Informatie- en beveiligingsprotocol

de Zorgnijverij

met hart en handen

Inhoudsopgave

Inleiding

Ter uitvoering van het privacyreglement heeft de Zorgnijverij een informatie- en beveiligingsprotocol. De Zorgnijverij heeft op grond van artikel 10.5 en 10.6 zowel technische als organisatorische maatregelen genomen om de persoonsgegevens welke op grond van het privacyreglement worden verwerkt, te beveiligen. In dit informatie- en beveiligingsprotocol is daarnaast opgenomen hoe de Zorgnijverij op het gebied van de cliënt en de medewerker uitvoering geeft aan het privacybeleid.

1. Technische maatregelen

Computerbeveiliging

- De computers die eigendom zijn van de Zorgnijverij, beschikken over Windows met Windows Defender; met regelmaat wordt gecontroleerd op updates en ook updates van bijv. browsers worden regelmatig uitgevoerd

Dossier

- Dossiervorming van de cliënten vindt alleen plaats binnen Carefriend; dit is een goed beveiligde Cloud oplossing, waar alleen medewerkers met eigen inlog in combinatie met een token toegang toe hebben; de informatie waartoe zij toegang hebben, is functie gebonden; Carefriend kent een eigen back-up systeem.

- Dossiervorming van de personeelsleden vindt alleen plaats binnen de SharePoint; dit is een goed beveiligde Cloud oplossing, waar alleen medewerkers met eigen inlog in combinatie met een tweestapsverificatie toegang toe hebben; de informatie waartoe zij toegang hebben, is functie gebonden.

Communicatie

- De e-mailomgeving is beschermd door middel van een tweestapsverificatie. De emailomgeving is onderdeel van Microsoft Office 365. Het back-up proces door Microsoft is ingericht om zelf te kunnen gebruiken in geval van een calamiteit. Microsoft maakt elke 12 uur een back-up en bewaart deze 14 dagen.

- Met de gemeente wordt gecommuniceerd via een beveiligde mailomgeving. Hierbij wordt gebruik gemaakt van ‘Zorgmail’, waarbij een mail wordt gestuurd in een afgesloten omgeving. De Zorgnijverij ontvangt via de gemeente een code om deze mail te openen.

- Met hoofdaannemers wordt gecommuniceerd via diverse kanalen. Vooralsnog wordt er veel gebruik gemaakt van de reguliere mailomgeving. Sommige hoofdaannemers communiceren via een beveiligde omgeving, zoals Zorgmail.

- Voor de cliënten met een Wmo-indicatie wordt er gecommuniceerd met de gemeente via ‘Vecozo’. Dit is een beveiligd communicatieomgeving, waar

voortdurend alles in het werk wordt gesteld om privacygevoelige informatie zo goed mogelijk te beschermen.

2. Organisatorische maatregelen

- Abonnement bij Stichting Privacy zorg inclusief Functionaris Gegevensverwerking (FG).
- Gedragscode privacy.
- Samenwerking met Qurentis & Carefriend, waarbij Qurentis voldoet aan de AVG-norm en hebben de certificaten NEN 7510:2017 en NEN-ISO/IEC 27001:2017 ontvangen. Het hele Information Security Management System (ISMS) is kritisch onderzocht en beoordeeld. Onderdeel van deze audit bij Qurentis was een uitgebreid documentenonderzoek en ook werd ons bedrijf specifiek op de implementatie van de AVG beoordeeld.
- Geheimhoudingsverplichting in arbeidsovereenkomsten.
- Register verwerking persoonsgegevens (waarin ook de bewaartermijnen zijn vastgelegd); bij de opstelling van dit register is gekeken op welke gebieden het aantal persoonsgegevens verminderd kan worden.
- Bij wijziging van het register verwerking persoonsgegevens wordt op grond van artikel 35 lid 7 AVG een gegevensbeschermingseffectbeoordeling uitgevoerd. [1]
- In de procedure datalek is opgenomen hoe wordt omgegaan met datalekken.

3. Uitvoering privacybeleid

Cliënten

De uitvoering van het privacybeleid voor cliënten en cliëntvertegenwoordiger wordt nader vormgegeven via processen en protocollen. Onderstaand wordt verwezen naar de verschillende documenten welke in de praktijk een uitwerking van het privacybeleid:

Kernprocessen

- Zorgproces
    - Aanmelding en intake - Stuurt het vroegtijdig verstrekken van informatiebrochure met daarin een paragraaf over dossier en privacy, verwijst naar diverse plaatsen van opslag van persoonsgegevens.
    - Planning en Evaluatie - Regelt bewaarplaats van dossiervorming, verwijst naar diverse plaatsen van opslag van persoonsgegevens.
    - Uitvoering - Regelt plaats van rapportage, setting van begeleiding.
    - Cliëntadministratie - Regelt beheer cliëntdossier.

- Personeelsmanagement - Regelt verstrekking huishoudelijk reglement, zaken rondom instroom en uitstroom zoals verstrekking van passen/sleutels/devices/inloggegevens.

[1] De minimale kenmerken van een gegevensbeschermingseffectbeoordeling zijn beschreven in artikel 35 lid 7 en overwegingen 84 en 90 AVG.

Procedures en protocollen

- Medicatie - Regelt bewaarplaats van medische informatie en de eisen rondom informatieoverdracht.
- Klachten - Regelt bewaarplaats van dossiervorming, anonimisering van gegevens en maximale bewaartermijn.
- Incidenten - Regelt bewaarplaats van dossiervorming, anonimisering van gegevens en maximale bewaartermijn, omgang met datalekken.
- Huiselijk geweld en kindermishandeling - Regelt in welke gevallen de geheimhoudingsplicht op welke wijze mag worden doorbroken.
- Inzage, wijzigen en vernietigen dossier gegevens - Regelt wanneer en hoe inzage, wijziging en vernietiging van gegevens gerealiseerd kan en mag worden.

Overige documenten

- Zorgovereenkomst - Samenvatting van privacyafspraken.
- Contract medewerkers en vrijwilligers - Regelt geheimhoudingsplicht.
- Contracten leveranciers software waarin/mee persoonsgegevens worden verwerkt.
- Toestemmingsformulier uitwisseling gegevens - Regelt toestemming van cliënt voor het uitwisselen van gegevens met specifiek benoemde instanties.
- Informatieboekje De Zorgnijverij - Bevat een paragraaf over; dossier en privacy als voorlichting over waar en hoe gegevens bewaard en beschermd worden, vertrouwenspersoon, geheimhoudingsplicht)
- Personeelshandboek - Bevat verwijzingen naar alle documenten inzake privacy, bevat kantoorregels en de gedragscode; o.a. papiervernietiger, als medewerker bij cliënt is en telefonisch iets doorkrijgt over een andere cliënt en alleen aannemen buiten aanwezigheid van andere cliënt, wanneer bekende/familielid van zorgverlener in zorg is bespreken met bestuurder, notulen en agenda waardevrij beschrijven en geen direct herleidbare persoonsgegevens in opnemen.

Autorisaties

- Er zijn per medewerker gebruikersrechten toegekend voor het gebruik van software van de organisatie door middel van een wachtwoord. Het wachtwoord is persoonsgebonden en mag niet worden doorgegeven. Medewerkers mogen alleen die persoonsgegevens inzien die voor hun taakuitoefening noodzakelijk zijn.
- Back-up regeling - Er wordt dagelijks een back-up gemaakt van het automatiseringsprogramma zodat gegevens niet verloren gaan.

Medewerkers

De uitvoering van het privacybeleid voor medewerkers, stagiaires en vrijwilligers wordt nader vormgegeven via processen en protocollen en diverse andere documenten. Onderstaand wordt verwezen naar de verschillende documenten welke in de praktijk een uitwerking van het privacybeleid:

Kernprocessen

- Administratie - Personeelsadministratie regelt beheer personeelsdossier, bewaarplaats en regels rondom kopie identiteitsdocument, werkwijze rondom VOG-verklaring.
- Personeelsmanagement - Regelt verstrekking huishoudelijk reglement, beveiliging en bewaartermijnen gegevens van sollicitanten, richtlijnen voor functioneringsgesprekken en opslag van informatie daaruit.

Procedures en protocollen

- Klachten - regelt bewaarplaats van dossiervorming, anonimisering van gegevens en maximale bewaartermijn.
- Incidenten calamiteiten ongevallen - Regelt bewaarplaats van dossiervorming, anonimisering van gegevens en maximale bewaartermijn.
- Verzuim - Richtlijnen voor ziek- en herstel meldingen.

Overige documenten

- Personeelshandboek - Bevat verwijzingen naar alle documenten over privacy, bevat kantoorregels en de gedragscode.
- Zorgovereenkomst (schending privacy medewerker kan reden zijn tot beëindiging zorg).

Versiebeheer

Versie 2.0 JdW – Technische en organisatorische maatregelen welke eerst waren opgenomen in het Privacyreglement zijn in een apart document verwerkt als uitwerking van het Informatie- en beveiligingsprotocol