverleners	7 jaar na beëindigen zorgverlening
Zivver	Beveiligde e-mail voor het versturen van vertrouwelijke informatie tussen zorginstelling en externe partijen.	- Persoonsgegevens, zorginformatie, voortgang, indicatieverlenging, evaluatie.	Beveiligde communicatie met derden, zoals gemeenten en zorgkantoor.	- End-to-end encryptie van berichten. - Verplicht gebruik van Zivver voor e-mailverkeer. - Loggen van communicatie. - Authenticatie.	Deelnemers, zorgverleners	5 jaar na laatste communicatie
NAS (Network Attached Storage)	Opslag van organisatie- en deelnemer gegevens voor interne en externe toegang.	- Persoonsgegevens, gezondheidsgegevens, medewerker- en zzp'er gegevens, kwaliteitsmanagementdocumenten.	Interne gegevensopslag, maar soms extern gedeeld voor rapportages of audits.	- Versleuteling van gegevens. - Beveiligde toegang via rol gebaseerde toestemming. - Back-up en herstel. - Loggen van toegang.	Deelnemers, medewerkers, zzp'ers	7 jaar na laatste zorgcontact of volgens wetgeving
Siilo	Beveiligde communicatie-app voor zorgverleners om onderling informatie uit te wisselen over deelnemers.	- Initialen van deelnemers, zorgbehoeften, voortgangsrapportages.	Beveiligde berichtenuitwisseling tussen zorgverleners binnen de zorginstelling.	- End-to-end encryptie. - Beperkingen voor toegang tot specifieke communicatiekanalen. - Beveiligde netwerken. - Periodieke audits van toegang.	Deelnemers, zorgverleners	6 maanden na laatste bericht
Colabaris	Software voor het declaratieproces met gemeenten en communicatie over zorg met de gemeente.	- Persoonsgegevens, zorgbehoeften, zorgdoelen, zorgvormen voor declaraties.	Gegevensuitwisseling tussen zorginstelling en gemeenten/zorgkantoor voor declaratieverwerking.	- Beveiligde communicatie. - Versleuteling van gegevens. - Beperkingen op toegang.	Deelnemers, gemeenten	7 jaar na laatste declaratie

				- Loggen van gegevensuitwisseling.		
Kloksystemen	Registratiesysteem voor werktijden van medewerkers bij ambulante begeleiding, inclusief locatiegegevens.	- Locatie (latitude, longitude), deelnemer naam, zorgvorm, begeleider, aantal uren, datum.	Gegevens worden verzameld via mobiele apparaten bij ambulante zorgverlening en geregistreerd in het systeem.	- Versleuteling van locatie- en tijdsdata. - Beveiligde inlog. - Gecontroleerde toegang tot registraties. - Gegevensopslag via versleutelde servers.	Deelnemers, zorgverleners	2 jaar na laatste registratie
Noodkaarten	Noodkaarten met belangrijke gegevens over deelnemers voor gebruik in noodgevallen.	- Voor- en achternaam, geboortedatum, telefoonnummer, adres, huisartsgegevens, verzekeringsgegevens, allergieën, zwemdiploma.	Gegevens worden alleen verstrekt aan hulpdiensten (politie, brandweer, artsen) bij noodgevallen.	- Gegevens zijn versleuteld. - Beveiligde toegang tot kaarten. - Fysieke beveiliging van papieren kaarten. - Enkel toegankelijk voor hulpdiensten.	Deelnemers, ouders/verzorgers	1 jaar na beëindiging zorgverlening
Aanwezigheidsapp	App voor het registreren van de aanwezigheid van deelnemers en de zorgverlening die zij ontvangen.	- Voor- en achternaam van de deelnemer, zorgvorm, begeleider, uren, locatiegegevens (latitude, longitude), e-mail van betrokkenen.	Gegevens worden verzameld via mobiele apparaten en gedeeld met zorgverleners voor registratie van aanwezigheid.	- Versleuteling van gegevens bij overdracht. - Beveiligde toegang tot de app. - Toegang alleen voor geautoriseerde medewerkers. - Periodieke controle van het dataverkeer.	Deelnemers, zorgverleners	7 jaar na laatste registratie

---

8. Evaluatie en updates

Het dataverkeerbeleid wordt jaarlijks geëvalueerd en geüpdatet om te waarborgen dat het in lijn blijft met de wetgeving, de technologie en de kwaliteit die de zorginstelling wil leveren en waarborgen. De evaluatie wordt uitgevoerd door de gegevensbeschermingsfunctionaris (DPO) in samenwerking met de IT-afdeling en het management.

Verwerkingsregister en dataverkeerbeleid in combinatie

Dit dataverkeerbeleid is een integraal onderdeel van het verwerkingsregister. Het verwerkingsregister moet bijhouden welke gegevens worden verwerkt, welke software wordt gebruikt, wie toegang heeft tot de gegevens, en welke technische en organisatorische maatregelen er worden genomen om dataverkeer te beveiligen.

Acties bij datalekken: *Wanneer er een datalek wordt vastgesteld, moet de procedure zoals eerder beschreven worden gevolgd, met nadruk op de melding aan de betrokkenen en de Autoriteit Persoonsgegevens, en het nemen van corrigerende maatregelen.*