Verwerkingsregister AVG John Hacking

1. Benoeming persoonsgegevens

De volgende persoonsgegevens leg ik vast van cliënten in een onderzoek aangeboden door de Studentenkerk Radboud Universiteit Nijmegen (voor studenten en medewerkers van de Radboud Universiteit (RU) en de Hogeschool Arnhem Nijmegen (HAN))

Naam, telefoonnummers, studierichting en E-mail adressen

Ik werk niet met minderjarige cliënten. Ik werk niet met opdrachtgevers.

Opmerking over het vastleggen van bijzondere persoonsgegevens:
Gegevens over godsdienst of levensovertuiging, gezondheid, zaken m.b.t. de seksualiteit, of strafrechtelijke gegevens worden bijzondere gegevens genoemd.
Het verwerken van bijzondere persoonsgegevens is in principe verboden, tenzij u zich op een wettelijke uitzondering kunt beroepen. Indien de gegevens worden verwerkt in het kader van gezondheidszorg, hulpverlening, of sociale dienstverlening is verwerking toegestaan, maar alleen als dat gebeurt door een beroepsbeoefenaar met een beroepsgeheim of andere persoon die aan geheimhouding is gebonden. Deze uitzondering geldt dus op basis van de Wet op de geneeskundige behandelovereenkomst (WGBO) ook voor complementaire of alternatieve zorgverleners die zijn geregistreerd bij RBCZ.

Indien dit in het belang is van de coaching, kunnen de volgende bijzondere persoonsgegevens besproken en vastgelegd worden echter alleen indien ze strikt zijn gerelateerd aan door cliënt aangegeven coaching aspecten:

Godsdienst of levensovertuiging, gezondheid, zaken m.b.t. seksualiteit, mogelijke gebruik van (seksueel) geweld en uiteraard de hulpvragen en coaching doelstellingen

Het Burger Service Nummer (BSN) leg ik niet vast.

In een ZKM coaching traject worden 'persoonlijke momenten' van cliënt vastgelegd, de cliënt formuleert zelf deze persoonlijke momenten. Ze blijven tijdens het gehele traject onderdeel uitmaken van het dossier.

2. Doeleinden van de persoonsgegevens die door mij worden verwerkt.

Behalve de AVG, is het ZKM Kwaliteitssysteem van mijn beroepsvereniging (de ZKMvereniging), van toepassing op mijn werk. In dit Kwaliteitssysteem en met name in het Privacyreglement is vastgelegd waarom en met welke beveiligingen persoonsgegevens vastgelegd kunnen en moeten worden. Ik werk volledig conform het ZKM Kwaliteitssysteem zoals ik zichtbaar is op de website van de Vereniging aangegeven door het kwaliteitskeurmerk bij mijn naam. Zie https://www.zkmvereniging.nl/vind-een-zkm-coach

Het vastleggen van de persoonsgegevens is nodig ter bevordering van de effectiviteit van het coaching traject voor de cliënt.

Dossierplicht
Op grond van de kwaliteitseisen van mijn beroepsverenigingen de ZKM-vereniging houd ik elektronisch een cliëntdossier bij, waarin de uitslagen van het onderzoek worden bewaard. Ik overhandig tijdens het traject de cliënt een fysieke kopie van deze elektronische documenten met de uitslagen van het onderzoek.

Fysiek bewaar ik alleen de getekende overeenkomsten en mijn persoonlijke aantekeningen. Deze fysieke documenten worden achter slot en grendel bewaard.

Bewaartermijn
Voor cliënten heeft mijn beroepsvereniging de ZKMvereniging de bewaartermijn op 7 jaar vastgesteld conform het privacyreglement. Mijn cliënten kunnen zelf aangegeven wanneer ze een andere bewaartermijn wensen te hanteren. Dat wordt opgenomen in de schriftelijke overeenkomst met cliënt. Na 7 jaar of korter indien afgesproken vernietig ik de cliëntgegevens zoals overeenkomst en persoonlijke aantekeningen. Ik bewaar geen fysieke dossiers met de uitkomsten van het ZKM onderzoek.

Beroepsgeheim
Voor mij als ZKM coach geldt op grond van de beroepscode van mijn beroepsvereniging de ZKMvereniging en het NIP een geheimhoudingsplicht. Ik heb geen Subverwerkers die aan de Studentenkerk zijn verbonden. Een ZKM coaching traject bestaat uit een of twee Zelfonderzoeken.

3. Hoe ik cliënt informeer over de vastlegging van persoonsgegevens

Deze informatie ligt vast in de overeenkomst waarin alle afspraken met cliënt zijn vastgelegd met betrekking tot het coaching traject.

4. Wie werken er daadwerkelijk met de cliëntdossiers?

Ik ben de enige die toegang heeft tot de dossiers. Vanuit de beroepscode heb ik een beroepsgeheim.

5. Hoe heb ik de beveiliging van de persoonsgegevens (cliëntendossiers) geregeld

Persoonlijke aantekeningen en getekende overeenkomsten bewaar ik in een afgesloten kast. Ik bewaar geen fysieke cliëntendossiers met de uitkomsten van het onderzoek.

Ik werk tevens met een digitaal dossier. Alle bestanden in dat dossier zijn geanonimiseerd en zijn beveiligd door een wachtwoord.

Ik maak dagelijks automatisch een back-up van mijn bestanden, op een server op de universiteit staat. Daarnaast maak ik ook regelmatig een back-up op een externe schijf die op een andere veilige locatie wordt opgeborgen.

Doordat ik regelmatig de laatste versie update van mijn software installeer, zorg ik er voor dat mijn software optimaal beveiligd is. Het gaat daarbij om:

- *Microsoft Windows 10 (via de universiteit)*
- *Apple software*
- *F-secure anti-virus (via de universiteit)*

6. Welke externe personen of bedrijven hebben toegang tot de persoonsgegevens en behoren daarmee tot de groep verwerkers waarmee ik een verwerkersovereenkomst heb afgesloten.

Leveranciers waarmee ik een verwerkersovereenkomst heb afgesloten zijn:

De ZKMvereniging als leverancier van het ZKM Computer Service waarmee ik werk om een Zelfonderzoek te kunnen doen.

De enige gegevens die tijdelijk worden vastgelegd in de ZKM Computer Service, zijn de 'persoonlijke momenten' van een cliënt. Gegevens zoals naam, emailadres e.d. worden niet vastgelegd in de ZKM Computer Service. Enkele weken nadat verwerking van de 'persoonlijke momenten' heeft plaatsgevonden, verwijder ik deze gegevens weer uit de ZKM Computer Service.

7. Hoe ga ik om met eventuele datalekken

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (dus ook ZKM coaches) direct (binnen 72 uur na het datalek) een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben.
Soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). *Voorbeelden van datalekken zijn:* een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Wanneer moet u een datalek melden?
U hoeft een datalek alleen te melden aan de Autoriteit Persoonsgegevens, als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als een aanzienlijke kans bestaat dat dit gebeurt. Dat is het geval als er bij het datalek ofwel persoonsgegevens verloren zijn gegaan (ze zijn voor u niet meer terug te halen en er was geen back-up) ofwel onrechtmatige verwerking van de persoonsgegevens niet is uit te sluiten (iemand heeft mogelijk toegang (gehad) tot de persoonsgegevens terwijl diegene daartoe niet bevoegd was en u hebt geen controle over wat diegene met de gegevens heeft gedaan of nog zal doen).

U hoeft de betrokkenen (de cliënten van wie u gegevens verwerkt) alleen te informeren als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. Dat kan het geval zijn als er gegevens van gevoelige aard zijn gelekt (bijvoorbeeld gezondheidsgegevens) die door derden kunnen worden misbruikt.

Ik heb de uitleg begrepen en zal er naar handelen:

Ik begrijp wanneer ik een datalek moet melden en zal daar naar handelen

Ik heb afspraken gemaakt in de verwerkersovereenkomst met leveranciers en ik word daardoor tijdig geïnformeerd als er een datalek is geweest

Nijmegen 25 mei 2018

John Hacking