Docnr4

From: 5.1.2.e <5.1.2.e @actiz.nl>
Date: Thursday, December 4, 2025, 9:21 AM
To: 5.1.2.e @eerstekamer.nl" <5.1.2.e @eerstekamer.nl>
CC: postbus@eerstekamer.nl" <postbus@eerstekamer.nl>
5.1.2.e <5.1.2.e @brancheorganisatieszorg.nl>
Subject: Brief van de Brancheorganisaties zorg (BoZ) betreffende de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

Attachments:

251203 - VWS - UAVG.pdf

Geachte 5.1.2.e beste 5.1.2.e

Graag deel ik hierbij de brief die de Brancheorganisaties Zorg (BoZ) gisteren met het ministerie van VWS hebben gedeeld. We sturen deze brief graag mee ten behoeve van de tweede vragenronde over de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

In de brief uiten wij onze zorgen over het voorgenomen artikel 23a van de UAVG, onderdeel van de Verzamelwet Gegevensverwerking, die momenteel ter behandeling ligt in de commissie voor Digitalisering (DIGI).

Ons verzoek is om deze brief te delen met de commissie.

Alvast hartelijk dank.

Met vriendelijke groet,

5.1.2.e

Communicatie & Public Affairs adviseur

actiz
branchevereniging van zorgorganisaties
verpleeghuiszorg | zorg thuis | revalidatie en herstel | jeugd

5.1.2.e @actiz.nl | 5.1.2.e | Oudlaan 4, 3515 GA Utrecht | **www.actiz.nl**

Oudlaan 4
3515 GA Utrecht
Postbus 9696
3506 GR Utrecht
Telefoon (030) 273 97 26
www.brancheorganisatieszorg.nl
IBAN NL33 FVLB0699 1645 59

Ministerie van VWS
t.a.v. de 5.1.2.e DG Langdurige Zorg
t.a.v. 5.1.2.e DG Curatieve Zorg
Postbus 20350
2500 EJ Den Haag

per email: 5.1.2.e @minvws.nl
5.1.2.e @minvws.nl

Datum : 3 december 2025
Ons kenmerk : BoZ/251203
Betreft : Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

Geachte 5.1.2.e en 5.1.2.e

De brancheorganisaties in de zorgsector ActiZ, de Nederlandse ggz, NVZ, UMCNL en VGN verenigd in Brancheorganisaties Zorg (BoZ), vragen graag uw aandacht voor zorgen die wij hebben over het voorgenomen artikel 23a van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), onderdeel van de Verzamelwet Gegevensverwerking die thans ter behandeling voorligt bij de Eerste Kamer.

Wij onderschrijven volledig de intentie van de wetgever om de gevestigde praktijk voor de controle op de jaarrekening door accountants wettelijk goed te regelen. De huidige regeling laat echter vragen open over de grondslag voor zorgaanbieders voor de aanlevering van grote hoeveelheden gepseudonimiseerde persoonsgegevens en het verstrekken van inzage in brondocumenten bij de steekproef aan accountants.

Onze juridische analyse laat zien dat artikel 23a lid 2 in de voorgestelde vorm een juridische en praktische onmogelijkheid creëert. Na de behandeling van het wetsvoorstel in de Tweede Kamer waren wij verrast door de versnelde agendering van het wetsvoorstel in de Eerste Kamer. Vanwege de knelpunten die wij hebben geconstateerd en de impact ten aan zien van de uitvoering van het wetsvoorstel, willen wij u hierbij toch in dit late stadium onze zorgen overbrengen ten aanzien van de uitvoerbaarheid van het wetsvoorstel.

Ten eerste is het een probleem voor zorgaanbieders dat zij geen goedkeurende verklaring voor de jaarrekening kunnen ontvangen nu de accountants geen betrouwbare steekproef op het niveau van brondata kunnen uitvoeren ten gevolg van de verplichting om de data te pseudonimiseren.

Ten tweede: ook wanneer de wetgever zou regelen dat accountants via een sleutel toegang krijgen tot de brondata, blijft pseudonimiseren voor zorgaanbieders geen werkbare of wenselijke oplossing. Voor een wettelijke jaarrekeningcontrole moeten accountants namelijk niet alleen volledige toegang hebben tot de brondata, maar óók kunnen controleren hoe de sleutel tot stand is gekomen en of deze correct en volledig is toegepast. Een accountant moet kunnen vaststellen dat geen gegevens zijn weggevallen, aangepast of verkeerd gekoppeld. Dat vergt inzicht in de oorspronkelijke, niet-gepseudonimiseerde gegevens én in het pseudonimiseringsproces zelf. Daarmee ontstaat een fundamenteel probleem: zodra pseudonimiseren wordt verplicht, dreigt er een vicieuze cirkel ten aanzien van de accountantscontrole te ontstaan, omdat accountants hebben aangegeven toegang nodig te hebben tot bijzondere persoonsgegevens, inclusief brondocumenten, om hun wettelijke taak te kunnen uitvoeren
Daarnaast leidt pseudonimiseren door zorgaanbieders tot aanzienlijke én structurele problemen: complex sleutelbeheer, hoge technische en organisatorische lasten, een forse administratieve en personele belasting, en extra juridische risico's bij fouten of incidenten.

Om die reden moet pseudonimiseren in dit domein niet verplicht worden gesteld. Een andere oplossing is noodzakelijk, namelijk een wettelijke grondslag die accountants rechtstreeks toegang geeft tot de benodigde bijzondere persoonsgegevens voor de steekproef en de controle op brondocumenten. Om de veiligheid van de (bijzondere) persoonsgegevens te garanderen kan bijvoorbeeld worden voorgeschreven dat het inzien van brondata alleen op de locatie van de aanbieder mag plaatsvinden en dat deze gegevens bij de aanbieder blijven, zodat ze niet in het bezit van de accountant komen.

Wij verzoeken u daarom om artikel 23a te repareren middels een wijziging op het voorliggende wetsvoorstel (novelle), zodat gezamenlijk met alle betrokken partijen een werkbare oplossing kan worden ontwikkeld die zowel privacybescherming als controleerbaarheid waarborgt.
Voor de juridische en technische onderbouwing verwijzen wij naar de onderstaande bijlage, die onlosmakelijk met deze brief verbonden is.

Wij zijn uiteraard bereid onze analyse nader toe te lichten. Indien gewenst kan dit plaatsvinden in een breed overleg met onder andere de NBA, de Autoriteit Persoonsgegevens en, indien passend, de AFM, de NZa en de IGJ, zodat een gedragen en uitvoerbare oplossing kan worden vormgegeven.

Met vriendelijke groet,

5.1.2.e

5.1.2.e 5.1.2.e

voorzitter BoZ directeurenoverleg

Bijlage – Nadere toelichting op artikel 23a UAVG

1. Kern van het probleem
Artikel 23a lid 2 UAVG verplicht zorginstellingen om persoonsgegevens die onder het medisch beroepsgeheim vallen (artikel 7:457 BW) te pseudonimiseren voordat deze aan accountants worden verstrekt, en deze pseudonimisering continu te handhaven. Hierdoor ontstaat een wederzijdse onmogelijkheid:

1. Naleving door zorginstellingen verhindert accountants om hun wettelijke controle naar behoren uit te voeren.
2. Een volledige accountantscontrole vereist inzage in bronbestanden, wat volgens het artikel niet meer zou mogen.

2. Gevolgen voor accountantscontrole
In de huidige praktijk controleren accountants gepseudonimiseerde databestanden, maar zij moeten ter verificatie altijd ook een steekproef uitvoeren op bronbestanden. Zonder die mogelijkheid ontstaat:

1. Geen volledige ketencontrole (verwijzing → indicatie → registratie → declaratie).
2. Geen zekerheid dat pseudonimisatie correct is toegepast.
3. Geen verificatie dat verwijzing, indicatie en zorglevering dezelfde persoon betreffen.

Dit maakt het onmogelijk voor accountants om een goedkeurende verklaring te geven.

3. Juridische en operationele gevolgen voor zorgaanbieders
Zorgaanbieders worden door artikel 23a geconfronteerd met:

a. Juridische classificatieproblemen
Zorginstellingen moeten per document bepalen of het onder het medisch beroepsgeheim valt. Dit is vaak niet eenduidig, bijvoorbeeld bij:

- CIZ-indicaties: administratieve én medische informatie.
- DBC-codes: financiële codes met diagnose-inhoud.
- Verwijsbrieven: combinatie van medische en administratieve gegevens.

b. Technische en organisatorische complexiteit
Correcte pseudonimisering vereist onder andere:

- Consistente pseudoniemen over alle documenten en systemen;
- Strikt gescheiden sleutelbeheer;
- DPIA's, logging en audittrails en
- Continue beoordeling van herleidbaarheidsrisico's.

Veel instellingen beschikken niet over de benodigde IT-systemen, expertise of capaciteit en zijn bovendien afhankelijk van hun ECD-leveranciers om consistente, veilige en juridisch correcte pseudonimiseringsfunctionaliteit te kunnen uitvoeren.

Een zorgaanbieder kan de data nooit volledig pseudonimiseren zolang de accountant toegang tot de brondata nodig heeft voor de controle. Als de wetgever het gebruik van een sleutel voorschrijft om terug te keren naar de brondata, ontstaan nieuwe problemen: beheer van sleutels, extra technische complexiteit, juridische aansprakelijkheid en aanzienlijke administratieve lasten. Hierdoor is uitvoering in de praktijk niet haalbaar.

c. Disproportionele verantwoordelijkheid en risico's
Zorginstellingen zouden volledige verantwoordelijkheid (en daaruit voortkomende aansprakelijkheid) dragen voor een foutloze toepassing van pseudonimisering en de garantie dat herleidbaarheid in de toekomst uitgesloten blijft.

d. Cumulatieve administratieve last en kosten
Per accountantscontrole moeten instellingen onder meer:

- Tientallen tot honderden documenten classificeren;
- Pseudonimisering implementeren en controleren en
- Veel extra documentatie en afstemming uitvoeren.

Een voorzichtige geschatte impact bedraagt 80 – 150 uur extra werk en tussen de 8 en 15 k extra kosten per controle. Sectorbreed komt dat neer op €32 tot 60 miljoen extra kosten per jaar.

4. Maatschappelijke gevolgen
Wanneer accountants geen goedkeurende verklaringen meer kunnen afgeven, ontstaan voor zorginstellingen:

- Problemen met financiers en toezichthouders;
- Reputatie- en continuïteitsrisico's en
- Onzekerheid over rechtmatigheid van zorguitgaven.

Daarmee komt de verlening van zorg en de bredere publieke verantwoording over circa €115 miljard zorguitgaven onder druk te staan.

Conclusie
Artikel 23a UAVG creëert een juridisch en praktisch onuitvoerbare verplichting die zowel de accountantscontrole als de bedrijfsvoering van zorgaanbieders ernstig belemmert. Reparatie en
een wijziging op het voorliggende wetsvoorstel (novelle) zijn nodig zodat gezamenlijk met alle betrokken partijen een werkbare oplossing kan worden ontwikkeld.

Accountants zijn reeds gebonden aan strikte geheimhoudingsplichten, beroepsethische regels en AVG-verplichtingen; vraag is dan ook welke meerwaarde het beoogde artikel brengt. Het creëren van een wettelijke grondslag voor accountants zonder dat aanbieders een verplichting krijgen om te pseudonimiseren lijkt de aangewezen oplossing.