

Inhoud

1. Anonimisering en pseudonimisering van cliëntgegevens bij AI-gebruik in Europa	2
2. AVG-verplichtingen en interpretatie.....	4
3. Nationale richtlijnen	5
3.1 België: AI-gebruik zonder pseudonimisering is verboden	5
3.2 Duitsland: volledige anonimisering vereist vóór AI-toepassing	6
3.3 Frankrijk: pseudonimisering en encryptie verplicht.....	8
4. De medische sector: Handreiking Anonimiseren (2019)	10
5. Slotconclusie en de situatie in Nederland.....	12

1. Anonimisering en pseudonimisering van cliëntgegevens bij AI-gebruik in Europa

Rechtspraak van het Hof van Justitie van de EU als kader

Op 4 september 2025 wees het Hof van Justitie van de EU een belangrijk arrest in de zaak *EDPS v. Single Resolution Board* (C-413/23 P). Daarin verduidelijkte het Hof de verhouding tussen pseudonimisering, anonimisering en de toepasselijkheid van de AVG.

Hoewel dit arrest formeel betrekking had op Verordening (EU) 2018/1725, die specifiek geldt voor de verwerking van persoonsgegevens door EU-instellingen en agentschappen, is de redenering van het Hof breder toepasbaar. In de rechtspraak wordt deze lijn ook onder de AVG (Verordening (EU) 2016/679) aangehouden. Voor advocaten betekent dit dat het arrest richtinggevend is voor de beoordeling van pseudonimisering en anonimisering in de context van het beroepsgeheim en cliëntgegevens.

Het Hof stelde expliciet dat gepseudonimiseerde gegevens niet automatisch en onder alle omstandigheden persoonsgegevens blijven:

“pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data ... in so far as pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject.” (par. 86)

Interpretatie: Het Hof legt de nadruk op de context. Voor advocaten betekent dit dat wanneer juridische e-items in gepseudonimiseerde vorm worden ingezet in AI-tools, telkens moet worden beoordeeld of de ontvanger redelijkerwijs over middelen beschikt om her identificatie mogelijk te maken.

Verder benadrukt het Hof dat deze beoordeling **plaatsvindt vanuit het perspectief van de verwerkingsverantwoordelijke**:

“the identifiability of the data subject must be assessed at the time of collection of the data and from the point of view of the controller.”

Dit legt de verantwoordelijkheid bij het advocatenkantoor dat gegevens verwerkt en deelt. Achteraf verwijzen naar de leverancier volstaat niet.

Tot slot onderstreept het Hof dat ook de **informatie- en transparantieplicht** blijft bestaan, zelfs wanneer de ontvanger de data mogelijk niet langer als persoonsgegevens beschouwt:

“the obligation to provide information ... prior to the transfer of the data at issue and irrespective of whether or not those data were personal data, from the third party recipient’s point of view after any potential pseudonymization.”

Gevolg voor de advocatuur: Alleen volledige anonimisering brengt gegevens definitief buiten de reikwijdte van de AVG. Pseudonimisering kan soms voldoende zijn, maar alleen wanneer de kans op her identificatie uitgesloten is en de verantwoordelijke dit kan aantonen.

2. AVG-verplichtingen en interpretatie

De Europese privacyverordening AVG (Verordening (EU) 2016/679) bevat geen expliciete bepalingen over kunstmatige intelligentie. Dit komt doordat de verordening in 2016 werd opgesteld, toen AI nog geen rol speelde.

Toch hebben toezichthouders en beroepsorganisaties in verschillende lidstaten geconcludeerd dat de beginselen van de AVG volledig van toepassing zijn op AI-gebruik in de advocatuur. Juridische documenten bevatten vrijwel altijd bijzondere persoonsgegevens, zoals medische gegevens, strafbare feiten of gevoelige familiegegevens. Zonder anonimisering of pseudonimisering zou invoer in AI-systemen direct in strijd zijn met de AVG.

In de AVG zelf zijn de volgende bepalingen richtinggevend:

- **Overweging 28:** *verwerkingsverantwoordelijken moeten, indien mogelijk, pseudonimisering toepassen.*
- **Overweging 29:** *aanvullende gegevens moeten afzonderlijk worden opgeslagen en onderworpen zijn aan technische maatregelen.*
- **Artikel 4(5):** *pseudonimisering is het verwerken van persoonsgegevens op zo'n manier dat koppeling met een specifieke betrokkene alleen mogelijk is via aanvullende gegevens.*
- **Artikel 32:** *pseudonimisering en encryptie gelden als passende beveiligingsmaatregelen.*

Deze bepalingen vormden de basis voor nationale richtlijnen die verplichte anonimisering of pseudonimisering voorschrijven bij het gebruik van AI in de advocatuur.

3. Nationale richtlijnen

3.1 België: AI-gebruik zonder pseudonimisering is verboden

Richtlijnen OVB – 20 januari 2025, sectie 1.2 Gegevensbescherming en Beroepsgeheim

Pseudonimisering als basisregel

“De advocaat pseudonimiseert de persoonsgegevens.”

Alle persoonsgegevens moeten vooraf worden gepseudonimiseerd of, waar mogelijk, volledig geanonimiseerd voordat ze als input in een AI-tool worden gebruikt.

Verbod op invoer van ruwe persoonsgegevens

“De advocaat onthoudt zich van het invoeren van persoonsgegevens in prompts, input en/of andere documenten bij het gebruik van AI-tools.”

Het is uitdrukkelijk verboden om namen, adressen of andere herleidbare persoonsgegevens rechtstreeks in een AI-tool in te voeren.

Uitzondering: wanneer verwerking noodzakelijk is

“In het geval de verwerking van persoonsgegevens essentieel is, is de advocaat transparant en vraagt hij toestemming aan de betrokken persoon.”

Indien verwerking onvermijdelijk is, moet de advocaat vooraf duidelijk communiceren en toestemming vragen. In uitzonderingsgevallen kan daarnaast ook een andere rechtsgrond gelden.

Deontologische verankering

Deze verplichtingen kaderen binnen de algemene deontologische kernplichten van de advocaat. Zoals vastgelegd in **art. 455 Ger.W.** en de **Codex Deontologie**, moet de advocaat handelen met waardigheid, onafhankelijkheid en partijdigheid. De advocaat blijft altijd eindverantwoordelijk voor de output van een AI-tool.

3.2 Duitsland: volledige anonimisering vereist vóór AI-toepassing

Standpunt van de BRAK over AI-tools en anonimisering van documenten

Bundesrechtsanwaltskammer (BRAK) – „Hinweise zum Einsatz von künstlicher Intelligenz (KI)“, december 2024

De BRAK publiceerde eind 2024 een leidraad met expliciete instructies voor advocaten over het gebruik van AI-tools bij het verwerken van documenten. De kern ligt bij verplichte anonimisering, bescherming van het beroepsgeheim en naleving van gegevensbescherming.

Verplichte anonimisering van documenten

„Soweit es erforderlich ist, Dokumente hochzuladen, sollten diese wenn möglich vorher vollständig anonymisiert sein.“

(BRAK-Leitfaden, p. 3, Abschnitt 3.1)

„Dabei reicht es regelmäßig nicht, Namen und Anschriften von Mandanten zu entfernen, wenn sich Mandatsinformationen aus dem Kontext ergeben können.“

(BRAK-Leitfaden, p. 4, Abschnitt 3.2)

Advocaten mogen uitsluitend geanonimiseerde documenten invoeren in AI-tools. Het verwijderen van alleen namen en adressen is onvoldoende als uit de context toch herleidbare informatie blijkt.

Beroepsgeheim en geheimhoudingsplicht

„Die anwaltliche Verschwiegenheit [...] muss auch beim Einsatz von KI und LLMs gewahrt bleiben.“

(BRAK-Leitfaden, p. 3, Abschnitt 3)

Alle informatie die een advocaat in het kader van een mandaat verkrijgt, inclusief de identiteit van de cliënt, valt onder de geheimhoudingsplicht (§ 43a Abs. 2 BRAO). Deze mag niet via AI worden gedeeld, tenzij aan de strikte voorwaarden van § 43e BRAO is voldaan.

Extra voorwaarden bij gebruik van externe AI-diensten

Wanneer externe AI-diensten of cloudoplossingen worden gebruikt, gelden aanvullende waarborgen:

„Falls möglich, müssen die Daten anonymisiert oder verschlüsselt werden.“

(BRAK-Leitfaden, p. 4, Abschnitt 3.2)

„Bei Cloud- und KI-Lösungen [...] sollte zumindest KI-Anbieter mit Serverstandorten in Deutschland oder Europa bevorzugt werden.“

(BRAK-Leitfaden, p. 4, Abschnitt 3.2)

Dit betekent dat aanbieders uit derde landen (zoals de VS, China of India) alleen met grote voorzichtigheid mogen worden gebruikt en bij voorkeur vermeden worden.

Strafrechtelijke consequenties

De geheimhoudingsplicht is niet alleen een tuchtrechtelijke en civielrechtelijke norm, maar kent ook een strafrechtelijke dimensie.

Volgens § 203 StGB is het ongeoorloofd openbaren van aan een advocaat toevertrouwde geheimen strafbaar. Onzorgvuldig gebruik van AI-tools waarbij mandaatsgegevens herkenbaar blijven, kan dus leiden tot strafrechtelijke vervolging, naast disciplinaire maatregelen.

Wettelijke basis

§ 43a Abs. 2 BRAO – Verschwiegenheitspflicht

§ 43e BRAO – Voorwaarden bij gebruik van IT-dienstverleners (incl. AI-aanbieders)

DSGVO (AVG) – Aanvullende regels inzake persoonsgegevensbescherming

Bronnen

Document: *Hinweise zum Einsatz von künstlicher Intelligenz (KI)*

Auteur: Rechtsanwalt Dr. Frank Remmert (BRAK)

Uitgave: Bundesrechtsanwaltskammer, december 2024

PDF: [BRAK-Leitfaden KI, december 2024](#)

3.3 Frankrijk: pseudonimisering en encryptie verplicht

Standpunt van de CNB over AI tools en anonimisering

Grille de lecture – Outils d’IA, juni 2025

“chiffrement, pseudonymisation et anonymisation des données personnelles, journalisation et traçabilité”

(Grille de lecture – Outils d’IA, p. 3, sectie RAG sécurisée)

“Les seules façons de garantir une étanchéité et une confidentialité totales pour les données du cabinet ‘injectées’ dans l’outil d’IA sont : l’anonymisation préalable des données”

(Grille de lecture – Outils d’IA, p. 11-12).

Hier wordt expliciet vermeld dat het verwerken van persoonsgegevens door AI-tools vereist dat deze pseudonimiseerd of geanonimiseerd worden als onderdeel van de technische maatregelen. De CNB geeft daarnaast aan dat volledige vertrouwelijkheid enkel kan worden gegarandeerd door voorafgaande anonimisering van gegevens

Artikelverwijzingen wetgeving

De CNB verwijst expliciet naar de toepasbaarheid van de Algemene Verordening Gegevensbescherming (AVG):

“article 28.1 du RGPD qui prévoit le recours uniquement à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées”

(Grille de lecture – Outils d’IA, p. 3–4).

Artikel 28.1 AVG vormt daarmee de juridische grondslag: advocaten en hun IT-leveranciers moeten aantonen dat er voldoende technische en organisatorische maatregelen zijn, waaronder pseudonimisering of anonimisering.

Bronverwijzingen

Thema: Pseudonimisering/nonimisering verplicht

“pseudonymisation et anonymisation des données personnelles” *(Grille de lecture – Outils d’IA, p. 3, sectie RAG sécurisée)*

Beveiligingsmaatregelen

“chiffrement pseudonymisation et anonymisation journalisation et traçabilité” *(ibid)*

“l’anonymisation des données des clients (...) suppression ou anonymisation automatique” *(ibid, p. 12-13)*

Wettelijke grondslag

“article 28.1 du RGPD qui prévoit le recours uniquement à des sous-traitants présentant des garanties” (*ibid*, p. 3–4)

Praktijkvoorbeelden

Doctrine (pseudonimisering), Juri’Predis (pseudonimisering), Jus Mundi (anonymisering) (*ibid*, p. 25 e.v.)

Bronvermelding

Document: *Grille de lecture – Outils d’IA*

Organisatie: Conseil National des Barreaux

Datum: juni 2025

Afdeling: RAG sécurisée en synthèse

Pagina’s: 3–4, 11–13, 25 e.v.

URL:

https://www.cnb.avocat.fr/sites/default/files/documents/CNB_Grille_evaluation_IA.pdf

4. De medische sector: Handreiking Anonimiseren (2019)

In mei 2019 verscheen de **Handreiking Anonimiseren** vanuit de Community van Data Experts Zorggegevens van het *Informatieberaad Zorg*. Deze handreiking wordt breed gezien als hét referentiedocument voor de omgang met zorggegevens in Nederland.

De handreiking definieert anonimisering als volgt:

“Anonimiseren is het proces waarbij persoonsgegevens onomkeerbaar worden veranderd, zodanig dat de betreffende persoon niet langer kan worden geïdentificeerd, direct of indirect.” (p. 5)

En verder:

“Alleen als het anonimiseren volledig en onomkeerbaar is uitgevoerd, vallen de gegevens buiten de reikwijdte van de AVG.” (p. 6)

Het enkele verwijderen van namen en adressen is niet voldoende:

“Ook indirecte identificatoren kunnen leiden tot herleidbaarheid.” (p. 8)

Juridisch kader en toepassingsbereik

De handreiking sluit direct aan bij de AVG en verduidelijkt de hoge lat voor anonimisering. Zij geldt voor **alle zorgpartijen** die medische gegevens verwerken: ziekenhuizen, huisartsen, specialisten, onderzoekers en ICT-afdelingen.

Link naar de handreiking: [Handreiking Anonimiseren – AVG-Helpdesk Zorg \(PDF\)](#)

Aanvullende noot: medische gegevens in de advocatuur

Wanneer advocaten dossiers behandelen waarin medische gegevens een rol spelen, bijvoorbeeld in letselschadezaken, arbeidsrecht of medische aansprakelijkheidskwesties, vallen zij onder een dubbele verplichting.

Enerzijds zijn medische gegevens volgens artikel 9 AVG *bijzondere persoonsgegevens*, waarvoor een verhoogde beschermingsdrempel geldt. Dit betekent dat verwerking alleen onder strikte voorwaarden is toegestaan, zoals met uitdrukkelijke toestemming of wanneer dit noodzakelijk is voor de instelling, uitoefening of onderbouwing van rechtsvorderingen. Daarnaast spelen ook sectorale normen uit de medische praktijk (zoals de KNMG-richtlijnen en de WGBO) een rol bij de bescherming van deze gegevens.

Anderzijds blijven voor advocaten hun eigen beroepsrechtelijke verplichtingen gelden, waaronder het beroepsgeheim (artikel 11a Advocatenwet en de Gedragsregels) en de verplichting om vertrouwelijke informatie zorgvuldig te behandelen.

Het verwerken van medische gegevens binnen AI-tools betekent dus dat advocaten **twee parallelle regimes** in acht moeten nemen: de strikte eisen uit de medische sector en de regels die voortvloeien uit de beroepsplichten binnen de advocatuur. Dit dubbele beschermingskader onderstreept dat bij medische gegevens een heldere richtlijn van de NOvA onmisbaar is, om te voorkomen dat advocaten onbewust het beroepsgeheim of de AVG schenden.

Conclusie voor de advocatuur: gebruik van medische gegevens in AI is alleen toegestaan buiten de AVG wanneer deze **onomkeerbaar geanonimiseerd** zijn. In alle andere gevallen blijven de AVG-verplichtingen en het beroepsgeheim gelden.

5. Slotconclusie en de situatie in Nederland

Europese kaders

De AVG noemt AI niet expliciet, omdat deze verordening in 2016 werd opgesteld, toen AI nog geen rol speelde in de juridische praktijk. Inmiddels hebben de rechtspraak van het Hof van Justitie van de EU en nationale richtlijnen dit hiaat ingevuld: verplichte anonimisering (of pseudonimisering indien niet herleidbaar) is noodzakelijk om de rechten van cliënten en het beroepsgeheim van advocaten te beschermen. Het arrest van het Hof van Justitie van 4 september 2025 bevestigt dit.

Situatie in Nederland

De Nederlandse Orde van Advocaten (NOvA) heeft echter nog geen richtlijn gepubliceerd over het gebruik van AI-tools. Daarmee loopt Nederland duidelijk achter op zowel de Europese rechtspraak als de richtlijnen van omliggende landen.

Risico van onomkeerbaar datadelen

Het ontbreken van duidelijke richtlijnen betekent dat advocaten nu mogelijk vertrouwelijke cliëntgevoelige gegevens in AI-tools invoeren, die geen anonimisering toepassen. Dit is een onomkeerbaar proces: eenmaal ingevoerde data kan niet meer worden verwijderd of teruggehaald. Het beroepsgeheim en de bescherming onder de AVG worden hierdoor blijvend aangetast.

Dubbele regimes bij medische dossiers

De risico's worden nog groter wanneer advocaten werken met medische gegevens. Deze vallen onder artikel 9 AVG als bijzondere persoonsgegevens en zijn dus extra beschermd, maar vallen óók onder de beroepsrechtelijke verplichtingen van advocaten zelf, waaronder het beroepsgeheim (artikel 11a Advocatenwet). Dit creëert een dubbele verplichting en maakt dat onzorgvuldig gebruik van AI in dit domein des te schadelijker is.

Oproep tot duidelijkheid

Juist nu AI steeds belangrijker wordt in de juridische praktijk, is snelle duidelijkheid noodzakelijk. Een formele richtlijn van de NOvA is onmisbaar om advocaten houvast te geven, dubbele regimes werkbaar te maken en onomkeerbaar verlies van vertrouwelijkheid te voorkomen. Alleen zo kan het vertrouwen in de advocatuur en de bescherming van cliëntgegevens in het AI-tijdperk worden gewaarborgd.