Privacy Policy

Datum: 02-03-2024

Ervarend Wijs hecht veel waarde aan de bescherming van uw persoonsgegevens. In deze Privacy Policy willen we heldere en transparante informatie geven over hoe wij omgaan met persoonsgegevens. Wij doen er alles aan om uw privacy te waarborgen en gaan daarom zorgvuldig om met uw persoonsgegevens. Ervarend Wijs houdt zich in alle gevallen aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming. Dit brengt met zich mee dat wij in ieder geval:

- Uw persoonsgegevens verwerken in overeenstemming met het doel waarvoor deze zijn verstrekt, deze doelen en type persoonsgegevens zijn beschreven in deze Privacy Policy;
- Verwerking van uw persoonsgegevens beperkt is tot enkel die gegevens welke minimaal nodig zijn voor de doeleinden waarvoor ze worden verwerkt;
- Vragen om uw uitdrukkelijke toestemming als wij deze nodig hebben voor de verwerking van uw persoonsgegevens;
- Passende technische en organisatorische maatregelen hebben genomen zodat de beveiliging van uw persoonsgegevens gewaarborgd is;
- Geen persoonsgegevens doorgeven aan andere partijen, tenzij dit nodig is voor uitvoering van de doeleinden waarvoor ze zijn verstrekt;
- Op de hoogte zijn van uw rechten omtrent uw persoonsgegevens, u hierop willen wijzen en deze respecteren.

Als Ervarend Wijs zijn wij verantwoordelijk voor de verwerking van uw persoonsgegevens. Indien u na het doornemen van ons Privacy Policy, of in algemene zin, vragen heeft hierover of contact met ons wenst op te nemen, kan dit via de contactgegevens onderaan dit document.

Verwerking van persoonsgegevens van klanten of leveranciers

Doelstelling:

Persoonsgegevens van klanten of leveranciers worden door Ervarend Wijs verwerkt ten behoeve van de volgende doelstelling(en):

- Administratieve doeleinden;
- Communicatie over de opdracht en/of uitnodigingen;
- Het uitvoering geven aan of het uitgeven van een opdracht.

Grondslag:

Grondslag voor deze persoonsgegevens is:

- De overeengekomen opdracht;
- Wettelijk bepalingen.

Persoonsgegevens:

Voor de bovenstaande doelstelling(en) kan Ervarend Wijs de volgende persoonsgegevens van u vragen:

- Voornaam;
- Tussenvoegsel;
- Achternaam;
- Adres;
- (Zakelijk) Telefoonnummer;

- (Zakelijk) E-mailadres;
- Geslacht;
- Bankrekeningnummer;
- BTW-nummer.

Bewaartermijn:

Uw persoonsgegevens worden door Ervarend Wijs opgeslagen ten behoeve van bovengenoemde verwerking(en) voor de periode:

- Gedurende de looptijd van de overeenkomst en daarna alleen in de financiële administratie voor maximaal 7 jaar.

Rechten:

U heeft het recht om uw gegevens in te zien, een verzoek in te dienen, deze te wijzigen indien deze niet kloppen of te laten vernietigen indien ze onrechtmatig gebruikt worden.

Verwerking van persoonsgegevens van cliënten

Doelstelling

Persoonsgegevens van cliënten worden door Ervarend Wijs verwerkt ten behoeve van de volgende doelstelling(en):

- Administratieve doeleinden;
- Vastleggen cliëntendossier;
- Het uitvoering geven aan de behandelingsovereenkomst.

Grondslag:

Grondslag voor deze persoonsgegevens is:

- Toestemming volgens de behandelingsovereenkomst;
- Wettelijke bepalingen;

- Noodzakelijk voor het uitvoeren van de overeenkomst.

Persoonsgegevens:

Voor de bovenstaande doelstelling(en) kan Ervarend Wijs de volgende persoonsgegevens van u vragen:

- Voornaam;
- Tussenvoegsel;
- Achternaam;
- Geboortedatum;
- Woonadres;
- Telefoonnummer;
- E-mailadres;
- Geslacht;
- Zorgverzekeraar en polisnummer;
- Huisarts;
- Gegevens over gezondheid (indien van belang voor de behandeling);
- Strafrechtelijke gegevens (indien van belang voor de behandeling);
- BSN (indien verplicht volgens wetgeving).

Bewaartermijn:

Uw persoonsgegevens worden door Ervarend Wijs opgeslagen ten behoeve van bovengenoemde verwerking(en) voor de periode:

- De bewaartermijn voor het cliëntendossier is 20 jaar. Deze termijn gaat in na het 18e levensjaar van de cliënt. Hierna wordt het dossier vernietigd.
- Uw persoonsgegevens worden door Ervarend Wijs opgeslagen ten behoeve van bovengenoemde verwerking(en) voor de periode van 20 jaar. Deze termijn gaat in na het 18e levensjaar van de cliënt.

Rechten:

Cliënten hebben het recht hun dossier in te zien en om correctie, aanvulling, of vernietiging van hun dossier te vragen. Cliënten hebben de mogelijkheid om op de behandelovereenkomst te kiezen om toestemming te geven voor vernietiging van hun dossier na een periode van 7 jaar. Ook kunnen zij vragen hun gegevens over te dragen (recht op dataportabiliteit). De zorgverlener kan een medisch dossier niet vernietigen als: Een voorschrift of wet bepaalt dat de gegevens bewaard moeten blijven; Als gegevens bewaard moeten blijven vanwege het belang van iemand anders.

Verstrekking aan derden

De gegevens die u aan ons geeft kunnen wij aan derde partijen verstrekken indien dit noodzakelijk is voor uitvoering van de hierboven beschreven doeleinden. Zo maken wij gebruik van een derde partij voor:

- Het verzorgen van de (financiële) administratie;
- Het gebruik van software voor het veilig versturen van e-mails en bestanden;
- Het gebruik van software voor het veilig opslaan van gegevens;
- Het gebruik van software voor het elektronisch cliëntendossier;
- Het gebruik van software voor het declareren bij gemeenten.

Wij geven nooit persoonsgegevens door aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten. Met deze partijen (verwerkers) maken wij hierin uiteraard de nodige afspraken om de beveiliging van uw persoonsgegevens te waarborgen.

Verder zullen wij de door uw verstrekte gegevens niet aan andere partijen verstrekken, tenzij dit wettelijk verplicht en toegestaan is. Een voorbeeld hiervan is dat de politie in het kader van een onderzoek (persoons)gegevens bij ons opvraagt. In zo'n geval dienen wij medewerking te verlenen en zijn dan ook verplicht deze gegevens af te geven. Tevens kunnen wij persoonsgegevens delen met derden indien u ons hier schriftelijk toestemming voor geeft.

Binnen de EU

Wij verstrekken geen persoonsgegevens aan partijen die gevestigd zijn buiten de EU.

Minderjarigen

Wij verwerken enkel en alleen persoonsgegevens van minderjarigen (personen jonger dan 16 jaar) indien daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.

Bewaartermijn

Ervarend Wijs bewaart persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor deze zijn verstrekt dan wel op grond van de wet is vereist. Voor het cliëntendossier is de wettelijke bewaartermijn 20 jaar. Deze termijn gaat in na het 18e levensjaar van de cliënt.

Beveiliging

Wij hebben passende technische en organisatorische maatregelen genomen om persoonsgegevens van u te beschermen tegen onrechtmatige verwerking, zo hebben we bijvoorbeeld de volgende maatregelen genomen;

- Alle personen die namens Ervarend Wijs van uw gegevens kennis kunnen nemen, zijn gehouden aan geheimhouding daarvan;
- We hanteren een gebruikersnaam en wachtwoord beleid op al onze systemen;
- We pseudonimiseren en zorgen voor de encryptie van persoonsgegevens als daar aanleiding toe is;
- Wij maken back-ups van de persoonsgegevens om deze te kunnen herstellen bij fysieke of technische incidenten;
- We testen en evalueren regelmatig onze maatregelen;

Rechten omtrent uw gegevens

U heeft recht op inzage, rectificatie of verwijdering van de persoonsgegevens die wij van u ontvangen hebben. Tevens kunt u bezwaar maken tegen de verwerking van uw persoonsgegevens (of een deel hiervan) door ons of door één van onze verwerkers. De zorgverlener kan een medisch dossier niet vernietigen als: Een voorschrift of wet bepaalt dat de gegevens bewaard moeten blijven; Als gegevens bewaard moeten blijven vanwege het belang van iemand anders. Ook heeft u het recht om de door u verstrekte gegevens door ons te laten overdragen aan uzelf of in opdracht van u direct aan een andere partij. Wij kunnen u vragen om u te legitimeren voordat wij gehoor kunnen geven aan voornoemde verzoeken.
Mogen wij uw persoonsgegevens verwerken op basis van een door u gegeven toestemming hiertoe, dan heeft u altijd het recht deze toestemming in te trekken.

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.

<u>Voorbeelden van een datalek zijn:</u>
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 Ervarend Wijs word 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.

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 Ervarend Wijs zijn, of met een informatiebeveiligingsincident, dient dit te melden bij het bestuur. 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 het Bestuur hiervoor benaderen. Het bestuur 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 risico.

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. 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	Kun je op basis van het datalek eenvoudig zien om wie het gaat?

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 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 Persoongsgevens 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):

1. 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.
2. 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.
3. 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 Ervarend Wijs op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden introkken.

Bestuur eindverantwoordelijk

Het bestuur is eindverantwoordelijk voor het voldoen aan de meldplicht datalekken. Op grond van de mandaatregeling meldt Ervarend Wijs het datalek aan de toezichthouder en zorgt voor de verdere vervolgacties die kunnen voortkomen uit de melding.

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 Ervarend Wijs 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) zal Ervarend Wijs 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

Het Bestuur 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

Het Bestuur is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder.
Het Bestuur 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

Klachten

Mocht u een klacht hebben over de verwerking van uw persoonsgegevens dan vragen wij u hierover direct contact met ons op te nemen. Komen wij er samen met u niet uit dan vinden wij dit natuurlijk erg vervelend. U heeft altijd het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, dit is de toezichthoudende autoriteit op het gebied van privacybescherming. Voor meer informatie bij klachten verwijzen wij u naar het document Klachtenregeling.

Cookies

Wij maken op onze website gebruik van cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van deze website wordt meegestuurd en door uw browser op uw harde schijf van uw computer wordt opgeslagen. Wij gebruiken cookies om het gebruik van onze website te vergemakkelijken. U kunt deze cookies uitzetten via uw browser, maar dit kan het functioneren van onze website negatief beïnvloeden.

Vragen

Als u naar aanleiding van onze Privacy Policy nog vragen of opmerkingen heeft neem dan contact met ons op!

Contactgegevens

Ervarend Wijs

Oude Bornseweg 85-1

7556 GW Hengelo

Algemene nummer: 06-57428477

info@ervarendwijs.nl

www.ervarendwijs.nl