Basisregels

Er gelden voor alle medewerkers een aantal basisregels betreffende privacygevoelige informatie. Deze basisregels dienen ten aller tijden opgevolgd worden.

Overzicht te verwerken persoonsgegevens

- Voor- en achternaam
- Geboortedatum
- BSN-nummer
- Adresgegevens
- Telefoonnummer
- E-mailadres
- Huisarts
- Locatiegegevens
- Gegevens die betrekking hebben tot het productaanbod.
- Bijzondere en/of gevoelige persoonsgegevens.

Gegevens van personen jonger dan 16 jaar

Ouders/verzorgers/professionals/jongeren verstrekken informatie over de hulpvraag die zij hebben waar Praktijk voor Heelheid mogelijk mee van dienst kan zijn. Ze delen alle relevante informatie die mogelijk van invloed kunnen zijn op het probleem en/of de oplossing uitsluitend via de beveiligde omgeving.

Bij personen onder de 16 jaar dient voorafgaand aan een onderzoek een toestemmingsformulier getekend te worden; door beide ouders ondertekend.

Persoonlijke gegevens

Als iemand ervan overtuigd is dat Praktijk voor Heelheid zonder diens toestemming persoonlijke gegevens heeft verzameld over een minderjarige, dient er contact opgenomen te worden via info@astridlammers.nl, dan wordt deze, indien onrechtmatig verkregen informatie verwijderd.

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838

Rapport

De cliënt heeft het recht het therapeutisch rapport te lezen, voordat het naar de opdrachtgever wordt verstuurd. In het rapport staat niet meer dan nodig is voor de beantwoording van de hulpvraag. De cliënt heeft het recht feiten die niet kloppen in het rapport te verbeteren. De cliënt heeft het recht te verbieden dat het rapport naar de opdrachtgever gaat. Dit geldt echter niet bij een onderzoek waarbij Praktijk voor Heelheid door de wet verplicht is te rapporteren.

Delen van persoonsgegevens met derden of gegevensoverdraagbaarheid

Een therapeut is verplicht tot geheimhouding. Alle gegevens over de cliënt worden vertrouwelijk behandeld. Praktijk voor Heelheid zal in het algemeen alleen gegevens uit het dossier doorgeven aan derden als de cliënt daarvoor van tevoren schriftelijk toestemming heeft gegeven. Voor het doorgeven van gegevens aan bijvoorbeeld de huisarts is toestemming van de cliënt nodig en zal pas plaatsvinden nadat alle onderzoeksresultaten met de cliënt besproken zijn. Gaat het echter om het doorgeven van gegevens binnen een team van behandelaars dan is daarvoor geen afzonderlijke toestemming van de cliënt nodig. Verder zal Praktijk voor Heelheid persoonsgegevens uitsluitend verstrekken indien dit nodig is voor de uitvoering van de overeenkomst of indien dit noodzakelijk is om te voldoen aan een wettelijke verplichting zoals onder andere het inschakelen van veilig thuis of de meldcode voor (vermoedens van) huiselijk geweld of kindermishandeling. Als naar beoordeling van de eigenaar van de gezondheid van betrokkenen in het geding is, zal met toestemming van de directie de huisarts geconsulteerd worden.

Bewaring persoonsgegevens

Praktijk voor Heelheid bewaart gegevens over een cliënt in een dossier. Hierin worden onderzoeksgegevens bewaard, en bij behandeltrajecten ook gegevens over het verloop van de behandeling. De cliënt heeft het recht het eigen dossier in te zien. Praktijk voor Heelheid bewaart persoonsgegevens en medische dossiers niet langer dan wettelijk is vereist en wettelijk is toegestaan, welke is vastgesteld op 20 jaar, nadat de cliënt 18 jaar is geworden. Indien gewenst, kan men contact opnemen om de persoonsgegevens eerder te verwijderen. Aan dit verzoek zal voldaan worden indien dit past binnen de kaders van de regelgeving waaraan de therapeut moet voldoen.

Klachten

Bij eventuele klachten over het verwerken van persoonsgegevens kunt u een klacht indienen bij de Autoriteit Persoonsgegevens.

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838

Misbruik en verlies

Praktijk voor Heelheid neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan d.m.v. o.a. code beveiliging op laptop, verbod op het gebruik van mobile gegevensdragers (zoals USB), verplichting van vingerafdruk telefoon en door papieren gegevens achter slot en grendel te bewaren. Mail wordt via een veilige SSL//TLS verbinding verstuurd via Zivver of Protonmail. Alle mogelijke betrokkenen van Praktijk voor Heelheid dragen bij tot en hebben inzage in de voor hun functie relevante informatie. Alle werknemers zijn gezamenlijk gebonden door het beroepsgeheim. Praktijk voor Heelheid zal enkel toegang verlenen tot de dossiers aan derden met uitdrukkelijke toestemming van de wettelijke vertegenwoordigers of om te voldoen aan een wettelijke verplichting.

Procedure Datalekken

Procesbeschrijving Datalek

Volgens de Algemene Verordening Gegevensbescherming (AVG) is er sprake van een datalek als zich een inbreuk voordoet op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Voorbeelden van een datalek zijn:

- Verlies van een mobiel apparaat waarop gevoelige persoonsgegevens staan.
- Het delen van persoonsgegevens waarvoor geen toestemming is verkregen van de betrokkene.
- Computer hacking.
- Besmetting met ransomware, etc.

Niet ieder datalek-incident hoeft gemeld te worden bij de toezichthouder of bij de betrokkene. Als bijvoorbeeld verloren of gestolen persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijke risico op schade aan de persoonlijke levenssfeer.

Alle incidenten, ook diegene die niet bij de Autoriteit Persoonsgegevens gemeld worden, moeten worden opgenomen in het register van de functionaris gegevensbescherming.

Een datalek dient uiterlijk binnen 72 uur na ontdekking van het datalek te worden gemeld volgens bijgevoegde flowcharge.

Binnen Praktijk voor Heelheid wordt er volgens onderstaande stapplan gewerkt:

1) het signaleren, analyseren en registreren van incidenten, waarbij er sprake is van een inbreuk op een beveiligingsmaatregel en persoonsgegevens betrokken zijn;
2) het inhoudelijk beoordelen en onderzoeken van het incident of er op grond van de AVG sprake is van een datalek dat gemeld moet worden bij de toezichthouder en betrokkenen;
3) het melden van het datalek aan de toezichthouder en betrokkenen namens het bestuur;
4) het documenteren van het datalek bij zowel interne als externe meldingen.

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838

Het signaleren, analyseren en registreren van incidenten

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van Praktijk voor Heelheid zijn, of met een informatiebeveiligingsincident, dient dit te melden bij de eigenaar van Praktijk voor Heelheid. Dit moet direct telefonisch/mondeling gebeuren.

De medewerker wordt verzocht de naam en contactgegevens van de melder te noteren met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de Autoriteit Persoonsgegevens.

Ook als de medewerker twijfelt of er sprake is van een incident of wat hij moet doen, kan hij de eigenaar van Praktijk voor Heelheid hiervoor benaderen. De eigenaar van Praktijk voor Heelheid analyseert of er bij het incident persoonsgegevens betrokken zijn. Indien de melding telefonisch is gedaan, vraagt de medewerker dit na bij de melder.

Vanwege het gegeven dat we als zorgorganisatie binnen 72 uur calamiteiten dienen te melden aan de toezichthouder dient de melding door alle betrokken medewerkers direct en met hoogste prioriteit te worden opgepakt.

Beoordelen of er sprake is van een datalek met meldingsplicht

Zo snel mogelijk na de melding van een incident beoordeelt de FG of er sprake is van een datalek dat valt onder de meldingsplicht van de AVG en of deze gemeld moet worden aan de toezichthouder en de betrokkene. Een organisatie hoeft niet alle datalekken te melden. De privacywet eist dat organisaties een datalek melden bij de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor ‘de rechten en vrijheden van betrokkenen’. De betrokken personen informeert de organisatie alleen als er sprake is van een hoog risico1.

Onderstaande factoren helpen om een objectieve afweging te maken:

- De aard van de inbreuk
- Zijn er persoonsgegevens gewist, gewijzigd of gelekt?
- De aard, gevoeligheid en omvang van de persoonsgegevens
- Hoe gevoeliger de gegevens, hoe groter het risico op schade
- Kun je op basis van het datalek eenvoudig zien om wie het gaat?

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838

Persoonsgegevens van gevoelige aard zijn:

- Bijzondere persoonsgegevens conform (artikel 9 AVG);
- Gegevens over de financiële of economische situatie van de betrokkene;
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting
- Gebruikersnamen, wachtwoorden en andere inloggegevens
- Gemak waarmee personen kunnen worden geïdentificeerd

Ernst van gevolgen voor personen

De gevolgen voor de betrokkene kunnen ernstig zijn als het datalek kan leiden tot bijvoorbeeld identiteitsdiefstal of reputatieschade. Het risico wordt kleiner wanneer de gegevens in handen zijn gekomen van een betrouwbare ontvanger die er niet op uit is om schade te veroorzaken.

Bijzondere kenmerken van de persoon

Wanneer gegevens van kwetsbare personen betrokken zijn bij het datalek, kunnen zij een groter risico op schade lopen. Bijvoorbeeld kinderen.

Bijzondere kenmerken van uw organisatie

Het delen van de persoonsgegevens binnen (zorg)ketens kan betekenen dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen optreden.

Het aantal getroffen personen

Over het algemeen kan een datalek grotere gevolgen hebben naarmate er meer personen bij betrokken zijn. Een inbreuk kan echter zelfs voor één persoon ernstige gevolgen hebben.

Een datalek hoeft niet gemeld te worden aan de Autoriteit Persoonsgegevens of aan de betrokkenen in de volgende gevallen:

1. Maatregelen vooraf

De organisatie heeft voordat het datalek plaatsvond passende maatregelen getroffen. Hierdoor zijn de gelekte persoonsgegevens onbegrijpelijk voor onbevoegden. Bijvoorbeeld doordat de gegevens goed zijn versleuteld. Dit geldt alleen als:

- De gegevens nog volledig intact zijn;
- De organisatie nog steeds de volledige controle over de gegevens heeft;
- De sleutel die voor de encryptie of voor de hashing is gebruikt geen gevaar heeft gelopen bij

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838

- Het datalek. En deze ook met de beschikbare technologie niet vindbaar is voor onbevoegden.

2. De onjuiste ontvanger is betrouwbaar

Zijn de persoonsgegevens verzonden aan een verkeerde maar betrouwbare ontvanger?

Dan betekent dit mogelijk dat het niet langer waarschijnlijk is dat het datalek een risico oplevert. In dat geval hoeft de organisatie het datalek dus niet te melden aan de Autoriteit Persoonsgegevens of aan de getroffen personen.

Een organisatie hoeft de betrokkenen (de personen van wie de gegevens zijn verwerkt) alleen te informeren als een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert. In de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) staat dat in de volgende situaties een datalek ook niet gemeld hoeft te worden bij betrokkene(n):

- Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens vooraf aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
- Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.
- Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

Het melden van het datalek

Het is mogelijk dat op het moment dat er gemeld moet worden, nog geen volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval vindt de melding plaats op basis van de gegevens waarover Praktijk voor Heelheid op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden introkken.

Eindverantwoordelijk

De eigenaar van Praktijk voor Heelheid is eindverantwoordelijk voor het voldoen aan de meldplicht datalekken. Op grond van de mandaatregeling meldt Praktijk voor Heelheid het datalek aan de toezichthouder en zorgt voor de verdere vervolgacties die kunnen voortkomen uit de melding.

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838

Termijn van melden

Voor het melden van een datalek aan betrokkenen geldt dat dit ‘onverwijld’ moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Gelet hierop dient een datalek binnen 72 uur te worden gemeld aan de toezichthouder. De wijze waarop betrokkenen worden geïnformeerd, bepaalt Praktijk voor Heelheid zelf.

Melden aan andere partijen

In afspraken met partijen waarmee persoonsgegevens worden uitgewisseld (verwerkers) is afgesproken dat zij een eventueel en/of potentieel datalek van persoonsgegevens die ten behoeve van CBZ worden verwerkt, onverwijld zullen melden aan CBZ. Indien zij als “verwerkingsverantwoordelijke” worden gekenmerkt zijn zij daarnaast zelf verantwoordelijk voor het maken van een melding bij de Autoriteit Persoonsgegevens.

Indien sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) Praktijk voor Heelheid moeten beoordelen of een datalek-incident aan de externe partij gemeld moet worden. Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn.

Documenteren van het datalek

De eigenaar van Praktijk voor Heelheid houdt een register bij van de meldingen van datalekken. In dit register verwerkt zij de interne en externe meldingen. Organisaties moeten alle datalekken documenteren, inclusief de feiten over het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. Dat geldt ook voor datalekken die organisaties niet hoeven te melden. Met deze documentatie moet de Autoriteit Persoonsgegevens (AP) kunnen controleren of organisaties aan de meldplicht datalekken hebben voldaan.

Verantwoordelijkheden

De eigenaar van Praktijk voor Heelheid is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder.

De eigenaar van Praktijk voor Heelheid houdt een register bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.

Astrid Lammers Praktijk voor heelheid, Gerard Doustraat 2, 7574 VW Oldenzaal
Email: info@astridlammers.nl, Tel.: 0610114532
KVK nr: 37155602, IBAN: NL11INGB0005133838