syndion

Dienstverlening en ondersteuning aan mensen met een beperking

Privacybeleid Syndion

Inhoud

Inleiding

Privacy is een grondrecht, vastgelegd in de Universele Verklaring van de Rechten van de Mens en het Europees Verdrag voor de Rechten van de Mens. Het is de bescherming van de persoonlijke levenssfeer. De bescherming van de persoonlijke levenssfeer uit zich in territoriale privacy (bijv. de vrijheid in en om je huis of werkplek), lichamelijke integriteit (recht om niet zomaar onderworpen te worden aan bijvoorbeeld genetische testen), privacy in communicatie (bijv. briefgeheim) en informationele privacy (ziet toe op de verwerking van persoonsgegevens). Als we in dit beleid spreken over Privacy, doelen we op informationele privacy.

De AVG en de UAVG (Uitvoeringswet AVG) vormen de belangrijkste wettelijke kaders voor privacy en de omgang met persoonsgegevens. De AVG bevat regels voor het rechtmatig gebruik van persoonsgegevens en formuleert de beginselen waaraan een gegevensverwerking minimaal moet voldoen om rechtmatig te zijn. Ook legt de AVG een verantwoordingsplicht op aan organisaties die persoonsgegevens verwerken, dit houdt in dat organisaties aantoonbaar moeten voldoen aan de wettelijke vereisten voor rechtmatig gebruik van persoonsgegevens.

Dit privacybeleid geeft richting aan privacy en laat zien dat Syndion privacy waarborgt, beschermt en handhaaft.

Dit beleid is vastgesteld op 2 april 2026 door het MT van Syndion. Het beleid wordt jaarlijks geëvalueerd en indien nodig aangepast. Bij bijzondere omstandigheden, zoals ingrijpende organisatorische wijzigingen, wetswijzigingen of bevindingen uit een DPIA (Data Protection Impact Assessment), kan het MT besluiten tot een tussentijdse herziening.

Managementteam
Syndion

1. Scope, visie en ambitie van Syndion voor privacy

Het Privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens binnen Syndion zoals processen, onderliggende systemen en het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord.

Onze missie luidt:

Syndion ondersteunt cliënten om met eigen zeggenschap een zinvol leven te leiden, midden in de maatschappij.

Dit sluit aan bij onze visie:

Cliënt, verwant en begeleider vormen de belangrijkste eenheid voor Syndion. De totale organisatie is erop gericht deze eenheid optimaal te ondersteunen. We zijn binnen en buiten de organisatie blijvend in dialoog. Samen zijn we in beweging om continue te verbeteren en te ontwikkelen.

Onze missie en visie vormen de basis van al onze dienstverlening. Wij bieden begeleiding en ondersteuning aan mensen in elke levensfase — van kind tot oudere — die leven met een beperking of ontwikkelingsstoornis.

Onze zorg richt zich op mensen met:

- Een verstandelijke beperking
- Een lichamelijke beperking
- Een meervoudige beperking
- Niet-aangeboren hersenletsel (NAH)
- Autisme of een aan autisme verwante contactstoornis

De missie en visie hebben wij vertaald naar een ambitie en visie voor privacy: Syndion wil betrouwbare en stabiele dienstverlening leveren aan mensen die leven met een beperking of ontwikkelingsstoornis en een betrouwbare werkgever voor onze medewerkers.

Privacy stellen wij daarom in dienst van onze primaire dienstverlening en wordt zodanig opgezet dat het ons primaire proces en de hierbij behorende dienstverlening ondersteunt.

Wij zorgen voor een aantoonbare beheersing van privacy en een stabiele bedrijfsvoering in de vorm van technische en organisatorische maatregelen. Dit alles ondersteund door relevante wet- en regelgeving.

Syndion wil een stabiele en efficiënte werkomgeving bieden waarbinnen onze medewerkers hun werk kunnen doen en kunnen bijdragen aan de continue verbetering van hun werkprocessen (PDCA).

2. Privacybeleid

2.1 Doel

Als organisatie die midden in de maatschappij staat, is het van belang dat ook in de bedrijfsvoering zorgvuldig met privacy en persoonsgegevens wordt omgegaan. Dat brengt de verplichting met zich mee om de verwerking van persoonsgegevens gedegen in te richten waarbij de relevante wettelijke en normgevende kaders als vertrekpunt voor borging, beheer en toetsing worden gebruikt. Dit uitgangspunt geldt als algemeen kader voor het organisatiebreed regelen van privacy binnen Syndion en de maatregelen die hiervoor getroffen worden.

Deze maatregelen hebben tot doel een blijvend niveau van privacy te realiseren waarbij het gewenste niveau van privacy ook op langere termijn gehandhaafd blijft.

2.2 Verantwoordelijkheden

Binnen de organisatie zijn specifieke functies verantwoordelijk gemaakt voor onderdelen van het privacybeleid. Dit draagt bij aan risicobeheersing, naleving van de AVG en het versterken van vertrouwen bij cliënten en partners.

2.2.1 Raad van Bestuur en het MT

De bestuurder en de MT-leden hebben een belangrijke rol bij het borgen van privacy in de organisatie. Hierbij worden de volgende principes gehanteerd:

1. Het MT stimuleert een cultuur voor rechtmatige verwerking van persoonsgegevens en informatieveilig werken;
2. Managementleden borgen en beheren privacy binnen de scope van hun verantwoordelijkheden;
3. Privacy is van iedereen;
4. Privacy behoeft ook aandacht in (keten)samenwerking;
5. Privacy kost geld;
6. Onzekerheid dient ingecalculeerd te worden;
7. Verbetering komt voort uit lering en ervaring;
8. Bestuurlijke verantwoording vindt plaats door formele verslaglegging.

2.2.2 Managers

Het zorgvuldig verwerken van persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid, dat betekent dat de managers de verantwoordelijkheid dragen voor een zorgvuldig gebruik van persoonsgegevens van cliënten, ouders en medewerkers op hun afdeling en locatie. Dit omvat ook het beslissen van (beveiligings)maatregelen en de uitvoering ervan.

Daarnaast dient de manager ervoor te zorgen dat zijn of haar medewerkers op de hoogte zijn van het privacybeleid, en periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

2.2.3 ICT Manager

De ICT-manager is verantwoordelijk voor het technisch waarborgen van privacy binnen de organisatie door het implementeren van beveiligingsmaatregelen zoals versleuteling, toegangscontrole en firewalls. Hij/zij ondersteunt het privacybeleid door te zorgen dat de IT-infrastructuur voldoet aan de AVG, identificeert en beheert privacyrisico's, voert controles uit op naleving, en werkt nauw samen met de privacy officer, FG en het MT. Daarnaast is de ICT-manager betrokken bij datamanagementprocessen en speelt een sleutelrol in de technische afhandeling van datalekken.

2.3 Uitgangspunten

Syndion hanteert de volgende uitgangspunten voor het privacybeleid.

Rechtmatig, behoorlijk en transparant
Persoonsgegevens worden in overeenstemming met de geldende wet- en regelgeving en op rechtmatige en behoorlijke wijze verwerkt. Voor betrokkenen is inzichtelijk dat van hen

persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt. Informatie en communicatie in verband met de verwerking van persoonsgegevens zijn eenvoudig toegankelijk en begrijpelijk voor betrokkenen.

Doelbinding en grondslag
Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen en alleen op grond van een in de wet vastgelegde rechtmatige grondslag. De doelen waarvoor de gegevens worden verwerkt zijn expliciet en gerechtvaardigd en zijn vastgesteld voordat de persoonsgegevens worden verwerkt. De verwerking van persoonsgegevens voor andere doeleinden dan waarvoor de persoonsgegevens eerder zijn verzameld, vindt enkel plaats indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Proportionaliteit en subsidiariteit
Bij het verwerken van persoonsgegevens wordt voldaan aan de beginselen van proportionaliteit en subsidiariteit. De inbreuk op de persoonlijke levenssfeer van de betrokkenen waarvan persoonsgegevens worden verwerkt staat in redelijke verhouding met het doel waarvoor de gegevens worden verwerkt (*proportionaliteit*). Voor het bereiken van de doeleinden waarvoor de persoonsgegevens worden verwerkt, wordt de inbreuk op de persoonlijke levenssfeer van betrokkenen waarvan gegevens worden verwerkt zoveel mogelijk beperkt. Als het doel met geen of minder persoonsgegevens kan worden bereikt, dan wordt daar altijd voor gekozen (*subsidiariteit*).

Dataminimalisatie
Persoonsgegevens die worden verwerkt zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Alleen die persoonsgegevens worden verwerkt die noodzakelijk zijn voor het realiseren van het vooraf bepaalde doel. Er wordt gestreefd naar minimale gegevensverwerking.

Juistheid van de gegevens
Persoonsgegevens die worden verwerkt zijn juist en worden actueel gehouden. Alle redelijke maatregelen worden genomen om de persoonsgegevens die onjuist zijn, zo snel mogelijk te wissen of te rectificeren.

Opslagbeperking
Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk is voor het realiseren van de doeleinden waarvoor de gegevens zijn verwerkt. Voor de bewaartermijnen wordt aangesloten bij de geldende wettelijke bewaartermijnen.

Integriteit en vertrouwelijkheid
Er wordt zorgvuldig omgegaan met persoonsgegevens en de gegevens worden als vertrouwelijk behandeld. Er worden passende technische- en organisatorische maatregelen genomen zodat een passende beveiliging van de persoonsgegevens is gewaarborgd en waardoor de gegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Delen met derden
Bij samenwerking met externe partijen zoals (keten)partners waarbij sprake is van het verwerken van persoonsgegevens, worden in overeenstemming met de geldende wet- en regelgeving doelen specifiek uitgewerkt, zijn rollen en verantwoordelijkheden duidelijk beschreven en zijn er afspraken gemaakt over de eisen waaraan de gegevensuitwisseling moet voldoen. Dit leggen wij vast in een verwerkersovereenkomst.

Rechten van betrokkenen
Wij bieden betrokkenen de mogelijkheid om hun rechten te kunnen uitoefenen. Deze rechten worden beschreven in de privacyverklaring op onze website en hierin wordt tevens het proces beschreven van de wijze waarop betrokkenen een verzoek hiervoor kunnen indien.

Compliance aan wet- en regelgeving
Wij voldoen aan alle voor onze organisatie van toepassing zijnde wet- en regelgeving ter bescherming van privacy waaronder de AVG en de UAVG.

2.3 Specifieke maatregelen

Onze organisatie treft de volgende specifieke maatregelen op het gebied van privacy:

Verwerkingsregister
Wij houden een verwerkingsregister bij waarin alle verwerkingen staan vermeld met betrekking tot persoonsgegevens van zowel het primaire proces als de ondersteunende processen.

DPIA
Bij de verwerking van persoonsgegevens die mogelijk een risico voor de betrokkenen met zich meebrengen, voeren wij een Data Protection Impact Assesment (DPIA) uit.

Aan de hand van de risico's die hieruit naar voren komen worden technische en organisatorische maatregelen getroffen om de risico's in te perken. DPIA's worden jaarlijks opnieuw beoordeeld en waar nodig, geactualiseerd.

Verwerkersovereenkomsten
Met onze opdrachtgevers en leveranciers waarbij persoonsgegevens worden verwerkt, sluiten wij verwerkersovereenkomsten af.

Datalekken
Datalekken handelen wij aantoonbaar af middels een vastgestelde workflow en registreren wij in een register. Al naar gelang de impact van het datalek wordt een melding gedaan bij de Autoriteit Persoonsgegevens en de betrokkenen.

Wij evalueren onze datalekken en nemen maatregelen ter voorkoming en verbetering.

Verzoekproces en rechten van betrokkenen
Verzoeken van betrokkenen handelen wij adequaat en binnen de hiervoor geldende termijn af. Wij hebben hiervoor een proces ingericht zodat betrokken een beroep kunnen doen op hun rechten tot inzage, rectificatie, wissen, beperking, dataportabiliteit en bezwaar.

De rechten waarop betrokkenen zich kunnen beroepen, worden beschreven in de privacyverklaring op de website. Hierin wordt tevens beschreven hoe zij het verzoek kunnen indienen.

Privacy bewustzijn
Onze medewerkers zijn zich bewust van de persoonsgegevens die zij verwerken en handelen daar ook naar. Medewerkers hebben een geheimhoudingsplicht en volgen onze gedragscode voor privacy. Wij stimuleren continu privacybewustzijn binnen onze organisatie door medewerkers op verschillende manieren te betrekken bij het veilig omgaan met persoonsgegevens. Daarnaast bevorderen we een cultuur waarin mogelijke risico's en incidenten rondom privacy bespreekbaar zijn.

Functionaris Gegevensbescherming (FG)
Onze organisatie heeft een FG aangesteld. De FG ziet erop toe dat persoonsgegevens op de juiste manier verwerkt en beschermd worden volgens de eisen van de AVG. De FG zal daarbij ook samenwerken met de toezichthoudende autoriteit indien gevraagd en desgevraagd de rechten van betrokkenen inwilligen.

De contactgegevens van de FG zijn gepubliceerd in de privacyverklaring op onze website en tevens gedeeld met onze medewerkers.

Privacy by Design & Privacy by Default
Onze organisatie past de principes van Privacy by Design en Privacy by Default toe voor alle verwerkingen met persoonsgegevens.

Privacy by Default is toegepast op alle systemen, waarbij gebruik wordt gemaakt van specifieke rechten voor een medewerker op basis van de functie. Alle standaardinstellingen zijn zo gekozen dat de privacy maximaal wordt geborgd. Daarnaast zullen wij actief toestemming vragen aan de betrokkenen wanneer 'toestemming' de wettelijke verwerkingsgrondslag is.

Verder hanteren wij het uitgangspunt dat alleen medewerkers die vanuit hun functie toegang tot persoonsgegevens nodig hebben, die toegang krijgen. Wij volgen hierbij het need-to-know principe.

Het Privacy by Design principe wordt door ons toegepast tijdens het (laten) ontwerpen en ontwikkelen van de voor verwerking van persoonsgegevens gebruikte mechanismen, waarbij zo veel mogelijk rekening wordt gehouden met de privacy van betrokkenen. Verder beperken we de verwerking van persoonsgegevens tot die welke noodzakelijk zijn om onze doelen te realiseren en waarvoor een wettelijke grondslag bestaat.

3. Haalbaarheid van het privacybeleid

Om de naleving van de privacywetgeving structureel te borgen, hanteren wij een systematische aanpak voor het monitoren, evalueren en verbeteren van ons privacybeleid. Deze aanpak wordt hieronder nader uiteengezet.

Om de uitvoerbaarheid van ons privacybeleid te waarborgen, organiseren wij periodiek overleg met de directie, de Functionaris Gegevensbescherming (FG) en relevante leden van het managementteam. Tijdens deze bijeenkomsten wordt de voortgang besproken en worden eventuele knelpunten gesignaleerd.

Volgens een vastgestelde jaarplanning evalueren wij onze Data Protection Impact Assessments (DPIA's) en de getroffen technische en organisatorische maatregelen. Doel hiervan is te toetsen of deze nog steeds adequaat zijn voor de betreffende verwerkingen van persoonsgegevens.

Privacyrisico's die als onacceptabel worden beoordeeld, worden vertaald naar concrete verbetermaatregelen, in lijn met het geldende privacybeleid.

Verwerkersovereenkomsten worden regelmatig beoordeeld op actualiteit en relevantie. Daarbij worden tevens de prestaties van de verwerkers geëvalueerd. Deze beoordeling vindt plaats op basis van een risicogestuurde aanpak, waarbij met name de kritieke leveranciers periodiek onder de loep worden genomen.

Jaarlijks vindt een privacy-audit plaats om vast te stellen of de werkwijze van medewerkers in overeenstemming is met het privacybeleid en de Algemene Verordening Gegevensbescherming (AVG).

Aan het einde van het jaar stelt de FG een rapportage op waarin de uitgevoerde privacyactiviteiten en eventuele issues worden beschreven. Tevens wordt het volwassenheidsniveau van de organisatie op het gebied van privacy beoordeeld.

4. Controle en naleving

Dit privacybeleid wordt minimaal ieder jaar getoetst en daar waar nodig bijgesteld. Hierbij wordt rekening gehouden met:

- De status van privacy als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Syndion een jaarlijkse planning en control cyclus voor privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het privacybeleid worden getoetst.

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van Syndion door de Functionaris Gegevensbescherming. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Syndion wordt actief aandacht besteed aan privacy bij de aanstelling, tijdens functioneringsgesprekken, met een gedragscode en met periodieke bewustwordingscampagnes.

Voor de bevordering van de naleving van de AVG vervult de FG een belangrijke rol. De FG wordt aangesteld door de directie en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving ernstig tekortschieten, dan kan Syndion de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO Gehandicaptenzorg (cao GHZ) en de wettelijke mogelijkheden.

Vastgesteld op: 2 april 2026 door het MT van Syndion