BOZ Verwerkingsovereenkomst

Data Processing Agreement (DPA)

Waarom nieuwe BOZ verwerkersovereenkomst?

- **Vervanging Nederlandse Wbp (mei 2018) door de Europese AVG**
  - Oude model was gebaseerd op Wbp
- **AVG in verhouding tot Wbp;**
  - Aanvullende verplichtingen voor de verwerkingsverantwoordelijke m.b.t. (bijzondere) persoonsgegevens en de derde als verwerker.
- **Zorgorganisaties**
  - Verwerken vooral (bijzondere) persoonsgegevens van patiënten/medewerkers
    - Rechtspersonen die een uitwisselingssysteem hanteren waarmee zorgaanbieders medische persoonsgegevens van patiënten kunnen uitwisselen (LSP, RSO's, Zorggroepen) vallen hier ook onder!
- **Verwerkingsovereenkomst**
  - Als zorgorganisatie (verwerkingsverantwoordelijke) het verwerken van persoonsgegevens uitbesteed aan een derde, moet met deze derde een verwerkingsovereenkomst worden aangegaan.

Aanpassingen op hoofdlijnen 1

- **Van Bewerkers- naar Verwerkingsovereenkomst**
  - Strengere regels aan verwerking (hoe ermee om te gaan en waarvoor te gebruiken.)

- **Wat moet in de verwerkersovereenkomst worden geregeld?**
  - Doeleind(en) van de verwerking (doelbinding),
  - De manier van beveiliging van gegevens (psuedonimisering),
  - De te verlenen hulp bij het uitvoeren van rechten van individuen en/of beveiliging verwerking, melding datalek aan AP en betrokkene, uitvoeren DPIA incl. raadpleging AP bij een hoog risico;
  - Omgang met persoonsgegevens buiten de EU/EER.
  - Dat verwerker op basis schriftelijke instructies van verantwoordelijke persoonsgegevens verwerkt;
  - Welke typen persoonsgegevens er verwerkt worden / op welke categorieën betrokkenen de gegevens betrekking hebben;
  - De verplichting om geheimhouding op te leggen aan de tot het verwerken van de persoonsgegevens gemachtigde personen.
  - Instructieplicht van verantwoordelijke richting bewerker en Informatieplicht van bewerker richting verantwoordelijke
  - Na afloop overeenkomst wissen/teruggave van alle persoonsgegevens aan de verantwoordelijke, tenzij er een plicht tot opslag bestaat;

Aanpassingen op hoofdlijnen 2

- **Onderaannemer van verwerker en hoofdelijke aansprakelijkheid**
  - AVG: derde alleen inschakelen met schriftelijke toestemming van de verantwoordelijke.
  - Als bewerker dit niet doet is deze aansprakelijk voor alle schade die daardoor ontstaat (deze hoofdelijke aansprakelijkheid is een noviteit).

- **Data sharing**
  - Als de bewerker zelf ook een doel heeft voor de verwerking van persoonsgegevens, dan zijn ze beiden verantwoordelijk en is een bewerkersovereenkomst niet nodig.
  - Betrokkene moet wel toestemming geven verwerking van zijn gegevens voor meerdere doelen.

- **Register**
  - Verantwoordelijke is verplicht om een verwerkingenregister bij te houden waarin is opgenomen welke bewerkers worden ingeschakeld en waarvoor.

En dan de boetes….

- **Op basis AVG kan AP stevige boetes opleggen.**
- **Zware overtredingen (20 miljoen € of 4% van de omzet):**
  - Overtreden AVG basisbeginselen (voorwaarden voor vragen van toestemming en overtreden van de verplichtingen m.b.t. rechten van betrokkenen (dataportabiliteit, recht van verzet).
- **Lichte overtredingen (10 miljoen € of 2% van de omzet)**
  - Voor niet of te weinig implementeren van privacy beschermende maatregelen en voor het inschakelen van een verwerker zonder de wettelijke verplichtingen voor een verwerkersovereenkomst.
- **Gaan die boetes echt uitgedeeld worden?**
  - Ja als we de AP mogen geloven (bevoegdheid en waarschuwing)
- **Lopen zorginstellingen straks het meeste risico?**
  - Kans is redelijk groot, meeste klachten personen bij AP hebben betrekking op de zorg.

Dus zet alles op alles om tijdig aan de AVG te voldoen.

Welke partijen waren bij de BOZ verwerkingsovereenkomst betrokken?

actiz
organisatie van zorgondernemers

NFU
NEDERLANDSE FEDERATIE VAN UNIVERSITAIR MEDISCHE CENTRA

vgn vereniging gehandicaptenzorg nederland

GGZNEDERLAND

NVZ Nederlandse Vereniging van Ziekenhuizen

boz Brancheorganisaties Zorg

Team van juristen en (ICT) beleidsadviseurs

Wanneer toepassen?

- Als bijlage bij iedere bestaande of nieuw af te sluiten overeenkomst waarbij een derde in opdracht van de zorgorganisatie persoonsgegevens verwerkt

- De modelovereenkomst kan een integraal onderdeel uitmaken van de set Inkoopvoorwaarden Zorg (AIVG)

AIVG: artikel 19 Bescherming van persoonsgegevens

- In artikel 19.2 is beschreven:
  - *'Leverancier zal, indien in het kader van de uitvoering van de Overeenkomt persoonsgegevens bewerkt (waaronder ingezien) worden, een bewerkersovereenkomst sluiten met instelling'.*
- *Bij overeenkomsten op basis waarbij de AIVG, is dit de kapstok om een (in AVG) termen een verwerkingsovereenkomst aan te gaan.*
- *Dit artikel geeft helaas geen duidelijkheid wie de te sluiten verwerkingsovereenkomst, aanbiedt Leverancier of Instelling*

Dit gegeven is een bron van discussie tussen Leverancier en Instelling(en)

Wanneer niet aangaan?

- Verwerker (ontvanger van gegevens) kan zelf ook als verantwoordelijke worden aangemerkt
  - Samenwerkingsverbanden
  - Als betrokken partij een eigen relatie met betrokkene heeft (toestemming heeft van betrokkene voor verwerking)

- Er is een gezamenlijke verantwoordelijkheid (meerdere verwerkingsverantwoordelijken voor verwerking)

Bijlage 1: bij welke overeenkomst is deze verwerkersovereenkomst een bijlage?

Ingangs datum contract	Kenmerk / nummer / titel contract	Korte omschrijving diensten	Aard van de verwerking	Soort Persoons-gegevens	Categorieën van betrokkenen	Doeleinden van de verwerking	Goed-gekeurde sub verwerkers	Afspraken bewaar - termijnen
[invullen]	[invullen]	Bijv. levering en hosting EPD/ECD	Bijv. Verwerking patient gegevens,	Bijv. NAW gegevens, medische gegevens, financiële gegevens, etc.	Bijv. Patiënten, familieleden, personeels-leden	Bijv. Verlenen en organiseren van zorg, interne bedrijfsvoering doeleinden, etc	-	
[invullen]	[invullen]	Levering, onderhoud en hosting van verzuim applicatie / ERP	Verwerking verzuim, planning en financiële gegevens	NAW, medische gegevens, gegevens omtrent verzuim, gegevens omtrent aanwezigheid	Personeels-leden	Uitvoering geven aan wettelijke verplichtingen rondom re-integratie en verzuim, berekening management informatie		
….	….	…	…	…	…	…	…	

Bijlage 2 en 3 verwerkingsovereenkomst

- **Bijlage 2: concretisering veiligheidsmaatregelen**
  - Denk hierbij verder dan alleen aan anonimiseren en pseudonimiseren

- **Bijlage 3: Specificatie tarieven**
  - Wat mag verwerker in rekening brengen voor uitvoering geven aan verwerkersovereenkomst?
  - In aantal gevallen wordt dit aangegrepen om nodige (ondoorzichtige) hoge kosten in rekening te brengen.

Bijlage 4: Aanpassingen

- Bij voorkeur geen aanpassingen aan de tekst, uitgezonderd bijlagen 1, 2 en 3 die per overeenkomst specifieke invulling behoeven

- Mochten als resultaat van onderhandelingen toch wijzigingen in de tekst nodig zijn dan kunnen die in Bijlage 4 beschreven worden onder opgaven van artikelnummer, betreffende standaardtekst die vervalt, de vervangende tekst en de reden voor de wijziging

Bijlage 4: veel voorkomende wijziging

Artikel 8 Aansprakelijkheid

- Beperking aansprakelijkheid in de Overeenkomst is ook van toepassing op de Verwerkersovereenkomst.

- **Uitgesloten zijn uitsluitingen van aansprakelijkheid voor:**
  - Verlies en/of verminking van persoonsgegevens
  - Boetes (bijv. AP) die rechtstreeks verband houden met een toerekenbare tekortkoming, gedraging, nalaten van verwerker

- **Maximering bedragen in geval van verwijtbaar handelen**
  - Veelal gekoppeld aan een te verzekeren bedrag door verwerker

Issues 1

- **Wel of niet verwerker van persoonsgegevens?**
  - Aantal EPD/ECD leveranciers beschouwen zich ten onrechte niet als verwerker, terwijl ze wel in kader van onderhoud en ontwikkeling – in op opdracht van de instelling – bij persoonsgegevens kunnen

- **Leverancier wil alleen eigen verwerkingsovereenkomst tekenen**
  - Vanuit koepelorganisaties wordt leden dringend afgeraden akkoord te gaan met de door leveranciers zelf opgestelde verwerkingsovereenkomsten en maar één model aan te houden, de BOZ verwerkingsovereenkomst

Issues 2

- Als software, waarmee persoonsgegevens wordt verwerkt, intern (on premiss) is geïnstalleerd, maar door een derde wordt beheerd, *is dan een wel of niet een verwerkersovereenkomst vereist?*

- Er is sprake van een Acceptatie & Productieomgeving van een EPD (met persoonsgegevens) bij de instelling, maar een Ontwikkel en/of Testomgevingen hiervan bij de leverancier met daarin (test) persoonsgegevens. W*anneer is hier wel en wanneer niet een verwerkersovereenkomst noodzakelijk?*

Issues 3:

- U slaat sec persoonsgegevens op in de cloud zonder verdere bewerker; *is een verwerkersovereenkomst hier vereist?*

- Een zorginstelling is de verantwoordelijke voor de verwerking van persoonsgegevens inzake bijv. de gezondheid van betrokkenen, maar besteed de verwerking ervan uit aan collega zorginstelling; *is een bewerkersovereenkomst dan noodzakelijk?*

Issues 4:

- Een instelling voor Beschermd / Begeleid Wonen (RIBW) moet persoonsgegevens van cliënten (zoals BSN) leveren aan de gemeente in kader van de WMO bekostiging; *moet de instelling een bewerkersovereenkomst sluiten met de gemeente?*

- U werkt met een aanbieder van 'Cloud' diensten voor het beheer van uw hosted mailboxen; *moet u een bewerkersovereenkomst sluiten?*

- Als een derde uw nieuwsbrieven rondstuurt op basis van van uw klantenbestanden; *moet u een bewerkersovereenkomst sluiten?*

Ten slotte

- Begin 2019 verschijnt een nieuwe versie als daar aanleiding toe is
- In BOZ verband is er een werkgroep AVG die de vinger aan de pols houdt
- De documenten zijn te vinden op de website van de VGN (http://legacy.vgn.nl/media/5a2ff2163071 4/Toelichting+BOZ+model+verwerkersovereenkomst+121217.pdf)

Contactgegevens

Jos Schimmelpennink
NVZ-Ziekenhuizen
J.Schimmelpennink@NVZ-ziekenhuizen.nl
Tel. 06-30387227