Privacybeleid Factor Twee

Persoonsgegevens bij Factor Twee

Uw privacy is voor Factor Twee van groot belang. Wij houden ons dan ook aan de Algemene Verordening Gegevensbescherming, waarin is geregeld hoe met uw persoonsgegevens moet worden omgegaan. Hierin staat ook dat wij aan moeten kunnen tonen dat wij ons aan de wet houden. Wij hebben de privacy van onze cliënten, medewerkers en anderen hoog in het vaandel staan. In dit beleid hebben wij beknopt de verplichtingen van Factor Twee en de rechten van onze cliënten (of hun vertegenwoordigers) beschreven.

Betekenis privacybeleid

Wij hebben de verantwoordelijkheid u te vertellen wat er met uw persoonsgegevens gebeurt. Welke persoonsgegevens wij vragen, waar we die voor gebruiken, wie ze gebruikt en aan wie we gegevens mogelijk verstrekken. Het uitgangspunt daarbij is dat we alleen persoonsgegevens gebruiken indien dat noodzakelijk is en natuurlijk op een veilige manier.

Welke (standaard) gegevens hebben we van u nodig en waarvoor?

1. Algemene persoonsgegevens (naam, geboortedatum, burgerlijke staat, etc.), contactgegevens (ook van wettelijk vertegenwoordiger), verzekeringsgegevens, verleende zorgproducten, sociaal profiel / netwerk, medische en gedragsgegevens, voor zover relevant voor het kunnen bepalen van de benodigde zorg- en dienstverlening.

   Deze gegevens gebruiken we voor onze bedrijfsvoering, correspondentie en persoonlijke communicatie; in het bijzonder voor de instandhouding van de dienstverlening en externe verantwoording over de verleende zorg (declareren naar zorgkantoor, zorgverzekeraar, gemeente), maar ook voor het betrekken van het sociale netwerk en mantelzorger.
2. Burgerservicenummer (BSN).

   Dit nummer hebben we nodig om gegevens met betrekking tot de cliënt uit te wisselen met zorgkantoor, zorgverzekeraar, overheid en andere zorgaanbieders; gebruik van dit nummer is voor Factor Twee dan verplicht.
3. Medische, gedragsgerelateerde, sociaal-maatschappelijke en verpleegkundige/ begeleidings-gegevens.

   Deze gegevens gebruiken we voor het vaststellen, toetsen, volgen en uitvoeren van de individuele zorg- en dienstverlening.
4. Toegediende medicatie.

   Met af te tekenen medicatielijsten maken wij inzichtelijk welke medicatie cliënten hadden moeten ontvangen en of ze deze ook daadwerkelijk hebben ontvangen.
5. Omschrijving en aard van incidenten met betrekking tot cliënten, getroffen maatregelen en schade/letsel.

   Deze gegevens hebben we nodig voor handhaving en optimalisering van de kwaliteit van zorgverlening aan cliënten.
6. Omschrijving en toedracht van (seksueel) misbruik met betrekking tot een cliënt, en de ondernomen actie n.a.v. het misbruik.

   Deze gegevens hebben we nodig om het beleid te bepalen ten aanzien van het (seksueel) misbruik (afhandeling, nazorg en preventie).

Overige persoonsgegevens

Gegevens dienen altijd met een omschreven doel te worden vastgelegd. Overige bijzondere, extra gevoelige persoonsgegevens (bijvoorbeeld godsdienst, geaardheid, politieke voorkeur en ras) mogen wij niet vastleggen. In een aantal situaties kan toestemming hiervoor een uitzondering vormen. Pasfoto's kunnen bijvoorbeeld ook iets over iemands ras of religie zeggen. Wanneer we foto's willen vastleggen voor onze eigen registratie of om ergens te publiceren, kan toestemming als basis worden gebruikt om dit toch mogelijk te maken. Toestemming hiervoor kan overigens altijd door u weer worden ingetrokken. Ook euthanasieverklaringen en reanimatieverklaringen worden alleen op verzoek van de cliënt vastgelegd.

Wanneer Factor Twee een gerechtvaardigd belang heeft om gegevens te verzamelen en vast te leggen, mag dit zonder toestemming worden gedaan. Denk dan bijvoorbeeld aan agressief gedrag dat voor onze medewerkers van belang is om te weten.

Hoe verkrijgt Factor Twee de persoonsgegevens?

De meeste gegevens van een cliënt ontvangen we rechtstreeks wanneer de zorgovereenkomst wordt afgesloten en de zorg wordt gestart. Daarnaast kunnen gegevens worden ontvangen van andere zorgaanbieders.

Het dossier/zorgplan vult zich gedurende de periode dat de cliënt bij Factor Twee in zorg is.

Inzage van de gegevens

Inzage in uw persoonsgegevens heeft u als cliënt zelf alsmede uw (wettelijk) vertegenwoordiger.

Intern gebruik van de gegevens

Om uw privacy zoveel mogelijk te beschermen beperken we het intern gebruik van persoonsgegevens zoveel als mogelijk. Alleen medewerkers die op basis van hun functie uw gegevens moeten gebruiken, mogen dat. Dat regelen we door die medewerkers specifieke bevoegdheid te verlenen (autorisatie) voor toegang tot geautomatiseerde systemen.

Beveiliging van de gegevens

Factor Twee neemt passende technische en organisatorische maatregelen om uw persoonsgegevens veilig te bewaren en tevens ongewenste handelingen met persoonsgegevens tegen te gaan. Deze maatregelen zijn in overeenstemming met de voor de zorgsector geldende beveiligingsnormen. Mailverkeer met persoonsgegevens vindt via beveiligde mails plaats, toegang tot digitale bestanden vindt plaats met een dubbele authenticatie en uiteraard hebben de eventueel ingezette andere partijen getekend voor geheimhouding.

Extern gebruik van gegevens

Verplichte doorgifte

Als zorginstelling heeft Factor Twee de verplichting om gegevens over benodigde en geleverde zorg te delen met zorgkantoor, zorgverzekeraar en gemeenten (declaraties). Deze uitwisseling vindt plaats via beveiligde verbindingen.

In bijzondere situaties kunnen wij ook aan andere instanties verplicht worden om gegevens over u te verstrekken; denk aan de kantonrechter in verband met de verantwoording over beheerde gelden of in geval van een justitieel onderzoek.

Inzage door leveranciers van software/computerprogramma's
Voor haar bedrijfsvoering maakt Factor Twee gebruik van computerprogramma's. De leveranciers van de programma's ondersteunen en onderhouden die en daardoor zijn de persoonsgegevens in die programma's ook toegankelijk voor medewerkers van die leveranciers. Daarvoor sluiten we met hen een verwerkersovereenkomst waarmee we de leverancier verplichten op een even zorgvuldige manier met persoonsgegevens om te gaan als Factor Twee zelf.

Overige doorgifte
Wij delen gegevens alleen met derden wanneer dat noodzakelijk is voor het uitvoeren van de zorgovereenkomst en om te voldoen aan een eventuele wettelijke verplichting. Wanneer wij aan anderen gegevens verstrekken doen wij dit alleen nadat we van u toestemming hebben verkregen.

Hoe lang bewaren we je persoonsgegevens?
In het kader van de Wet Geneeskundige Behandelovereenkomst (WGBO) dient Factor Twee voor het cliëntendossier een bewaartermijn van minimaal 20 jaar te hanteren na beëindiging van de zorgovereenkomst, tenzij een kortere termijn geldt zoals 15 jaar in geval van Wmo-zorg. Voor medicatielijsten wordt een bewaartermijn van twee jaar gehanteerd. Voor overige gegevens geldt dat we de gegevens niet langer bewaren dan nodig is. Wij zullen de gegevens dan zo spoedig mogelijk verwijderen.

Rechten met betrekking tot de eigen persoonsgegevens
Als zorginstelling moeten we persoonsgegevens van cliënten gebruiken. Maar die persoonsgegevens hebben wel op de cliënt zelf betrekking. Daarom heeft de cliënt het recht om de persoonsgegevens:

- in te zien,
- te corrigeren als ze niet juist zijn,
- over te laten dragen naar andere personen of organisaties.

Daarnaast is er het recht te verzoeken gegevens te (laten) verwijderen of bezwaar te maken tegen verwerking van gegevens.

Datalekken
Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, spreken we van een datalek. Indien dit aan de orde is, nemen we terstond maatregelen om het lek te stoppen. We registreren ieder datalek en nemen maatregelen om te voorkomen dat het nog eens gebeurt.
Indien er sprake is van een risico op een inbreuk van rechten en vrijheden van betrokkene(n) melden wij het datalek uiterlijk 72 uur nadat wij er kennis van hebben genomen, aan de Autoriteit Persoonsgegevens en brengen wij betrokkene(n) persoonlijk op de hoogte over de aard van het datalek, de mogelijke gevolgen en de maatregelen die we getroffen hebben en/of zullen gaan treffen.

Bij een datalek geldt het volgende protocol:

1. Zorg voor overzicht op de situatie.
2. Neem onmiddellijk maatregelen om het datalek te stoppen en de schade van het datalek te beperken. Schat daarbij ook de risico's in.
3. Bepaal of het datalek wel of niet moet worden gemeld aan de Autoriteit Persoonsgegevens. Zo ja, dan doen we dit zo snel mogelijk.
4. Bepaal of de slachtoffers wel of niet geïnformeerd moeten worden. Zo ja, dan doen we dit zo snel mogelijk.

5. Registreer het datalek in het interne datalekregister.

Een uitwerking van dit protocol is opgenomen in het Datalek-protocol van Factor Twee.

Wijzigingen in dit privacybeleid

Het kan voorkomen dat de situatie zich voordoet dat het privacybeleid moet worden gewijzigd. Let dus altijd op de datum van dit beleid en kijk daarom regelmatig of er nieuwe versies zijn. Factor Twee zal tevens wijzigingen apart aankondigen.

Vragen of kritiek

Als u vragen hebt over uw rechten, niet tevreden bent over hoe wij hieraan uitvoering geven, of specifieke vragen heeft over de verwerking van persoonsgegevens door ons, kunt u altijd contact met ons opnemen. Zie de contactgegevens hieronder.

Contactpersoon bij Factor Twee:

Naam:	Lotte Sleebos
Telefoonnummer:	0742015922
E-mailadres:	lotte@factortwee.nl

Let op dat u altijd duidelijk aangeeft wie u bent, zodat we zeker weten dat we geen gegevens van de verkeerde persoon aanpassen of verwijderen. Wij kunnen u ook vragen om u te legitimeren en een formulier in te vullen.

Klacht indienen

Als u vindt dat Factor Twee niet op de juiste manier omgaat met uw persoonsgegevens, dan heeft u het recht om een klacht bij ons in te dienen. Hoe dat in zijn werk gaat staat in onze klachtenregeling, deze kunt u op onze website vinden. U kunt ook altijd een klacht indienen bij de toezichthouder, dit is de Autoriteit Persoonsgegevens.

Privacybeleid Factor Twee, maart 2024

Datalek-protocol Factor Twee[1]

Bij een datalek geldt het volgende protocol:

1. Zorg voor overzicht op de situatie.
2. Neem onmiddellijk maatregelen om het datalek te stoppen en de schade van het datalek te beperken. Schat daarbij ook de risico's in.
3. Bepaal of het datalek wel of niet moet worden gemeld aan de Autoriteit Persoonsgegevens. Zo ja, dan doen we dit zo snel mogelijk.
4. Bepaal of de slachtoffers wel of niet geïnformeerd moeten worden. Zo ja, dan doen we dit zo snel mogelijk.
5. Registreer het datalek in het interne datalekregister.

Een uitwerking van dit protocol is hieronder opgenomen:

Stap 1: Overzicht krijgen bij datalek

De eerste stap bij een datalek is zorgen voor overzicht op de situatie, zodat de juiste vervolgstappen genomen kunnen worden. Daarvoor moet allereerst duidelijk zijn om wat voor soort datalek het gaat.

Zodra bekend is om wat voor soort datalek het gaat, dan helpen de volgende vragen om verder overzicht te krijgen op de situatie:

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En is het datalek nog steeds gaande?
- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn gelekt? Bijvoorbeeld naam, adres, e-mailadres en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het?
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Is er zicht op wie die onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?
- Welke maatregelen zijn vooraf getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Stap 2: Beperken schadelijke gevolgen datalek

Hoe de gevolgen van een datalek beperkt kunnen worden, hangt volledig af van de situatie. Ten eerste moet het datalek onmiddellijk gestopt worden als het nog bestaat. Daarnaast moeten er maatregelen worden genomen om de negatieve gevolgen te beperken.

[1] Bij het opstellen van dit protocol is gebruik gemaakt van de informatie van de Autoriteit Persoonsgegevens over wat te doen bij datalekken.

Voorbeelden van maatregelen om schade bij een datalek te beperken zijn:

- Een laptop, tablet of smartphone op afstand wissen of versleutelen.
- Een gepubliceerd bestand offline halen.
- Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd. Hoewel op basis van zo'n bevestiging niet 100% zeker is dat de gegevens gewist zijn, kan het wel worden meegenomen in derisico-inschatting.
- De toegang tot een account of clouddienst op afstand blokkeren.
- Wanneer de verplichting bestaat om de slachtoffers te informeren, dan aangeven wat zij zelf kunnen doen om de schade te beperken.

Diepgaand onderzoek bij complexe datalekken

Soms is er sprake van een complex datalek. Dan is het vaak nodig om een diepgaand digitaal forensisch onderzoek uit te voeren om de ernst en omvang van het lek vast te stellen. En vervolgens te bepalen welke maatregelen genomen moeten worden om de gevolgen van het datalek te beperken en om nieuwe, soortgelijke datalekken te voorkomen.

Als er sprake is van een complex datalek, bijvoorbeeld een datalek door ransomware, en binnen de organisatie is niet bekend wat te doen, dan wordt een expert ingeschakeld. Bijvoorbeeld een digitaal forensisch expert.

Stap 3: Melden datalek en informeren slachtoffers

Er kan een verplichting zijn zijn om het datalek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Ook kunt er een verplichting zijn om de slachtoffers te informeren over het datalek. Er moet worden beoordeeld of dit het geval is, zie daarvoor de handleiding van de Autoriteit Persoonsgegevens op: https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-wel-of-niet-melden

Stap 4: Registreren datalek in datalekregister

Volgens de AVG is het opstellen en bijhouden van een datalekregister verplicht. Hierin wordt bijgehouden welke datalekken er in de organisatie zijn geweest. In het register moeten alle datalekken worden vastleggen die zich binnen de organisatie hebben afgespeeld. Ook de datalekken die niet aan de Autoriteit Persoonsgegevens zijn gemeld.

Het doel van het datalekregister is dat de organisatie:

- leert van eerdere datalekken en bewust is van datalekken die in het verleden hebben plaatsgevonden;
- effectieve maatregelen neemt om de kans op nieuwe, soortgelijke datalekken te verminderen;
- met het datalekregister aan de Autoriteit Persoonsgegevens kan laten zien dat de organisatie zich houdt aan de meldplicht datalekken.

Vorm en inhoud datalekregister

Er is geen eis aan de vorm van het register, zolang het maar de wettelijk verplichte informatie bevat. Over elk datalek wordt ten minste de volgende informatie vermeld: (i) de feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegeven het gaat; (2) de gevolgen van het datalek; (3) de corrigerende maatregelen die zijn genomen.

De datalekregistratie wordt meegenomen bij de organisatiebeoordeling die jaarlijks plaatsvindt, om zo als onderdeel van een 'plan-do-check-act'-cyclus te worden gebruikt om te leren van fouten.