Privacy beleid

Opgesteld: Oktober 2016

Herzien: september 2024

Evaluatie: september 2025

Opgesteld door: Lilian Nijland

Inhoudsopgave

Persoonsgegevens die wij verwerken

De Algemene Verordening Gegevensbescherming is door de Nederlandse wetgever opgesteld ter bescherming van privacy en persoonsgegevens. De wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de plichten zijn van een organisatie (Trevin) die de gegevens gebruikt. In de termen van de wet is Trevin de verantwoordelijke en zijn de cliënten en medewerkers (iedereen die in opdracht is of namens Trevin een taak uitvoert) de betrokkenen. De wet spreekt van het "verwerken van persoonsgegevens". Dit begrip omvat alles wat men met persoonsgegevens kan doen: vanaf het verzamelen tot en met het vernietigen ervan. Naast deze algemene privacywet gelden specifieke regels voor de privacy in de gezondheidszorg. Deze regels staan bijvoorbeeld vermeld in de Wet geneeskundige behandelingsovereenkomst (WGBO) en Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz). Trevin verwerkt persoonsgegevens over jou omdat je gebruik maakt van onze diensten en/of omdat je deze gegevens zelf aan ons verstrekt. Hieronder een overzicht van de persoonsgegevens die wij verwerken:

- Voor- en achternaam
- Geslacht
- Geboortedatum
- Geboorteplaats
- Adresgegevens
- Telefoonnummer
- E-mailadres
- BSN nummer
- Gegevens ouders (indien jonger dan 18 jaar)/wettelijk vertegenwoordiger
- Gegevens 2e contactpersoon
- Medische gegevens cliënten
- Verklaring gebruik gegevens/foto’s
- Gegevens over indicaties

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken

Trevin verwerkt de volgende bijzondere en/of gevoelige persoonsgegevens van jou, indien deze van belang/relevant zijn voor begeleiding:

- godsdienst of levensovertuiging
- gezondheid
- strafrechtelijk verleden
- (DSM-)diagnoses

Waarom we gegevens nodig hebben

Trevin verwerkt jouw persoonsgegevens, voor de volgende doelen:

- Het afhandelen van jouw betaling
- Verzenden van onze nieuwsbrief
- Je te kunnen bellen indien dit nodig is om onze dienstverlening uit te kunnen voeren
- Je te informeren over wijzigingen van onze diensten en producten
- Trevin verwerkt ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals bijvoorbeeld gegevens die wij nodig hebben voor onze belastingaangifte.
- Passende zorg kunnen bieden

Hoe lang we gegevens bewaren

Trevin zal je persoonsgegevens niet langer bewaren dan strikt nodig is om de doelen te realiseren waarvoor je gegevens worden verzameld. Onze bewaartermijn(en) zijn:

- gegevens die zijn gegenereerd door Trevin en die direct verband houden met de zorg en ondersteuning aan de cliënt (gezondheidsgegevens). Deze worden 20 jaar bewaard;
- gegevens die Trevin niet zelf heeft gegenereerd, maar van de cliënt zelf heeft gekregen zoals financiële gegevens, bankafschriften. Deze worden zoveel mogelijk geretourneerd na het einde van de behandeling;
- gegevens die Trevin zelf heeft gegenereerd die nog wel verband houden met de zorg en ondersteuning, maar geen gezondheidsgegevens zijn (de financiële administratie); hiervoor geldt de bewaartermijn op grond van andere regels, bijvoorbeeld die voor de boekhoudplicht/financiële verslaglegging. Voor dergelijke fiscale gegevens geldt over het algemeen een termijn van 7 jaar.

- overige gegevens. Niet langer bewaren dan strikt noodzakelijk.

Delen met anderen

Trevin deelt jouw persoonsgegevens met verschillende derden als dit noodzakelijk is voor het uitvoeren van de overeenkomst en om te voldoen aan een eventuele wettelijke verplichting. Dit doen wij alleen met jouw nadrukkelijke toestemming. Als de veiligheid van een kind of jongere in het geding is, zijn wij op basis van de meldcode 'huiselijk geweld en kindermishandeling' verplicht een melding te maken. De meldcode 'huiselijk geweld en kindermishandeling' kan ter inzage worden opgevraagd bij Trevin.

Gegevens inzien, aanpassen of verwijderen

Je hebt het recht om je persoonsgegevens in te zien, te corrigeren of te verwijderen. (m.u.v. gegevens die wij nodig zijn voor onze dienstverlening of daaraan gerelateerde zaken). Je kunt een verzoek tot inzage, correctie of verwijdering sturen naar info@trevin.nl. Om er zeker van te zijn dat het verzoek tot inzage door jou is gedaan, vragen wij jou een kopie van je identiteitsbewijs bij het verzoek mee te sturen. Hierbij vragen we jou om in deze kopie je pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart te maken. Dit ter bescherming van je privacy. Trevin zal zo snel mogelijk, maar binnen vier weken, op jouw verzoek reageren. Het management van Trevin heeft inzicht in de gegevens van de medewerkers. Voor de gegevens van de cliënt geldt dat de personen die met de cliënten werken, inzicht in de gegevens hebben.

Beveiliging

Trevin neemt de bescherming van jouw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Wij maken gebruik van diverse systemen waar twee-stapsverificatie is toegepast en de beveiliging is gewaarborgd. Daarnaast maken wij voor beveiligd mailen gebruik van Zivver, daar waar gevoelige gegevens uitgewisseld worden. Doormiddel van bovenstaande systemen worden ook datalekken tegengegaan. Mede hierdoor kunnen er juiste koppelingen gelegd worden en hoeven documenten zo min mogelijk per mail verstrekt worden. Tevens maakt Trevin gebruik een tweetal NAS schijven voor het opslaan van documenten op een beveiligde wijze (incl. back-up). Als jij het idee hebt dat jouw gegevens toch niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op via info@trevin.nl of telefonische 0570-244047.

Datalek protocol

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (’AP’), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.

1: Wat is een datalek?

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP-persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoonsgegevens per ongeluk gepubliceerd
- hacking, mailware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

2: Contactpersoon aanwijzen

De organisatie moet een eigen contactpersoon aanwijzen aan wie eventuele datalekken gemeld moeten worden. Dit kan bijvoorbeeld een bestuurslid of de Functionaris Gegevensbescherming zijn. (hierna: 'Contactpersoon"). Binnen Trevin is Lilian Nijland, mede-eigenaar, de contactpersoon.

3: Informeren medewerkers

Medewerkers binnen Trevin dienen zich ervan bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de aangewezen Contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan.

4: Uitvoeren van het stappenplan Datalekken

De binnen Trevin aangewezen Contactpersoon draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Indien er een datalek optreedt dienen de stappen in het stappenplan Datalekken doorlopen te worden.

STAPPENPLAN DATALEKKEN

PROCESSTAPPEN	ACTIVITEIT	VERANTWOORDELIJKE PERSOON
1. ER WORDT EEN (MOGELIJK) DATALEK ONTDEKT	- Maak direct intern melding van (mogelijke) datalek - Informeer de verantwoordelijke Contactpersoon	Medewerker die het ontdekt
2. BEOORDEEL HET DATALEK	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Aangewezen contactpersoon

	- Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	
3. BESTRIJDT HET DATALEK	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Aangewezen contactpersoon
4.VASTSTELLEN IMPACT DATALEK	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op de betrokken personen - Stel vast wat de nadelige gevolgen kunnen zijn	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Aangewezen contactpersoon

5. VASTSTELLEN MELD EN HERSTELAANPAK	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Aangewezen contactpersoon
6. MELDEN AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP - Van tevoren kan het Meldformulier Datalekken gebruikt worden	Aangewezen contactpersoon Bestuur
7. MELDEN BETROKKENEN**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Aangewezen contactpersoon Bestuur
8. UITVOEREN HERSTELWERKZAAMHEDEN	- Herstel het datalek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	Aangewezen contactpersoon

9. OPTIMALISEER HET BEVEILIGINGS- EN HET DATALEK PROCES	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Aangewezen contactpersoon Bestuur

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

** Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden.

Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken terstond (binnen 24 uur) meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de

organisatie om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.