PROCEDURE
KRAAMZORG-ADMINISTRATIE

LIA VAN DER MEIJS

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing, welke de Europese vervanger van de Wet bescherming persoonsgegevens is. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacy rechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

De zelfstandige/ZZP is hoofdverantwoordelijk voor het naleven van de AVG.

Risico's verminderen

In de kraamzorg worden vele privacygevoelige gegevens van cliënten opgeslagen. Je moet er niet aan denken dat die gegevens op straat komen te liggen. Denk hierbij aan diefstal/verminking van gegevens, of dat onbevoegde personen de gegevens bekijken. Of zelfs die gegevens ongewenst veranderen. Het belangrijkste is dat degene die deze gegevens administreert, zich er bewust van is dat ze deze data moeten beschermen.

Eenvoudige gedragsregels doorvoeren kan al veel schelen:

1. Stuur geen privacygevoelige informatie over de reguliere e-mail, zonder versleuteling met een wachtwoord.
2. Vergrendel je PC als je wegloopt. Dit kan door Windows-L in te toetsen.
3. Zorg voor goede virusscanners op je computer.
4. Maak een veiligheidskopie van je data op een usb-stick en bewaar die in een kluis.
5. Als je informatie doorstuurt, weeg dan goed af aan welke partijen je welke informatie geeft, en op welke manier je dat verstuurt.
6. Vraag aan cliënten om toestemming, indien van toepassing. Leg vast dat toestemming is gegeven.

Beveiliging met wachtwoord.

- Het is van groot belang om te kiezen voor een sterk wachtwoord (minimaal 8 tekens en gebruik hoofdletters, speciale tekens en cijfers).
- Zorg dat je wachtwoord niet gemakkelijk te raden is (gebruik bijvoorbeeld géén namen en geboortedata).
- Bewaar inloggegevens op een veilige plek, liefst achter een code of wachtwoord. Een post-it op je computerscherm plakken is géén goede locatie.
- Deel je inloggegevens niet met andere personen en maak ook géén gezamenlijke inloggegevens.

De volgende gegevens worden vastgelegd:

Client, zwangerschap en bevalling

- Registratie van de gegevens rondom de cliënt, zwangerschap, bevalling, partner en kinderen.
- Registratie van uren, verbruikte producten en vaste kosten (bijvoorbeeld inschrijfkosten) met betrekking tot de cliënt.
- Het bepalen van benodigde zorguren op basis van het Landelijk Indicatieprotocol Kraamzorg (LIP).
- Gebruik van brieven en e-mail (aansluitmogelijkheden op Vecozo-dienstverlening blijven volgen).
- Documentbeheer; ook externe documenten kunnen worden opgeslagen bij de betreffende cliënt, of indien niet van toepassing in een algemene folder.
- Registratie van verloskundige Samenwerkingsverbanden (VSV's), mogelijk via Vecozo.
- Registratie van zorgplan/zorgpaden.

Op de PC via beveiliging (AxCrypt) vastleggen:

- Aparte folder per cliënt,
- Hierin brieven, bestede uren, zorgplannen, overdrachtsdocumenten etc. bewaren.
- De folders te beveiligen met een wachtwoord (kan in een keer als je alles onderbrengt onder een groepsfolder).
- Financiële en zorgdocumentatie te scheiden in aparte folders.
- Eenmaal per maand back-up maken en deze opbergen op veilige plaats (bij voorkeur kluis).
- Minimaal de twee laatste versies in een back-up bestand blijven bewaren.

Persoonsgegevens moeten op volgende wijze worden vastgelegd:

- Op een rechtmatige en transparante wijze,
- Alleen verzameld te worden op grond van een duidelijk doel en niet te worden gebruikt voor andere zaken dan dat doel,
- Echt nodig te zijn om je kraamzorgactiviteiten uit te voeren. Verzamel en verwerk alleen de gegevens die je echt nodig hebt.
- Correct te zijn als ze worden opgeslagen. Gegevens die niet correct zijn dienen te worden aangepast of verwijderd.
- Goed te worden beveiligd, zodat het risico op verlies of verandering wordt geminimaliseerd.
- Verwijder gegevens welke je niet meer nodig hebt,
- Verwijder gegevens welke niet meer nodig zijn om in de toekomst nog op enigerlei wijze te moeten verantwoorden (na 7 jaar moeten bestanden worden verwijderd).

Het AVG-10 stappenplan

Met het AVG-10 stappenplan krijgt u snel overzicht op een aantal belangrijke AVG-thema's waar u zich op moet voorbereiden. Dit zijn:

1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data protection impact assessment (DPIA)
5. Privacy by design & privacy by default
6. Functionaris voor de gegevensbescherming
7. Meldplicht datalekken
8. Verwerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

In 10 stappen voorbereid op de AVG

- Stap 1: Bewustwording

  Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

  De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven. Zoals de website hulpbijprivacy.nl en de AVG-regelhulp. Maar ook guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.
  Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

- Stap 2: Rechten van betrokkenen

  Onder de AVG krijgen betrokkenen (de mensen van wie u persoonsgegevens verwerkt) meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

- Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht.
U kunt het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

- Stap 4: Data protection impact assessment (DPIA)

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.
Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start.

Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

- Stap 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.
Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.
Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

- Stap 6: Functionaris voor de gegevensbescherming

  Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

- Stap 7: Meldplicht datalekken

  De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.
  Dit gaat verder dan de huidige protocolplicht uit de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de gemelde datalekken.

  De Europese privacytoezichthouders hebben in oktober 2017 guidelines gepubliceerd over de meldplicht datalekken onder de AVG. Deze guidelines zijn nog niet definitief, maar staan open voor publieke consultatie. Wanneer de guidelines definitief zijn, kunnen wij u volledig informeren over de meldplicht datalekken onder de AVG.
- Stap 8: Verwerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? (nu nog 'bewerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

- Stap 9: Leidende toezichthouder
  Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.
- Stap 10: Toestemming
  Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan.
  Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.