

HOE BESCHERM JE DE PRIVACY VAN CLIËNTEN?





INHOUDSOPGAVE

Abrona, aandacht voor privacy	4
Welke privacyrechten hebben cliënten?	6
Hoe worden cliënten geïnformeerd over hun privacyrechten?	7
Hoe bescherm je de privacy van cliënten als je zorg verleent?	8
Hoe kun je bewuster omgaan met persoonlijke informatie van de cliënt?	9
Toestemming vragen, hoe zit dat?	11
Waar bewaar je cliëntgegevens?	13
Hoe lang mag je cliëntgegevens bewaren?	14
Hoe wissel je cliëntgegevens uit?	15
Hoe gebruik je cliëntgegevens in sociale media?	16
Wat doet de functionaris gegevensbescherming?	17
Een datalek! En nu?	18
Heb jij weleens een privacymomentje?	20
Tien privacytips	21
Meer informatie	22



ABRONA, AANDACHT VOOR PRIVACY

Abrona wil voor haar cliënten een veilige en respectvolle ontmoetingsplaats zijn. Dat betekent dat het belangrijk is om zorgvuldig om te gaan met de persoonsgegevens en informatieveiligheid van cliënten, familie én medewerkers. Wij noemen dit aandacht voor privacy.

In de Algemene Verordening Gegevensbescherming (AVG) staat hoe organisaties moeten omgaan met persoonsgegevens en de informatieveiligheid die nodig is. Wij verwerken alleen persoonsgegevens als daar een goede reden voor is. En we doen dit alleen voor een specifiek doel. In de wet staat ook dat cliënten, familie en medewerkers recht hebben op informatie en inzage.

Omgaan met persoonsgegevens en informatieveiligheid is niet alleen een ict-aangelegenheid. Ook jij bent belangrijk als het gaat om de privacy van cliënten en familie. Het is belangrijk dat je op de hoogte bent van onze privacy-afspraken. Daarom dit boekje. Je vindt er antwoorden op belangrijke vragen over de privacy van cliënten en familie. Op dezelfde manier beschermen we ook de gegevens van medewerkers.

Meer informatie vind je in de community Privacy & Informatie-veiligheid op ons intranet. Heb je vragen? Stuur dan een mail naar de functionaris gegevensbescherming: privacy@abrona.nl.

We rekenen op je medewerking!

Jan Duenk

Voorzitter raad van bestuur





WELKE PRIVACYRECHTEN HEBBEN CLIËNTEN?

Rechten van cliënten zijn vastgelegd in verschillende wetten. Ook in de privacywetgeving zijn bepaalde rechten van cliënten opgenomen.

Het gaat hierbij om rechten op het gebied van gegevensverwerking:

- het recht op inzage in de persoonsgegevens die wij van hen verwerken
- het recht op informatie over welke gegevens wij van hen verwerken en hoe wij met deze gegevens omgaan
- het recht om hun persoonsgegevens eenvoudig over te dragen aan een andere zorgaanbieder
- het recht om (een deel van) hun gegevens te laten verwijderen, te corrigeren en af te schermen
- het recht om bezwaar in te dienen als zij van mening zijn dat hun persoonsgegevens niet juist worden verwerkt.



HOE WORDEN CLIËNTEN GEÏNFORMEERD OVER HUN PRIVACYRECHTEN?

Op de website van Abrona, bij het aanmeldformulier of bij het eerste contact met een behandelaar wordt de cliënt geïnformeerd door middel van een privacyverklaring. Hierin staat informatie over de doeleinden waarvoor Abrona persoonsgegevens verwerkt en met wie deze persoonsgegevens worden gedeeld. Ook staat hierin beschreven welke rechten cliënten hebben en bij wie je terecht kunt als je vragen of klachten hebt.

Cliënten kunnen jou ook vragen stellen over privacy. Lees daarom de privacyverklaring goed door. Voor cliënten is er een eenvoudige versie van de privacyverklaring. Deze kun je vinden in de community Privacy & Informatieveiligheid op intranet.



HOE BESCHERM JE DE PRIVACY VAN CLIËNTEN ALS JE ZORG VERLEENT?

Zorg verlenen aan mensen met een verstandelijke beperking betekent ook vaak een inbreuk op hun persoonlijke levenssfeer. Bijvoorbeeld bij een medische handeling, diagnostisch onderzoek en als je bij een cliënt in zijn woning of kamer zorg verleent of begeleiding biedt. Hierbij is het van belang dat dit discreet en zorgvuldig gebeurt, buiten de waarneming om van anderen, tenzij de cliënt daarmee heeft ingestemd. Ook op het gebied van persoonlijke informatie van de cliënt kunnen we de privacy van cliënten beschermen door zorgvuldig te handelen. Dit doe je door rekening te houden met de volgende punten:

- Weet wanneer je toestemming moet vragen voor het verwerken van persoonsgegevens. Lees verderop: 'Toestemming vragen, hoe zit dat?'
- Denk na voor welk doel je persoonsgegevens verwerkt. Dit is bijvoorbeeld: het rapporteren in het dossier van een cliënt over de voortgang van de gemaakte afspraken.
- Zorg voor zo min mogelijk inbreuk op de privacy van cliënten.
- En verwerk persoonsgegevens alleen wanneer dat noodzakelijk is voor goede zorg, behandeling of ondersteuning.



HOE KUN JE BEWUSTER OMGAAN MET PERSOONLIJKE INFORMATIE VAN DE CLIËNT?

In de privacywet staan twee niveaus van persoonlijke informatie:

- **Persoonsgegevens**
Een persoonsgegeven is alle informatie die herleidbaar is tot een persoon, zoals naam, adres en ook beeld en geluid. Je kunt bijvoorbeeld met postcode én huisnummer al achterhalen waar iemand woont.
- **Bijzondere persoonsgegevens**
Gevoelige persoonsgegevens krijgen extra bescherming. De privacywet noemt dit 'bijzondere persoonsgegevens'. Informatie over gezondheid, ras en godsdienst zijn voorbeelden van bijzondere persoonsgegevens.

Verwerken van persoonsgegevens

Als je persoonsgegevens opslaat, verzamelt, wijzigt, raadpleegt, wist of verspreidt, dan verwerk je persoonsgegevens. Als je rapporteert over de voortgang van de gemaakte afspraken met cliënten, dan



verwerk je persoonsgegevens, ook als je gegevens van de cliënt op een formulier invult.

Privacyreglement Abrona

Denk goed na of het verwerken van persoonsgegevens in lijn is met het privacyreglement van Abrona. Hierin staat welke afspraken er zijn binnen Abrona over hoe we omgaan met privacy. Het privacyreglement is te vinden in de community Privacy & Informatieveiligheid op intranet.



TOESTEMMING VRAGEN, HOE ZIT DAT?

Toestemming vragen voor het delen van informatie

Als iemand je vraagt om informatie van een cliënt te delen, bedenk dan dat je meestal toestemming nodig hebt van de cliënt. Toestemming vraag je altijd schriftelijk. Hierbij geef je duidelijk aan waarvoor toestemming wordt gevraagd. Ook geef je aan dat de toestemming altijd mag worden ingetrokken en hoe cliënten dit kunnen doen. Het ingevulde toestemmingsformulier moet voorzien zijn van een datum en in het digitale dossier van de cliënt worden opgeslagen.

Wist je dat je altijd toestemming nodig hebt voor het maken van foto's en video's van cliënten? Je legt hierbij uit waarvoor je de foto of video wilt gebruiken. Ook heb je altijd toestemming nodig als studenten persoonsgegevens van cliënten willen opvragen voor onderzoek.

Er zijn verschillende toestemmingsformulieren beschikbaar, afhankelijk van waarvoor je toestemming vraagt. In het Kwaliteitshandboek vind je de Procedure Dossiervorming en de bijbehorende toestemmingsformulieren. In de community Privacy & Informatieveiligheid op intranet staan de verwijzingen naar alle beschikbare toestemmingsformulieren.



Wanneer is geen toestemming nodig?

Als er een wettelijke verplichting is om persoonsgegevens te verwerken, hoef je geen toestemming te vragen. Dit is bijvoorbeeld bij het aanleggen van een medisch dossier. Ook hoef je geen toestemming te vragen als het verwerken van persoonsgegevens noodzakelijk is om de dienstverleningsovereenkomst met de cliënt uit te voeren. Bijvoorbeeld voor het opstellen van het ondersteuningsplan. Twijfel je of toestemming gevraagd moet worden? Vraag dan de functionaris gegevensbescherming om advies.



WAAR BEWAAR JE CLIËNTGEGEVENS?

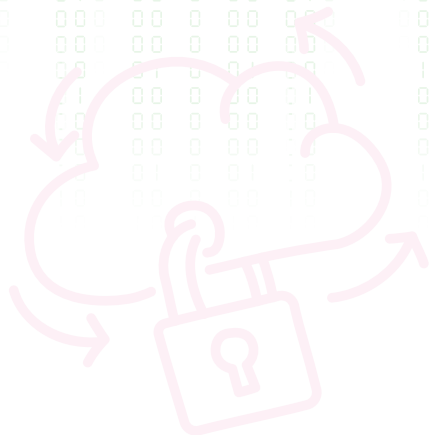
Cliëntgegevens worden opgeslagen in het ECD mijnCaress en/of behandeldossier Ysis. Dit is de enige plaats waar je cliëntgegevens mag opslaan en waar ze afdoende worden beveiligd. Een papieren archief is moeilijk actueel te houden en gevoelig voor verlies. Dit mag je daarom niet toepassen. Hetzelfde geldt voor algemeen toegankelijke netwerkschijven zoals de P-schijf en de G-schijf (of in Office 365 OneDrive, Sharepoint of Teams). Alleen met goed beveiligde opslag kun je verantwoording afleggen over het zorgvuldig omgaan met persoonsgegevens van cliënten.

TIP: Als papieren of digitale cliëntinformatie nog niet in het ECD mijnCaress of behandeldossier Ysis zit, plaats dit daar dan alsnog. Vernietig de oude (papieren) versie. Twijfel je? Overleg dan met de functionaris gegevensbescherming.



HOE LANG MAG JE CLIËNTGEGEVENS BEWAREN?

De wettelijke termijn voor het bewaren van zorggegevens is 15 jaar nadat het cliëntendossier is afgesloten of de zorg- of behandelrelatie is beëindigd. Lees meer hierover op intranet in het Kwaliteitshandboek (dossievorming).



HOE WISSEL JE CLIËNTGEGEVENS UIT?

Uitwisselen van cliëntgegevens binnen Abrona gaat via het ECD mijnCaress of via het behandel dossier Ysis. Interne mail wordt niet gebruikt voor het uitwisselen van cliëntgegevens. Is het toch noodzakelijk om cliëntinformatie te mailen? Dan kan dit alleen met beveiligde mail.*
Cliëntgegevens verstuur je nooit via WhatsApp of andere sociale media. Ook zijn onbeveiligde mail en fax niet toegestaan. In sommige gevallen worden cliëntgegevens per post uitgewisseld. Denk er dan wel aan dat deze post het kenmerk persoonlijk krijgt en aangetekend moet worden verzonden.
Controleer bij het verzenden van mail altijd of het adres van de ontvanger correct is en of de juiste bijlagen zijn bijgevoegd.

TIP: Overweeg altijd eerst of het echt noodzakelijk is dat je de gevoelige gegevens per mail verstuurt. Soms zijn er goede alternatieven.

** Beveiligd gegevens uitwisselen kan via M-Safe en in de nieuwe Outlook vanaf medio juni 2018*



HOE GEBRUIK JE CLIËNTGEGEVENS IN SOCIALE MEDIA?

Sociale media, zoals WhatsApp, Facebook, Twitter, Instagram, Snapchat of LinkedIn, gebruik je niet om informatie over cliënten te delen. Je communiceert op sociale media niet over cliënten.

Wil je toch graag een foto van een cliënt op sociale media plaatsen? Vraag dan altijd eerst vooraf schriftelijk toestemming aan de cliënt of zijn wettelijk vertegenwoordiger. Zonder toestemming mag je geen foto's plaatsen. Let op, de cliënt kan de toestemming weer intrekken. Je moet de foto dan weer verwijderen.

TIP: Beoordeel goed of het delen van de foto nadelige gevolgen kan hebben voor de cliënt.



WAT DOET DE FUNCTIONARIS GEGEVENS BESCHERMING?

Als je het onderwerp privacy regelmatig op de agenda van de teamvergaderingen zet dan kun je bespreken waar je tegenaan loopt, welke risico's jullie zien of waar nog vragen over zijn. Aarzel niet en neem gerust contact op met de functionaris gegevensbescherming (FG). De privacywet stelt de FG verplicht. De FG is onafhankelijk en is een vraagbaak voor alle privacy-gerelateerde vragen uit onze organisatie.

Deze functionaris:

- houdt intern toezicht op het verwerken van persoonsgegevens
- helpt cliënten en medewerkers met vragen over het verwerken van persoonsgegevens
- handelt klachten af die te maken hebben met privacy van cliënten
- zorgt voor meer bekendheid over privacywetgeving bij Abrona
- maakt een overzicht van alle gegevensverwerkingen
- zorgt dat risicoanalyses worden uitgevoerd voor de meest privacy-gevoelige gegevensverwerkingen
- houdt meldingen van datalekken bij
- ontwikkelt interne privacyregelingen
- levert input voor het opstellen of aanpassen van gedragscodes.



EEN DATALEK! EN NU?

Stel dat een laptop gestolen wordt waar persoonsgegevens op staan.

Dan kunnen deze persoonsgegevens blootgesteld zijn aan derden die geen toegang tot deze gegevens mogen hebben. Dit is een datalek.

Bij datalekken is altijd sprake van een inbreuk op de beveiliging van persoonsgegevens, waarbij de kans aanwezig is dat persoonsgegevens naar buiten zijn gekomen.

Andere voorbeelden van datalekken zijn:

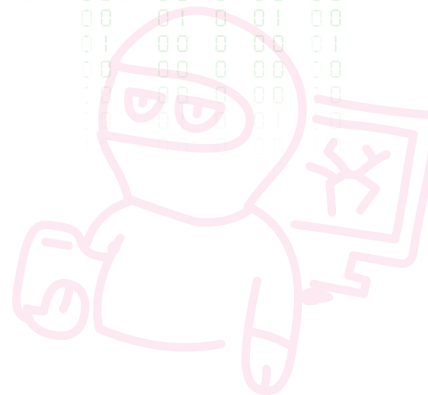
- een inbraak in een databestand door een hacker
- een gestolen of verloren mobiele telefoon
- een zoekgeraakte cliëntrapportage
- een kwijtgeraakte usb-stick
- een dossier is naar de verkeerde ontvanger verstuurd.

Waar meld je een datalek?

Heb je een vermoeden van een datalek? Meld dit meteen in onze applicatie Topdesk (onder de optie 'Datalek'). De melding komt dan automatisch terecht bij onze functionaris gegevensbescherming.

En daarna?

De melding van een datalek komt terecht bij onze functionaris gegevensbescherming. Deze stelt vast of we het datalek moeten melden bij de Autoriteit Persoonsgegevens (AP). De AP houdt toezicht op de naleving van de privacywetgeving en adviseert over de nieuwe regelgeving. Bij Abrona willen we ook leren van incidenten. Hoe heeft het kunnen gebeuren en hoe kunnen we een volgend datalek voorkomen? Zo helpen we elkaar in het nog beter beschermen van de privacy-gevoelige gegevens!





HEB JIJ WELEENS EEN PRIVACYMOMENTJE?

Kies eens een dag waarbij je bij alles wat je doet bewust nadenkt of je de privacybeschermingsmomenten herkent. Een paar voorbeelden:

- je zit achter je computer: kan er iemand meelesen?
- in een multi-disciplinair overleg bespreken jullie cliënten: kan er iemand meeluisteren die geen betrokkene is?
- met wie deel je gegevens van cliënten en vraag je je weleens af of dat wat minder kan en of het echt nodig is?
- op welke wijze deel je privacygevoelige gegevens?
- gebruik je misschien dezelfde inloggegevens als (een) collega('s)?
- hoe vaak print je een document met persoonsgegevens van een cliënt? Bedenk steeds of je het echt moet printen. Moet dat toch echt, vernietig het document dan na gebruik direct.

Deel de uitkomsten met je collega's om ervan te leren en stel zo nodig vragen aan de functionaris gegevensbescherming.

Het kan zijn dat er een vraag of klacht is over privacybescherming. Dan is het belangrijk dat de functionaris gegevensbescherming hiervan op de hoogte is, zodat deze met jou de vraag of klacht kan oplossen. Het mailadres van de functionaris gegevensbescherming is:
privacy@abrona.nl



TIEN PRIVACYTIPS

1. Praat nooit in een openbare ruimte over cliënten. Ga naar een afgesloten ruimte, dan blijft het gesprek vertrouwelijk.
2. Gebruik geen sociale media (Facebook, WhatsApp, Instagram, etc.) om informatie over je werk en/of cliënten te delen.
3. Vraag vooraf én schriftelijk toestemming aan de cliënt als je een foto of film waar de cliënt op staat, wilt publiceren.
4. Denk je een datalek te herkennen, geef dit dan direct door aan de functionaris gegevensbescherming.
5. Lees de privacyverklaring voor cliënten goed door, zodat je vragen van cliënten goed kunt beantwoorden.
6. Gebruik unieke wachtwoorden. Deel je wachtwoord niet. Een wachtwoordkluis helpt als je veel wachtwoorden moet onthouden.
7. Vergrendel je computer als je even van je werkplek wegloopt (Ctrl-alt-del-enter).
8. Koppel geen andere apparaten, zoals usb-sticks, diskdrives en camera's aan je computer.
9. Laat nooit een afdruk onbeheerd bij de printer achter. Haal het direct op.
10. Raadpleeg de community Privacy & Informatieveiligheid op intranet als je meer vragen hebt of neem contact op met de functionaris gegevensbescherming.



MEER INFORMATIE

Neem contact op met de Functionaris gegevensbescherming:

privacy@abrona.nl

Of ga voor meer informatie naar de Community Privacy & Informatie-veiligheid op intranet.

Sterrenberglaan 6
3712 XA Huis ter Heide
088 201 99 11

info@abrona.nl
www.abrona.nl

AANDACHT VOOR PRIVACY



