AP | bescherming in een digitale wereld

Gezondheidsgegevens in de cloud

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Inhoudsopgave

1. Inleiding

Heeft u gezondheidsgegevens[1] in de cloud ondergebracht? Of overweegt u dit te doen? Dan kunt u deze praktijkgids gebruiken om dit op een verantwoorde manier te doen.

De Autoriteit Persoonsgegevens (AP) heeft deze praktijkgids gemaakt omdat gezondheidsgegevens *bijzondere persoonsgegevens* zijn, waarmee u zeer zorgvuldig moet omgaan. Zulke gegevens zijn immers gevoeliger dan 'gewone' persoonsgegevens. Verwerkt u gezondheidsgegevens en bent u zorgaanbieder of zorgverlener, dan vallen ze bovendien onder het *medisch beroepsgeheim*. Het gebruiken van de cloud om gezondheidsgegevens in onder te brengen, brengt risico's met zich mee.

Een clouddienst kan voor u een goede oplossing zijn, maar is dus niet zonder risico's. In deze praktijkgids vindt u informatie over veelvoorkomende risico's en de afwegingen die u moet maken bij de keuze om gezondheidsgegevens[2] al dan niet in de cloud te verwerken.[3]

Risico's van gezondheidsgegevens in de cloud

- U merkt het mogelijk niet of pas te laat als informatie in verkeerde handen komt (datalek).
- De gezondheidsgegevens kunnen terechtkomen in een land waar de wettelijke bescherming van persoonsgegevens niet of onvoldoende is geregeld.
- De leverancier kan de gegevens voor eigen doeleinden (her)gebruiken zonder dat u hiervoor toestemming heeft gegeven.

2. Cloud

2.1 Wat is de 'cloud'?

De cloud, ofwel cloudcomputing, is het via een netwerk, zoals internet, aanbieden van *computing services*, zoals opslag, software, servers, databases, netwerk- en analysefuncties.[4] Deze diensten worden geleverd door een externe partij: de cloudprovider of leverancier.

Clouddiensten maken het mogelijk dat gegevens overal en altijd toegankelijk zijn, mits er een internetverbinding is. Ook is een clouddienst makkelijk op- en af te schalen, waardoor je snel over de benodigde capaciteit beschikt.

2.2 Soorten clouddiensten

Er zijn verschillende soorten clouddiensten. Sommigen zijn direct te gebruiken. Dit zijn 'kant en klare' producten, zoals de meeste elektronische patiëntendossiers (EPD's). Andere leveranciers bieden digitale omgevingen aan waarin u zelf applicaties kunt ontwikkelen.

Grofweg kunnen clouddiensten worden onderverdeeld in 'Software as a Service' (SaaS), 'Platform as a Service' (PaaS), en 'Infrastructure as a Service' (IaaS).

Software as a Service (SaaS)
U neemt een of meerdere applicatie(s) af via internet, meestal op basis van een abonnement. De leverancier is verantwoordelijk voor de ontwikkeling van de software, het beheer van de infrastructuur en (beveiligings)updates. Deze vorm van een clouddienst kunt u nagenoeg direct in gebruik nemen.[5] Vaak heeft u als afnemer weinig tot geen invloed op de functionaliteit van het afgenomen SaaS-product. In de zorg worden verschillende kwaliteits- en risicomanagementsystemen als een SaaS-product aangeboden. Verder kunt u denken aan leveranciers als Salesforce en SAP of producten als Google Docs en Microsoft Web Applicaties.[6]

Platform as a Service (PaaS)[7]
Als afnemer van een PaaS-oplossing krijgt u via de leverancier toegang tot ICT-infrastructuur en ondersteunende diensten, zoals servers, besturingssystemen, opslagcapaciteit, monitoringtools en ontwikkeltools. U heeft volledige controle over de functionaliteit van uw applicaties, maar u heeft mogelijk minder keuzevrijheid bij de hulpmiddelen die binnen het platform te gebruiken zijn, zoals ontwikkeltools. De PaaS-toepassingen in de zorg kunnen heel divers zijn. U kunt hierbij denken aan platforms voor telehealth[8] en verschillende zorgapplicaties.
Een bekende PaaS-leverancier is Google App Engine.

Voorbeelden van clouddiensten in de zorg

- Huisarts Jan maakt voor zijn patiënten gebruik van de persoonlijke gezondheidsomgeving (PGO) en een patiëntenportaal, waartoe hij toegang heeft via internet.
- Ziekenhuis X maakt gebruik van het elektronische patiëntendossier (EPD), waarin alle patiëntengegevens elektronisch worden vastgelegd en geraadpleegd. In de nachtdienst belt de verpleegkundige over een spoedgeval. De dienstdoende chirurg benadert vanuit huis het dossier van de desbetreffende patiënt.
- Verpleeghuizengroep Nightingale heeft een kwaliteits- en risicomanagementsysteem dat makkelijk via internet te benaderen is. Hierin melden de zorgverleners incidenten.

Infrastructure as a Service (IaaS)
Bij een IaaS-oplossing krijgt u via de leverancier alleen de ICT-infrastructuur, zoals servers, netwerken en opslagcapaciteit. U heeft de volledige vrijheid en verantwoordelijkheid om uw eigen systemen en diensten te ontwikkelen en beheren. Ook bent u vrij om zelf het besturingssysteem en de ontwikkeltools te kiezen. Een bekende IaaS-oplossing is Amazon Virtual Private Cloud.

Cloudmodellen
Er zijn verschillende cloudmodellen beschikbaar. Globaal kan er onderscheid worden gemaakt in een privaat,[9] publiek,[10] 'community'[11] en 'hybride' cloudmodel[12]. Ieder model kan in principe de verschillende soorten diensten aanbieden die eerder zijn beschreven.

2.3 Waarom is het belangrijk om te weten welke soort clouddienst u afneemt?

De soort clouddienst beïnvloedt de afwegingen over de bescherming van gezondheidsgegevens die u moet maken voordat u de dienst gaat gebruiken. Hoe meer taken u toevertrouwt aan de leverancier, hoe meer u er als verwerkingsverantwoordelijke[13] voor moet zorgen dat de leverancier deze taken in overeenstemming uitvoert met de relevante wet- en regelgeving en beveiligingsnormen. U kunt hierbij denken aan de gegevensbeschermingsaspecten vanuit de Algemene verordening gegevensbescherming (AVG), maar ook aan het benodigde niveau van beveiligingsmaatregelen om de gezondheidsgegevens te beschermen.

Het is aan u om van tevoren te verifiëren en documenteren dat de leverancier voldoende garanties biedt dat u als verwerkingsverantwoordelijke uw verplichtingen kunt nakomen op grond van de AVG én dat er afdoende bescherming is voor de gezondheidsgegevens die aan u zijn toevertrouwd.[14]

3. Verwerkingsverantwoordelijke en verwerker

Als u gezondheidsgegevens in de cloud onderbrengt, bent u in de termen van de AVG de *verwerkingsverantwoordelijke* en is de leverancier meestal een *verwerker*.[15] Omdat het begrippenpaar 'verwerkingsverantwoordelijke' en 'verwerker' een belangrijke rol speelt in de verhouding tussen u en de leverancier, lichten we deze begrippen hierna kort toe.

3.1 Verwerkings-verantwoordelijke

De AVG definieert de *verwerkingsverantwoordelijke* als: *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen."*[16]

De verwerkingsverantwoordelijke beslist aldus over bepaalde wezenlijke aspecten, oftewel het 'hoe' en het 'waarom' van de verwerking van persoonsgegevens.

Stelt meer dan een partij 'het doel van en de middelen voor' de verwerking van de gezondheidsgegevens vast? Dan is er sprake van gezamenlijke verwerkingsverantwoordelijkheid. Dit betekent dat u en de andere partij(en) op een transparante wijze onderlinge afspraken moeten maken waarin u de verantwoordelijkheden en verplichtingen onder de AVG vastlegt.[17]

Er is geen gezamenlijke verwerkingsverantwoordelijkheid voor een verwerking waar meerdere entiteiten gebruikmaken van een gedeelde database of een gemeenschappelijke infrastructuur waarbij elke entiteit zelfstandig eigen doelen vaststelt. Ook is er geen gezamenlijke verwerkingsverantwoordelijkheid als er een uitwisseling is van dezelfde gezondheidsgegevens of groep gegevens tussen twee of meer entiteiten zonder dat zij gezamenlijk 'doelen van' of 'middelen voor' de verwerking vaststellen. Dit is dan een uitwisseling van gegevens tussen afzonderlijke, 'zelfstandige' verwerkingsverantwoordelijken.

Voorbeeld

De cloud: Verwerker en verwerkersverantwoordelijke

Een leverancier biedt de mogelijkheid om grote hoeveelheden gezondheidsgegevens op te slaan. De SaaS-dienst is volledig gestandaardiseerd. Als afnemer van de dienst zijn er weinig mogelijkheden om de dienst aan te passen. Ook stelt de leverancier de voorwaarden op en zijn deze niet onderhandelbaar. Zorggroep X besluit een beroep te doen op de leverancier om de gezondheidsgegevens van cliënten op te slaan. De zorggroep is de verwerkingsverantwoordelijke, want deze bepaalt hoe de gegevens van cliënten worden verwerkt met de keuze voor een specifieke clouddienst. De leverancier is de verwerker, omdat deze de gezondheidsgegevens niet voor eigen doeleinden verwerkt en de gegevens uitsluitend opslaat namens en overeenkomstig de instructies van de zorggroep.

Voorbeeld

Onderzoeksproject onderzoeksinstellingen

"Verscheidene onderzoeksinstellingen besluiten deel te nemen aan een specifiek gezamenlijk onderzoeksproject en daartoe gebruik te maken van het bestaande platform van een van de bij het project betrokken instellingen. Elke instelling voert persoonsgegevens in het platform in die ze al in haar bezit heeft ten behoeve van het gezamenlijke gezondheidsonderzoek en gebruikt de door anderen via het platform verstrekte gegevens voor de uitvoering van het onderzoek. In dit geval worden alle instellingen aangemerkt als gezamenlijke verwerkingsverantwoordelijken voor de verwerking van persoonsgegevens die plaatsvindt door middel van het opslaan en bekendmaken van informatie uit dit platform, aangezien zij samen het doel van de verwerking en de te gebruiken middelen (het bestaande platform) hebben bepaald. Elke instelling is echter een afzonderlijke verwerkingsverantwoordelijke voor alle andere verwerkingen die voor hun respectieve doeleinden buiten het platform kunnen worden uitgevoerd."

Bron: EDPB Richtsnoeren 07/2020 over de begrippen verwerkingsverantwoordelijke en verwerker in de AVG, p. 26.

3.2 Verwerker

Bij de verwerking van persoonsgegevens kan de verwerkingsverantwoordelijke een verwerker inschakelen. De verwerker is volgens de AVG:

"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt". [18]

De verwerker is een aparte entiteit die los staat van de verwerkingsverantwoordelijke en die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke. Dat wil zeggen dat de verwerker uitsluitend persoonsgegevens verwerkt volgens de instructies[19] en onder de (uitdrukkelijke) verantwoordelijkheid van de verwerkingsverantwoordelijke. De verwerker mag aldus de persoonsgegevens niet op een andere manier verwerken dan volgens de instructies van de verwerkingsverantwoordelijke. Ook mag de verwerker de persoonsgegevens niet voor eigen doeleinden verwerken.[20]

3.3 Subverwerkers

Bij gebruik van clouddiensten wordt de dienstverlening soms uitgevoerd door een keten van verwerkers: de verwerker, die namens u gezondheidsgegevens verwerkt, laat (een deel van) de gezondheidsgegevens verwerken door een of meerdere derde partijen. Die derde partijen noemen we subverwerkers.[21] De leverancier mag alleen een andere partij inschakelen om namens u (een deel van) de gezondheidsgegevens te verwerken als u hiervoor toestemming heeft gegeven.[22] De toestemming kan specifiek of algemeen zijn, waarbij u het recht behoudt om bezwaar te maken tegen het inschakelen van nieuwe subverwerkers. U kunt de toestemming opnemen in de overeenkomst of andere rechtshandeling tussen u en de verwerker.[23] Wees u ervan bewust dat u als verwerkingsverantwoordelijke in zo'n geval verantwoordelijk blijft voor de gehele keten van verwerkers.[24]

3.4 Waar moet u rekening mee houden bij het kiezen van een leverancier?

Bij het kiezen van een leverancier is het belangrijk om bewust te zijn van de kwalificaties van een verwerker en verwerkingsverantwoordelijke. Meestal is het aan te raden om een leverancier in te schakelen die namens u en uitsluitend onder uw instructies de gezondheidsgegevens verwerkt in de rol van verwerker.[25] Voor u als verwerkingsverantwoordelijke geldt de plicht om uitsluitend een beroep te doen op verwerkers die afdoende garanties bieden dat zij passende technische en organisatorische maatregelen nemen om de gezondheidsgegevens te beschermen.[26] Ook moet de verwerker de

bescherming van de rechten van betrokkenen[27] waarborgen.[28] Aldus bent u verantwoordelijk voor het beoordelen van de toereikendheid van de door de verwerker geboden garanties. Ook bent u verplicht om de toereikendheid van de geboden garanties aan te tonen.[29]

De volgende elementen kunnen u helpen bij de beoordeling van de naleving van de AVG door de leverancier:

- privacybeleid;
- dienstverleningsvoorwaarden;
- het verwerkingsregister;
- het informatieveiligheidsbeleid;
- het beleid voor gegevensbeheer;
- verslagen van externe privacyaudits;
- verslagen van externe informatiebeveiligingsaudits;
- erkende en up-to-date relevante certificeringen, zoals NEN:7510 en ISO-certificeringen.[30]

Voor het beantwoorden van de vraag of de geboden garanties van de verwerker afdoende zijn, geldt een zekere risicobeoordeling. Die hangt af van de soort verwerkingen van gezondheidsgegevens die u aan de verwerker toevertrouwt. Deze risicobeoordeling moet u per geval uitvoeren. Hierbij moet u rekening houden met de aard, reikwijdte, context en doeleinden van de verwerking van gezondheidsgegevens, en met de risico's voor de rechten en fundamentele vrijheden van natuurlijke personen.

Voor u, als verwerkingsverantwoordelijke, kunnen de deskundigheid, betrouwbaarheid, middelen en reputatie van de verwerker op de markt van betekenis zijn.

De verplichting dat de verwerker afdoende garanties moet bieden, is een doorlopende verplichting. Dat betekent dat u als verwerkingsverantwoordelijke met passende tussenpozen de garanties van de verwerker moet verifiëren door bijvoorbeeld audits en inspecties te (laten) verrichten.[31] In hoofdstuk 4 wordt dieper ingegaan op de aspecten van gegevensbescherming die relevant zijn voor gezondheidsgegevens in de cloud en de relatie met de leverancier.

4. Welke aspecten van gegevensbescherming zijn in het bijzonder belangrijk als u overweegt uw gezondheidsgegevens in de cloud onder te brengen?

De gegevensbeschermingswetgeving is technologieneutraal opgesteld. Hierdoor heeft u de vrijheid om een service van een leverancier aan te schaffen die voldoet aan uw verwachtingen. Deze verwachtingen moeten wel voldoen aan de geldende wet- en regelgeving voor de bescherming van bijzondere persoonsgegevens, waaronder gezondheidsgegevens.

4.1 Identificeer uw verwerkingen

Om de gezondheidsgegevens rechtmatig te mogen verwerken, is het belangrijk om eerst te identificeren:

1. welke persoonsgegevens u verwerkt;
2. voor welke doeleinden;
3. onder welke grondslag en uitzonderingsgrond;[32]
4. hoe u de persoonsgegevens verwerkt.

Heeft u dit in kaart gebracht? Dan kunt u beoordelen of uw verwerkingsactiviteiten in overeenstemming zijn met de AVG of dat u de verwerking moet aanpassen. Deze beoordeling moet u vastleggen.[33]

4.2 Beoordeel de risico's van de verwerking

Pas wanneer u uw verwerkingsactiviteiten in kaart heeft gebracht, kunt u de risico's van de verwerking beoordelen voor de rechten en vrijheden van de betrokkenen. Om deze risico's af te wenden of te verminderen, moet u passende technische en organisatorische maatregelen treffen. Zodat de verwerking voldoet aan de AVG.[34]

U moet de risico's beoordelen van alle aspecten van de beoogde verwerking, niet alleen de risico's voor de beveiliging van de verwerking. Als de verwerking (deels) plaatsvindt in de cloud, moet u de cloud ook in uw beoordeling meenemen.[35] Het is daarbij belangrijk om u te realiseren dat clouddiensten vaak als gestandaardiseerde oplossing worden aangeboden. U heeft daarbij geen of weinig mogelijkheden om als verwerkingsverantwoordelijke de dienst of de applicaties aan te passen aan uw eigen vereisten.[36] Dit betekent dat er op basis van uw risicoanalyse clouddiensten kunnen zijn waarvan u zich moet afmelden als u geen technische maatregelen kunt implementeren die u noodzakelijk acht om te kunnen voldoen aan de eisen uit de AVG en sectorale wet- en regelgeving. Dit is meestal zo bij SaaS-oplossingen, omdat de controle over de oplossing daar bij de leverancier ligt. Maar dit kan ook zo zijn bij PaaS- en IaaS-oplossingen.[37]

Bij clouddiensten is het belangrijk om onder andere, alleen of in samenwerking met de leverancier, het volgende in overweging te nemen:

- Verwerkt de leverancier aanvullende persoonsgegevens? Anders dan de verwerking van de gezondheidsgegevens die u aan de leverancier heeft uitbesteed? Bijvoorbeeld metadata[38] of andere servicegegevens? Dan moet u beoordelen of dit een

geoorloofde verwerking is en wie hiervoor de verwerkingsverantwoordelijke is.
- Verwerkt de leverancier de gezondheidsgegevens ook voor eigen doeleinden? Dan handelt de leverancier in strijd met de AVG. De leverancier is dan de verwerkingsverantwoordelijke voor die verwerking.[39] U moet vervolgens beoordelen of u de persoonsgegevens nog aan de leverancier mag verstrekken. En zo ja, of deze verstrekking voldoet aan de beginselen voor de verwerking van persoonsgegevens,[40] inclusief de rechtmatigheid van de verwerking.

4.3 Beoordeel de beveiligingsrisico's van de verwerking

U moet voor elke verwerkingsactiviteit een passend niveau van beveiliging vaststellen.[41] Dit doet u zo mogelijk samen met uw leverancier. Om een passend beveiligingsniveau vast te stellen voor de verwerking en dit te handhaven, moet u de risico's beoordelen voor de rechten en vrijheden van de betrokkenen.[42]

Een risicobeoordeling is essentieel om afdoende beveiligingsmaatregelen te definiëren die u van de leverancier moet eisen bij de verwerking van gezondheidsgegevens. Hiervoor kunt u gebruikmaken van verschillende risicobeoordelingsmethodes.[43]

Bij clouddiensten is het belangrijk om in ieder geval rekening te houden met de volgende risico's, die in het bijzonder relevant zijn bij de bescherming van de gezondheidsgegevens:
- Verlies van controle over de verwerking van de gezondheidsgegevens.
- Technologische afhankelijkheid van de leverancier. Een voorbeeld hiervan is de onmogelijkheid om de oplossing te veranderen zonder gegevensverlies.
- Dat de gegevens die worden gehost op een virtueel systeem[44] worden gewijzigd of toegankelijk worden voor onbevoegde derden na een fout van de leverancier of slechte uitvoering van de toezichtrol door de leverancier.
- Verzoek tot toegang tot of afgifte van de gezondheidsgegevens door autoriteiten van derde landen.[45]
- Het niet nakomen van de schriftelijke afspraken en instructies van u als verwerkingsverantwoordelijke of het niet (volledig) nakomen van de relevante wet- en regelgeving, in het bijzonder de AVG, in de keten van subverwerkers.
- Onvoldoende of niet-vertrouwde manier van vernietiging van de gegevens, of een te lange bewaartermijn voor de gezondheidsgegevens.
- Problemen bij de rechten van betrokkenen omdat de leverancier ontoereikende maatregelen heeft geïmplementeerd.
- Onbeschikbaarheid van de dienst en van de toegangsmiddelen tot de dienst, bijvoorbeeld door netwerkproblemen.[46]
- Faillissement van de leverancier, beëindiging van de dienst of overname van de dienst door een derde partij.[47]
- Niet-naleving van de wet- en regelgeving, in het bijzonder van de AVG, zoals de regels voor internationale doorgifte van persoonsgegevens (hoofdstuk V van de AVG).

Maak vooraf afspraken met de leverancier om ervoor te zorgen dat u toegang houdt tot de persoonsgegevens wanneer de leverancier wordt overgenomen of failliet gaat. Leg dat vast in een verwerkersovereenkomst.

Afhankelijk van het model clouddienst dat u afneemt, heeft in de praktijk vaak de leverancier een bepaald niveau van beveiliging voor de verwerking vastgesteld. Uw taak als verwerkingsverantwoordelijke is daarom:
- Het niveau van beveiliging identificeren en beoordelen of dit passend is voor de verwerking van gezondheidsgegevens. Dit kunt u onder andere doen door de documentatie van de leverancier te beoordelen en, indien relevant, informatie op te halen via een gesprek met de leverancier.
- De beveiligingsmaatregelen verifiëren en uw beoordeling van deze maatregelen documenteren.

Is er sprake van een grootschalige verwerking van gezondheidsgegevens? En bent u van mening dat aanvullende maatregelen noodzakelijk zijn, buiten de maatregelen die de leverancier heeft geïmplementeerd? Dan moet u ervoor zorgen dat u het recht (en de mogelijkheid) heeft om aanvullende beveiligings-maatregelen te implementeren, op grond van uw overeenkomst of andere bindende rechtshandeling met de leverancier.

4.4 Verricht onderzoek naar de leverancier

Als verwerkingsverantwoordelijke heeft u de vrijheid om een leverancier te kiezen voor de verwerking van persoonsgegevens. Wel moet u een leverancier kiezen die voldoende garanties biedt dat deze zich houdt aan de wet- en regelgeving waaraan u gebonden bent. Dit betekent dat u voorafgaand aan het inschakelen van een leverancier voldoende onderzoek moet verrichten.

Algemene aandachtspunten:

- *Vendor lock-in*[48] en mogelijke uitdagingen bij het zoeken naar alternatieve leveranciers als een exit noodzakelijk is.[49]
- De mogelijkheden voor audits en toezicht op de leverancier.
- Transparantie over de inzet van onderaanbieders en de locatie van de gegevens.[50]
- Fysieke en regiospecifieke risico's, zoals de politieke stabiliteit van het land waar de diensten worden geleverd en/of de gegevens worden opgeslagen. Hierbij is ook belangrijk of de gegevens onder de reikwijdte vallen van wet- en regelgeving die:
  - de toegang tot de dienst en/of persoonsgegevens kan beperken;
  - anderzijds risico's oplevert voor de rechten en fundamentele vrijheden van betrokkenen;
  - het beschermingsniveau aantasten van de persoonsgegevens, waardoor de bescherming niet gelijkwaardig is aan het niveau van bescherming van persoonsgegevens in de Europese Economische Ruimte (EER).[51]
- Risico van een aanzienlijke kwaliteitsdaling of prijsstijging van de af te nemen dienst.
- Risico's van een *multi-tenant* omgeving.[52]

Enkele specifieke vragen over gegevensbescherming die u hierbij kunnen helpen:

- Verwerkt de leverancier alleen persoonsgegevens volgens uw gedocumenteerde/schriftelijke instructies? Of behoudt de leverancier zich het recht voor om deze persoonsgegevens ook voor eigen doeleinden te verwerken?[53]
- Heeft de leverancier beleid en procedures om ervoor te zorgen dat de medewerkers gebonden zijn aan geheimhouding? En kan de leverancier de naleving van deze verplichting aantonen?[54]
- Heeft de leverancier, rekening houdend met de rolverdeling van verwerkingsverantwoordelijke en verwerker, een passend niveau van beveiliging van de verwerking vastgesteld[55] voor de verwerkings-activiteiten die u aan de leverancier gaat toevertrouwen?[56] En is dat beveiligingsniveau voldoende voor u?
- Heeft de leverancier procedures om te waarborgen dat subverwerkers voldoen aan de gegevens-beschermingseisen die door u aan de leverancier zijn opgelegd? En omvatten deze procedures ook het verstrekken van de benodigde documentatie aan u als verwerkingsverantwoordelijke?[57]
- Bevat de procedure een termijn voor het indienen van de documentatie over de screening van subverwerkers door de leverancier? En komt deze termijn overeen met de termijn waarbinnen de leverancier u als verwerkingsverantwoordelijke moet informeren over het inzetten van nieuwe subverwerkers of wijziging van de subverwerkers?[58]
- Worden de afspraken in de verwerkersovereenkomst of andere rechtshandeling die u met de leverancier aangaat in zijn geheel doorgezet naar de subverwerker(s)?[59] Wat is het beleid van de leverancier hiervoor?[60]
- Heeft de leverancier op voorhand al een lijst met subverwerkers die de leverancier inzet voor het aanbieden van de clouddienst inclusief in welke landen deze subverwerkers zich bevinden? En uit welke landen de leverancier en deze subverwerkers toegang kunnen krijgen tot de persoonsgegevens?
- Is er sprake van een doorgifte van persoonsgegevens door u en/of door de leverancier naar een land buiten de EER? En zo ja, van welk doorgifte-instrument wordt gebruikgemaakt? En welke aanvullende maatregelen worden getroffen om de persoonsgegevens te beschermen?[61]

- Heeft de leverancier beleid en procedures om u te ondersteunen bij het afhandelen van verzoeken van betrokkenen (zie hoofdstuk III van de AVG)?[62]
- Heeft de leverancier beleid en procedures voor het omgaan met datalekken in de zin van de AVG? En omvatten deze procedures verplichtingen voor de leverancier om mee te werken als u een datalek moet melden bij de AP en/of aan betrokkenen?[63]
- Kan de leverancier de persoonsgegevens onherroepelijk wissen of retourneren aan het einde van of bij beëindiging van een verwerking?[64]
- Heeft de leverancier beleid en procedures waarin staat dat de leverancier verplicht is om mee te werken aan audits en inspecties die u initieert als verwerkingsverantwoordelijke? En ook als een onafhankelijke, externe auditor dit doet?

4.5 Sluit een (verwerkers) overeenkomst af

De rechtsverhouding tussen verwerkingsverantwoordelijke en verwerker moet worden geregeld in een overeenkomst. Dit kan een zogeheten verwerkersovereenkomst zijn of een andere rechtshandeling, zoals voorgeschreven in artikel 28 lid 3 van de AVG. Die overeenkomst of rechtshandeling wordt in schriftelijke vorm (inclusief digitaal) opgesteld en moet bindend zijn voor de verwerker ten opzichte van de verwerkingsverantwoordelijke.[65] In deze overeenkomst of andere rechtshandeling worden de verplichtingen en verantwoordelijkheden van de partijen opgenomen bij de betreffende verwerking van persoonsgegevens. Het ontbreken van de schriftelijke overeenkomst of andere toepasselijke rechtshandeling is een inbreuk op de AVG.[66]

De inhoud van de overeenkomst of andere bindende rechtshandeling moet **ten minste** de volgende elementen bevatten:[67]

- Het **onderwerp van de verwerking** van de gezondheidsgegevens. Dit moet u met voldoende specificaties opnemen, zodat duidelijk is wat het belangrijkste onderwerp van de verwerking is.
- De **duur van de verwerking**. Dit kan ofwel de exacte periode zijn, ofwel een specificatie van de criteria die u gebruikt om de duur van de verwerking te bepalen.
- De **aard van de verwerking**. Dit zijn de handelingen die voor de verwerking worden verricht, zoals het archiveren van persoonsgegevens. Afhankelijk van de specifieke verwerkingsactiviteit moet de beschrijving zo gespecificeerd en volledig mogelijk zijn.
- Het **doel van de verwerking**. Dit is het specifieke doel dat u nastreeft met de verwerking van de gezondheidsgegevens. Vanuit het beginsel van doelbinding mag u alleen persoonsgegevens verwerken voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.[68]
- Het **soort persoonsgegevens**. Dit moet u gedetailleerd vermelden. Het is niet genoeg als er in de overeenkomst of andere rechtshandeling alleen 'gezondheidsgegevens in de zin van artikel 4(7) en artikel 9 van de AVG' staat. U moet op zijn minst duidelijk maken om welke soorten gezondheidsgegevens het gaat.
- De **categorieën van betrokkenen**. Dit moet u specifiek vermelden. Bijvoorbeeld 'patiënten' of 'cliënten'.
- De **verplichtingen en de rechten van de verwerkingsverantwoordelijke** en de **verplichtingen van de verwerker** ten opzichte van de verwerkingsverantwoordelijke.
- Afhankelijk van de context en de risico's van de verwerking kunt u andere relevante informatie opnemen en eventuele andere aanvullende toepasselijke vereisten.[69]

In de AVG staan de eisen en uitgangspunten waaraan verwerkers moeten voldoen. Dat helpt u om de samenwerking met de cloudaanbieder goed in te richten.

Bij de cloud kunt u ook denken aan het maken van afspraken, al dan niet in de vorm van een schriftelijke (verwerkers)overeenkomst, over:

- continuïteit van bedrijfsvoering, back-up en datareplicatie, (wijzigingen in) de dienstverlening (inclusief kwaliteit), toepassing van encryptie,[70] en infrastructuurbeveiliging;[71]
- specifieke beveiligingsmaatregelen, zoals *cloud identity and access management*;
- de inzet van verwerkers en subverwerkers, inclusief afspraken over partijen die zich buiten de EER bevinden;
- het standaard periodiek aanleveren van een kopie van de persoonsgegevens en metadata (en andere relevante data);
- de exitmogelijkheid van de cloud;[72]
- audits en inspecties van de leverancier en mogelijke subverwerkers.[73]

Het is belangrijk dat u als verwerkingsverantwoordelijke, op basis van de overeenkomst of andere bindende rechtshandeling met de leverancier, in staat wordt gesteld om:

- de verwerkingen inclusief de datastromen te verantwoorden;
- een beoordeling te maken dat de leverancier de verwerking uitvoert in overeenstemming met de AVG en andere relevante sectorale wet- en regelgeving in de gezondheidszorg;
- transparantie te bieden over de verwerkingsactiviteiten die namens u worden verricht en de condities waaronder de verwerkingen plaatsvinden;
- audits en inspecties uit te voeren om de compliance te toetsen en mogelijke afwijkingen van de overeenkomst en/of overtredingen van de AVG te detecteren en hier opvolging aan te geven.

4.6 Exitmogelijkheid van de cloud

Een externe clouddienst biedt voordelen vergeleken met systemen die zelf on-premise[74] worden beheerd. Dit gaat echter gepaard met een vergroot risico op afhankelijkheid van de clouddienst in de bedrijfsprocessen. Het is daarom belangrijk om grip te houden op deze afhankelijkheid. Dit doet u door vóór het aangaan van de overeenkomst met de leverancier na te denken over in hoeverre u in uw bedrijfsprocessen afhankelijk wilt zijn van een externe partij én over welke redenen voor u de beëindiging van de clouddienst zouden rechtvaardigen.[75]

Recht om de overeenkomst te beëindigen

Het is belangrijk dat u in de overeenkomst met de leverancier mogelijke redenen opneemt voor beëindiging van de overeenkomst.[76] Hierbij kunt u denken aan:

- aanhoudend ontoereikende prestaties van de leverancier;
- aanzienlijk verlies van service;
- ernstige schendingen van contractuele voorwaarden of van toepasselijke EER-wet- en regelgeving, zoals de AVG en de NIS2-richtlijn;
- buitensporige kosten bij de contractuele afspraken, die u aan de leverancier kunt toeschrijven;
- relocatie van de leverancier(s) of datacenters;
- signalen dat de leverancier mogelijk in financieel zwaar weer verkeert;
- een fusie met een andere partij of overname van de leverancier door een andere partij;
- een wezenlijke wijziging in de onderaannemers;
- verplaatsing van het hoofdkantoor van de leverancier naar een (andere) jurisdictie buiten de EER;
- een wezenlijke wijziging in het sociale, politieke of economische klimaat die invloed heeft op de aangeboden dienst door de leverancier;
- een wijziging in de wet- en regelgeving die van invloed is op de uitbestedingsovereenkomst;
- een wijziging in de wet- en regelgeving die van invloed is op de locatie van de gegevens en de verwerking van gegevens;
- wezenlijke wijzigingen in het beheer van (cyber) beveiligingsrisico's in de keten van onderaannemers;
- het niet succesvol uitvoeren van testmigraties door de cloudleverancier op de overeengekomen tijdstippen.

Exitplan

Het is belangrijk dat u een exitplan opstelt dat u in staat stelt om snel te reageren als dat nodig is.[77] Neem in uw plan in ieder geval kritieke mijlpalen op, een beschrijving van taken en vaardigheden die nodig zijn om de exit uit te voeren, een ruwe inschatting van de tijd en de daarmee gepaard gaande kosten. Hiervoor is het ook essentieel dat u een goed beeld heeft van de partij die de dienstverlening kan overnemen. Kunt u dat zelf of is daarvoor een andere leverancier voorhanden die tijdig in actie kan komen? Een goed exitplan bevat ook een versneld implementatieplan bij de nieuwe leverancier of uw eigen organisatie.

U moet de inhoud van het exitplan periodiek toetsen op actuele ontwikkelingen, zoals nieuwe diensten die u afneemt bij de leverancier, of nieuwe standaarddataformaten die gangbaar zijn geworden, waardoor u de data in een ander format moet aanleveren. Naast de inhoud van het exitplan moet u de werking ervan periodiek testen, zodat u er zeker van bent dat procedures voldoen en het plan (technisch) uitvoerbaar is zodra u ervoor kiest om de dienstverlening te beëindigen.

Bovendien kunt u in uw afspraken met de leverancier over het exitplan rekening houden met:

- de verantwoordelijkheden van iedere partij (rol en verwachtingen);
- indien van toepassing: de wijziging en/of loskoppeling van koppelingen met allerlei systemen;
- de teruglevering van persoonsgegevens en metadata (en andere relevante data) en/of onherroepelijke verwijdering van de persoonsgegevens;
- de ondersteuning (inclusief de termijn of periode hiervan) door de leverancier bij beëindiging van de overeenkomst;
- indien wenselijk: een boeteclausule wanneer de leverancier niet meewerkt aan het vooraf afgesproken exitplan;
- de opzegtermijn;

- afspraken over intellectueel eigendom zoals het beschikbaar krijgen van de broncode met maatwerk voor uw organisatie;
- voortgezet gebruik na het einde van de overeenkomst zodat de periode wordt overbrugd tussen de oude en de nieuwe leverancier;
- mogelijke kosten van een cloud-exit;
- indien relevant: vastlegging van een escrow-regeling,[78] zodat de leverancier meewerkt.[79]

4.7 Audits en inspecties bij de verwerker en subverwerker(s)

Als verwerkingsverantwoordelijke bent u verplicht om verwerkers te auditen en/of inspecties te verrichten, om ervoor te zorgen dat de leverancier zich bij het verwerken van de gezondheidsgegevens houdt aan de AVG en aan de specifieke afspraken die u met de leverancier heeft gemaakt. Is er een subverwerker, dan kunt u de audit en/of inspectie bij de subverwerker laten verrichten door de verwerker (namens u)[80] of door een derde partij (auditor). Dit hangt af van de specifieke afspraken die u hierover heeft gemaakt.

Het is vaak lastig om vooraf aan te geven hoe intensief en frequent u een audit/inspectie gaat verrichten bij de verwerker. Uitgangspunt is: hoe hoger het risico van de verwerking door de verwerker, hoe hoger de eisen aan de audit/inspectie.

De beoordeling van het risico moet gaan over de risico's voor de betrokkenen, zoals de cliënten, patiënten, etc. De vragen die u hierbij in ieder geval moet stellen:

1. Wat is de kans dat er iets misgaat?
2. Wat zijn de gevolgen voor de betrokkenen als er daadwerkelijk iets misgaat?

Belangrijke factoren die de intensiteit van de audit/inspectie (mede)bepalen:

3. Het volume aan (bijzondere) persoonsgegevens. Hoe meer persoonsgegevens de verwerker verwerkt, hoe strenger de vereisten bij een audit/inspectie.
4. Hoe gevoelig of vertrouwelijk zijn de gegevens? Worden de gezondheidsgegevens bijvoorbeeld door het beroepsgeheim beschermd?[81]

Belangrijke factor die de frequentie van de audit/inspectie (mede)bepaalt:

5. Het risico van de verwerking van gezondheidsgegevens voor de rechten en fundamentele vrijheden van de betrokkenen. Uitgangspunt is: hoe kritieker de verwerking is voor de betrokkenen (hoe groter het risico), hoe vaker u de verwerkingen moet controleren.

Let op!

Het verwerken van gezondheidsgegevens levert vanwege de aard van de persoonsgegevens een groter risico op voor de rechten en fundamentele vrijheden van personen en vergt daarom een hoger beschermingsniveau.[82] Aldus vereist dit frequentere controles op de verwerkingen dan bij 'gewone' persoonsgegevens. Ook moet u zowel bij het treffen van beschermingsmaatregelen als bij de controle op de verwerkingen via audits/inspecties rekening houden met gezondheidsgegevens die door het (medisch) beroepsgeheim worden beschermd.

Voorbeelden van factoren die impact hebben op de frequentie van de audits/inspecties bepalen

- Onvoldoende transparantie over de getroffen technische en organisatorische beveiligingsmaatregelen, de inzet van subverwerkers en/of de opvolging van de instructies van de verwerkersverantwoordelijke.
- De ervaringen met de cloudaanbieder, waaruit blijkt dat de aanbieder afspraken niet of niet volledig nakomt.
- Het is bekend dat de cloudaanbieder ernstige beveiligingsincidenten (inclusief datalekken) heeft meegemaakt.
- Subverwerkers worden vaak vervangen.
- Er vinden overnames, fusies of andere significante veranderingen bij de cloudaanbieder plaats.

N.B. Bij deze voorbeelden wordt verondersteld dat deze ontwikkelingen plaatsvinden na het afsluiten van de overeenkomst met de leverancier. Is op voorhand duidelijk dat de leverancier onvoldoende transparantie biedt, afspraken niet nakomt of ernstige, verwijtbare

beveiligingsincidenten heeft meegemaakt? Dan is dit immers voldoende aanleiding om de leverancier niet in te zetten, gelet op artikel 28 lid 1 AVG.

Leveranciers en hun eigen auditrapporten
Doorgaans hebben leveranciers als onderdeel van hun informatieveiligheidsbeleid procedures voor het uitvoeren van audits. Vaak heeft de leverancier het verrichten van audits uitbesteed aan een onafhankelijke derde partij die ook auditrapporten afgeeft. U kunt de auditrapporten opvragen als onderdeel van de controle op de naleving van de AVG en andere relevante wet- en regelgeving en van de afspraken die u heeft gemaakt in de overeenkomst of andere geldige rechtshandeling. Hierbij is het belangrijk dat u aandacht besteedt aan de reikwijdte van de auditrapporten en aan de vraag of deze rapporten de verwerkingsactiviteiten dekken die u heeft uitbesteed aan de leverancier.

Als de reikwijdte van de rapporten de verwerkingsactiviteiten niet dekt, dan kunt u op basis van uw overeenkomst of andere bindende rechtshandeling ervoor zorgen dat u het recht heeft om een audit met een andere reikwijdte uit te voeren bij de leverancier.

Let op!
De eigen auditrapporten van cloudleveranciers vervangen niet uw recht om als verwerkingsverantwoordelijke zelf audits (inclusief inspecties) te (laten) verrichten bij de cloudleverancier.[83]

4.8 Speciale regels voor gebruik van de cloud buiten de EER

Cloudtechnologieën beperken zich vaak niet tot landsgrenzen. Dit betekent dat ook wet- en regelgeving in het digitale domein grensoverschrijdend kan zijn. Het verwerken van gezondheidsgegevens in de cloud kan hierdoor onder de werking vallen van verschillende wet- en regelgeving die met elkaar in conflict is of elkaar doorbreekt.[84] Daarnaast veranderen de geopolitieke verhoudingen in een rap tempo. Hierdoor kunnen leveranciers die niet alleen onder de reikwijdte van de EER-wet- en regelgeving en jurisdictie vallen, verplichtingen hebben naar derde landen (landen buiten de EER) en politieke leiding daar. Dit maakt het bieden van het op grond van de AVG vereiste, gelijkwaardige beschermingsniveau voor bijzondere persoonsgegevens, zoals gezondheidsgegevens, erg lastig.[85] Het is belangrijk dat u vanwege deze risico's genoeg onderzoek doet naar passende cloudleveranciers. En dat u overweegt om de aan u toevertrouwde gezondheidsgegevens slechts te laten verwerken door leveranciers die alleen onder de EER-wet- en regelgeving en jurisdictie vallen. Dit ook met oog op de doelstellingen van de Cyberbeveiligingswet. Zie hierover meer in hoofdstuk 5.

Als verwerkingsverantwoordelijke moet u **zeggenschap** hebben over, **invloed** hebben op en **regie** hebben over de verwerking van gezondheidsgegevens in de cloud. Volgens de AVG bent u verantwoordelijk voor de gezondheidsgegevensverwerkingen in de keten van (sub)verwerkers, inclusief de verwerkingen die plaatsvinden in de cloud.[86] U bent het immers die kiest voor een specifieke leverancier aan wie u de gezondheidsgegevens toevertrouwt om deze namens u te verwerken. Wanneer de gegevensverwerkingen (deels) onder een andere jurisdictie vallen verliest u (een mate van) zeggenschap over, invloed op en regie over deze gegevens. Dat heeft gevolgen voor de rechten en fundamentele vrijheden van de betrokkenen. Met dit risico moet u rekening houden bij onder andere uw risicoanalyse,[87] contractuele afspraken,[88] exitstrategie en -plan,[89] beveiligingsmaatregelen en uw keuze voor de soort cloud en het soort cloudmodel.[90] U moet dit risico opnieuw beoordelen bij elke wijziging die het beschermingsniveau voor de rechten van betrokkenen nadelig beïnvloedt. U moet risico in ieder geval jaarlijks beoordelen.

Daarnaast heeft de AVG specifieke regels waaraan u moet voldoen als de gezondheidsgegevens in een cloud **buiten de EER** worden opgeslagen. Er is dan sprake van een 'doorgifte' zoals bedoeld in artikel 44 AVG. Ook bij het inzetten van verwerkers en subverwerkers in een derde land is er sprake van een doorgifte. Bovendien is er sprake van een doorgifte als een autoriteit in een derde land toegang krijgt tot de gezondheidsgegevens.[91]

Is er sprake van een doorgifte, dan wordt van u als verwerkingsverantwoordelijke verwacht dat u in ieder geval:

1. De doorgiften naar derde landen identificeert.
2. De wenselijkheid van de doorgiften naar de specifieke derde landen beoordeelt en deze documenteert.
3. De relevante grondslag voor de doorgifte identificeert voor de verwerking van gezondheidsgegevens (hoofdstuk V van de AVG).
4. Indien van toepassing: evalueert of het doorgifte-instrument van artikel 46 AVG waarop u of de (sub) verwerker vertrouwt, effectief is gezien alle

omstandigheden van de doorgifte.[92] En als dit niet zo is, dat u aanvullende maatregelen identificeert en deze maatregelen neemt of laat nemen door de (sub)verwerker.[93]

5. Regelmatig de doorgifte evalueert en de uitkomsten van de evaluatie vastlegt.

Verder is het belangrijk dat u de volgende informatie van de leverancier krijgt en deze gebruikt bij uw risicobeoordeling:

6. Transparante en volledige informatie van de landen waarin de datacenters zich bevinden en waar de gezondheidsgegevens zullen worden verwerkt.
7. Duidelijkheid over de voornemens van de leverancier om subverwerkers in te zetten die zich in derde landen bevinden (of hun datacenters).
8. Duidelijkheid over welke grondslag(en) uit hoofdstuk V van de AVG wordt gebruikt en welke garanties er worden geboden om adequate bescherming te bieden als de gezondheidsgegevens buiten de EER worden verwerkt.
9. Informatie over de ervaringen van de leverancier met verzoeken van autoriteiten van derde landen.[94]
10. Informatie over de exitmogelijkheden bij een beëindiging van de overeenkomst of stopzetting van mogelijke doorgiften.[95]

De AP adviseert dat u in beginsel een leverancier inschakelt die niet onder de wet- en regelgeving van een derde land valt waardoor de rechten en fundamentele vrijheden van betrokkenen worden ondermijnd. Bovendien beveelt de AP aan dat de verwerking van gezondheidsgegevens zich beperkt tot locaties binnen de EER.

5. Hoe beïnvloeden de NEN 7510 en de NIS2-richtlijn de verwerking van gezondheids-gegevens in de cloud?

De NEN 7510 is een norm voor informatiebeveiliging in de Nederlandse zorgsector[96] en de NIS2-richtlijn is een Europese richtlijn die organisaties op het gebied van informatiebeveiliging reguleert.[97]

5.1 Wat is de NEN 7510?

De NEN 7510 is gebaseerd op de ISO/IEC 27001/2 en biedt richtlijnen voor het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van medische en persoonlijke gegevens. Met de herziening van de NEN 7510 is de norm afgestemd op de Europese wetgeving waaronder de NIS2- richtlijn.[98]

De norm is niet altijd wettelijk verplicht, maar kan via wet- en regelgeving,[99] sectorafspraken en onderzoeken wel verplicht worden gesteld. De Inspectie Gezondheids-zorg en Jeugd (IGJ) verwacht bijvoorbeeld dat alle zorgaanbieders[100] aantoonbaar voldoen aan de NEN 7510.[101]

5.2 De NEN 7510 en de cloud

De NEN 7510:2024 bevat informatiebeveiligingsrichtlijnen voor het gebruik van clouddiensten geformuleerd vanuit het oogpunt van de afnemer.[102] Verder wordt er verwezen naar de ISO/TS 23535 en ISO/TR 21332, waarin zorg-specifieke informatie wordt gegeven over de beveiliging van en privacy bij binnen de gezondheidszorg gebruikte clouddiensten. Deze richtlijnen komen op hoofdlijnen overeen met de punten beschreven in hoofdstuk 4 van deze handreiking. De handreiking is echter toegespitst op de afnemer: een verwerkingsverantwoordelijke met AVG-verplichtingen, die gezondheidsgegevens laat verwerken door een cloudleverancier.

5.3 Wat is de NIS2-richtlijn?

De NIS2-richtlijn is eind 2022 vastgesteld door de Europese Unie (EU) en reguleert bedrijven en overheden op het gebied van cyber- en informatiebeveiliging. De richtlijn is gericht op het verbeteren van de cyberbeveiliging en de weerbaarheid van essentiële diensten in de EU-lidstaten. Deze richtlijn is noodzakelijk door de afhankelijkheid van digitalisering en de toegenomen dreigingen. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet (Cbw).[103] Om onder de Cbw te vallen moet een organisatie voldoen aan zowel de sectorcriteria als aan de groottecriteria. Uitzondering hierop is een aanwijzing bij besluit of regeling van de minister.[104]

De organisaties die onder de Cbw vallen zijn organisaties die actief zijn in de 'zeer kritieke' en 'andere kritieke' sectoren.[105] De gezondheidszorg valt onder de kwalificatie 'zeer kritieke sector'. De Cbw is van toepassing op verschillende soorten zorgentiteiten, waaronder:

- zorgaanbieders;
- EU- referentielaboratoria;
- entiteiten die onderzoeks- en ontwikkelings-activiteiten uitvoeren met betrekking tot geneesmiddelen;
- vervaardigers van farmaceutische basisproducten en farmaceutische bereidingen; en
- vervaardigers van medische hulpmiddelen.[106]

TABEL 1

Essentiële entiteiten	Belangrijke entiteiten
Organisaties met meer dan 250 fte; of	Organisaties met minimaal 50 fte; of
Organisaties met een jaaromzet van meer dan 50 miljoen euro, en een balanstotaal van meer dan 43 miljoen euro.	Organisaties met een jaaromzet van meer dan 10 miljoen euro (en minder dan 50 miljoen euro), en een balanstotaal van meer dan 10 miljoen euro (en minder dan 43 miljoen euro).

De cloud valt onder de categorie 'digitale infrastructuur'. Daarmee valt de cloud, net zoals de gezondheidszorg, onder de 'zeer kritieke sector' en is daarmee een essentiële entiteit.[107]

Organisaties uit deze sectoren moeten aan de Cbw voldoen als zij minimaal 50 fte in dienst hebben. Als dit niet het geval is, moet de organisatie zowel een jaaromzet hebben van meer dan 10 miljoen euro als een balanstotaal van meer dan 10 miljoen euro om onder de Cbw vallen.[108] Als de organisatie aan deze ondergrens voldoet, wordt op basis van de grootte van de organisatie een entiteit als 'essentiële entiteit' of 'belangrijke entiteit' gekwalificeerd. Zie tabel 1.

Los van de organisaties die vallen onder de 'zeer kritieke' of 'andere kritieke sectoren', zijn er natuurlijk ook andere organisaties die gezondheidsgegevens verwerken in de cloud. Het is daarom belangrijk om eerst te bepalen of uw organisatie onder de Cbw valt.[109] Het kan namelijk voorkomen dat uw organisatie niet wordt gekwalificeerd als een entiteit die onder een van deze sectoren valt. Dit betekent dat u niet aan de aanvullende eisen hoeft te voldoen van de Cbw. U moet dan wél nog steeds aantoonbaar voldoen aan de informatiebeveiligingseisen die gelden voor het verwerken van gezondheidsgegevens, oftewel de NEN 7510 en de AVG.

5.4 Wat betekent het voor mijn organisatie als deze onder een 'zeer kritieke sector' of 'andere kritieke sector' valt?

Als uw organisatie onder de Cbw valt, gelden de verplichtingen die voortvloeien uit de Cbw. Uw organisatie moet onder andere voldoen aan de zorgplicht, meldplicht en registratieplicht. Belangrijk om te weten is dat er toezicht wordt gehouden op organisaties die onder de Cbw vallen.

Zorgplicht

De Cbw schrijft zorgplichtmaatregelen voor waaraan organisaties in ieder geval moeten voldoen, naast de aanvullende normen en kaders die gelden voor specifieke sectoren, zoals de gezondheidszorg. De zorgplicht vergt van uw organisatie dat uw informatiebeveiliging aantoonbaar op orde is, zowel qua technische als organisatorische maatregelen.[110] Volgens de Cbw moet u ten minste deze maatregelen nemen: [111]

1. Maak voor uw organisatie een risicoanalyse om de cyberweerbaarheid te verbeteren.[112]
2. Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer.[113]
3. Stel een bedrijfscontinuïteitsplan op.[114]
4. Richt een *incident response* in.[115]
5. Stel de cyberhygiëne op orde.[116]
6. Stel schriftelijk beleid op voor de beveiliging van netwerk- en informatiesystemen.[117]
7. Zorg voor een veilige toeleveringsketen.[118]
8. Stel beleid en procedures vast voor het gebruik van cryptografie en encryptie.[119]
9. Implementeer het gebruik van MFA of andere beveiligde authenticatieoplossingen.[120]
10. Beoordeel de effectiviteit van de maatregelen voor het beheer van cyberbeveiligingsrisico's aan de hand van beleid en procedures.[121]

Het Nationaal Cyber Security Centrum (NCSC) heeft een infosheet over de zorgplicht gepubliceerd die u verder kan ondersteunen bij het treffen van bovenstaande maatregelen.[122]

Meldplicht

Organisaties die onder de Cbw vallen, moeten bij elk significant incident[123] **een vroegtijdige waarschuwing geven**[124] aan het Computer Security Incident Response Team (CSIRT)[125] en de bevoegde toezichthouder. De melding moet **onverwijld** of, als dat niet mogelijk is, **binnen 24 uur** na kennisname van het significante incident. De toezichthouder voor de gezondheidszorg is de IGJ. De Rijksinspectie Digitale Infrastructuur[126] houdt toezicht op de essentiële leveranciers van cloudvoorzieningen.

De 'essentiële entiteit' of 'belangrijke entiteit' zoals bedoeld onder de Cbw, moet **onverwijld** of, als dat niet mogelijk is, **binnen 72 uur** na kennisname van het significante incident een (vervolg)melding doen bij het CSIRT en de bevoegde toezichthouder.[127]

De melding bestaat uit verschillende fasen:

1. Een vroegtijdige waarschuwing over het significante incident aan het CSIRT en de toezichthoudende instantie.[128]
2. Een update van de vroegtijdige waarschuwing, een initiële beoordeling van het significante incident, de ernst en de gevolgen ervan, en indien beschikbaar, de indicatoren voor aantasting.[129]
3. Een tussentijds verslag, op verzoek van het CSIRT of de toezichthoudende instantie.[130]
4. Een eindverslag.[131]

Bij de (vroegtijdige) melding is het belangrijk om in ieder geval informatie te verstrekken over:

1. de mogelijke oorzaken van het significante incident;[132]
2. de mogelijke grensoverschrijdende gevolgen;[133]
3. de contactgegevens van de functionaris die verantwoordelijk is voor de melding;[134]
4. aard en omvang van het incident;[135]
5. (vermoedelijke) datum en tijdstip van aanvang van het incident;[136]
6. de (vermoedelijke) ernst en gevolgen van het incident;[137]
7. indien mogelijk: de door uw organisatie genomen of te nemen (technische en organisatorische) maatregelen om de gevolgen van het incident te beperken en/of herhaling te voorkomen;[138]
8. andere gedetailleerde informatie over het incident (inclusief technische details).[139]

De meldplicht wordt gehandhaafd door de aangewezen toezichthouder. Deze kan controleren of een organisatie correct en op tijd een melding heeft gedaan, en of de organisatie adequaat op het incident heeft gereageerd. Het niet nakomen van de meldplicht kan leiden tot sancties en/of aanwijzingen.

Registratieplicht

Entiteiten die onder de categorie 'zeer kritieke' en 'andere kritieke' sector vallen, en voldoen aan de groottecriteria, moeten zich registreren in het entiteitenregister bij het NCSC. Dit register vergroot het zicht op de digitale weerbaarheid. De gegevens die worden gevraagd zijn enerzijds nodig om te kunnen bepalen of de organisatie 'NIS2-plichtig' is en anderzijds om de organisatie in het entiteitenregister op te nemen.

Er wordt om deze gegevens gevraagd:

1. KvK-nummer;
2. bezoekadres (moet overeenkomen met de gegevens in het handelsregister);
3. correspondentieadres (moet overeenkomen met de gegevens in het handelsregister);
4. sector(en) waarin de organisatie actief is;
5. type NIS2-entiteit ('essentieel' of 'belangrijk');
6. indien van toepassing: het type aanwijzing van een departement of toezichthouder;
7. EU-lidstaat/-lidstaten waar de organisatie diensten/producten levert;
8. contactgegevens van de organisatie (naam contactpersoon, telefoonnummer, e-mailadres en functietitel);
9. aantal fte (<50, 50 -249 of >250);
10. jaaromzet voorgaand kalenderjaar (<10 miljoen euro, 10-50 miljoen euro of > 50 miljoen euro);
11. balanstotaal voorgaand kalenderjaar (<10 miljoen euro, 10-43 miljoen euro of >43 miljoen euro).

Naast deze gegevens wordt gevraagd om netwerkgegevens aan te leveren. Deze gegevens worden gebruikt voor monitoring en ondersteuning. De registratie kan afgerond worden als een van de onderstaande gegevens wordt opgegeven:

1. (publiek) IP-adres of reeks;
2. domeinna(a)m(en);
3. AS-nummer.[140]

Let op!

Is er in uw organisatie een significant incident[141] waarbij er ook een (ernstig) datalek[142] is? Dan moet u **ook** een melding bij de AP doen. Voor de melding bij de AP heeft u echter specifieke informatie nodig over de inbreuk op persoonsgegevens.[143] Als u een melding heeft gedaan onder de Cbw, dan kunt u (deels) de informatie van deze melding gebruiken voor de melding bij de AP. Vaak moet u deze informatie echter wel aanvullen. Dat komt door het verschil in de materie en reikwijdte tussen de Cbw- en de AVG-melding. Bovendien moet u het datalek mogelijk ook melden bij het individu waarvan de persoonsgegevens zijn gelekt.[144]

6. Begrippenlijst

Bijzondere persoonsgegevens	Gegevens als bedoeld in artikel 9 AVG, waaronder gegevens over gezondheid. Verwerking van deze gegevens is verboden, tenzij het verbod wordt opgeheven.
Cloud	Een gedeelde verzameling configureerbare computermiddelen (zoals netwerken, servers, opslag, toepassingen en diensten), toegankelijk via internet.
Datalek	'Inbreuk in verband met persoonsgegevens' (zoals bedoeld in artikel 4, onder 12, AVG): een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Leverancier	Aanbieder van clouddiensten.
Medisch beroepsgeheim	Geheimhoudingsplicht voor mensen die vanwege hun beroep met medische gegevens werken. Zij mogen in principe geen gegevens van een patiënt aan anderen verstrekken. Voor zorgverleners zoals artsen, verpleegkundigen, psychotherapeuten en andere beroepen die vallen onder de Wet op de beroepen in de individuele gezondheidszorg (BIG) geldt het wettelijk geregeld medisch beroepsgeheim (artikel 88 Wet BIG, en bij een geneeskundige behandelingsovereenkomst ook artikel 7:457 BW). Voor sommige andere hulpverleners, zoals maatschappelijk werkers, geldt een geheimhoudingsplicht op grond van hun beroepscode. De medewerkers van de zorginstelling (zoals een ziekenhuis) waar iemand een behandeling ondergaat, zijn via hun arbeidscontract aan een geheimhoudingsplicht gebonden.
Patiëntgegevens	De gegevens opgenomen in het dossier als bedoeld in artikel 7:454 lid 1 BW.
Zorgaanbieder	Zorginstelling, zorgpraktijk of een zelfstandig werkende individuele zorgverlener (zie ook artikel 1 Wet kwaliteit, klachten en geschillen zorg).

7. Juridisch kader

7.1 Burgerlijk Wetboek

Artikel 7:454 lid 1
De hulpverlener richt een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is.

Artikel 7:457
Lid 1 Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.

Lid 2 Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.

Lid 3 Daaronder zijn evenmin begrepen degenen wier toestemming ter zake van de uitvoering van de behandelingsovereenkomst op grond van de artikelen 450 en 465 is vereist. Indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.

7.2 Wet Beroepen in de Individuele Gezondheidszorg

Artikel 88
Een ieder is verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of wat daarbij te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen.

7.3 Cyberbeveiligingswet

Artikel 2 Doel van deze wet
Deze wet is, met het oog op het in stand houden van kritieke maatschappelijke of economisch belangrijke functies of activiteiten, gericht op het verhogen van de cyberbeveiliging door regels te stellen ten aanzien van:

a. het beheersen van risico's voor de beveiliging van netwerk- en informatiesystemen;
b. het voorkomen van incidenten;
c. het beperken van gevolgen van incidenten; en
d. het verkrijgen en verstrekken van informatie over incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden.

Artikel 8 Essentiële entiteit van rechtswege
1. De volgende entiteiten zijn essentiële entiteiten:
   a. gekwalificeerde verleners van vertrouwensdiensten;
   b. aanbieders van registers voor topleveldomeinnamen;
   c. DNS-dienstverleners;
   d. aanbieders van openbare elektronische communicatienetwerken, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;
   e. aanbieders van openbare elektronische communicatiediensten, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;

f. andere entiteiten, genoemd in bijlage 1 van deze wet, die de in artikel 2, eerste lid, van de bijlage bij Aanbeveling 2003/361/EG bedoelde drempel voor middelgrote ondernemingen overschrijden;
g. de ministeries, met inbegrip van de daartoe behorende dienstonderdelen doch met uitzondering van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- enveiligheidsdiensten 2017, en zelfstandige bestuursorganen van de centrale overheid, voor zover deze zelfstandige bestuursorganen kwalificeren als overheidsinstantie;
h. provincies, gemeenten en waterschappen, alsmede gemeenschappelijke regelingen voor zover deze laatste kwalificeren als overheidsinstantie;
i. kritieke entiteiten als bedoeld in artikel 6, eerste lid, van de Wet weerbaarheid kritieke entiteiten.

2. Ten aanzien van het bepaalde in het eerste lid, onderdelen d tot en met f, is artikel 3, vierde lid, van de bijlage bij Aanbeveling 2003/361/EG niet van toepassing.

Artikel 9 Essentiële entiteit op basis van criteria

1. Bij regeling of besluit van Onze Minister die het aangaat, na overleg met Onze Minister, wordt een in bijlage 1 of bijlage 2 van deze wet genoemde entiteit aangewezen als essentiële entiteit, op grond van de toepasselijkheid van één of meer van de volgende criteria:
   a. de entiteit is in Nederland de enige aanbieder van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten;
   b. verstoring van de door de entiteit verleende dienst kan aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;
   c. verstoring van de door de entiteit verleende dienst kan een aanzienlijk systeemrisico met zich brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;
   d. de entiteit is kritiek vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in Nederland.
2. Onze Minister die het aangaat trekt de aanwijzing in, indien de entiteit niet langer voldoet aan één of meer van de criteria, genoemd in het eerste lid.

Artikel 11 Aanwijzing instelling voor hoger onderwijs als essentiële entiteit

1. Bij regeling of besluit van Onze Minister van Onderwijs, Cultuur en Wetenschap, na overleg met Onze Minister, kan een instelling voor hoger onderwijs als bedoeld in artikel 1.1, onder g, van de Wet op het hoger onderwijs en wetenschappelijk onderzoek als essentiële entiteit worden aangewezen.
2. Onze Minister van Onderwijs, Cultuur en Wetenschap trekt de aanwijzing, bedoeld in het eerste lid, in, indien er voor die aanwijzing geen grond meer aanwezig is.

Artikel 12 Belangrijke entiteit van rechtswege

De volgende entiteiten zijn belangrijke entiteiten:

1. entiteiten, genoemd in bijlage 1 van deze wet, niet zijnde een essentiële entiteit, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG;
   a. entiteiten, genoemd in bijlage 2 van deze wet, niet zijnde een essentiële entiteit, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG of de in het eerste lid van laatstgenoemd artikel vastgestelde drempels voor middelgrote ondernemingen overschrijden;
   b. aanbieders van openbare elektronische communicatienetwerken, genoemd in bijlage 1 van deze wet, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit;
   c. aanbieders van openbare elektronische communicatiediensten, genoemd in bijlage 1 van deze wet, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit;
   d. verleners van vertrouwensdiensten, genoemd in bijlage 1 van deze wet, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit.
2. Ten aanzien van het bepaalde in het eerste lid is artikel 3, vierde lid, van de bijlage bij de Aanbeveling 2003/361/EG niet van toepassing.

Artikel 21 Zorgplicht

1. De essentiële entiteit of belangrijke entiteit neemt passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. Ook neemt

zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken.

2. De maatregelen, bedoeld in het eerste lid, zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's, bedoeld in het eerste lid. Bij het nemen van de maatregelen houdt de entiteit in ieder geval rekening met de stand van de techniek, de uitvoeringskosten en, indien van toepassing, de desbetreffende Europese en internationale normen. Ten aanzien van de evenredigheid van de maatregelen, bedoeld in het eerste lid, houdt de entiteit naar behoren rekening met de mate waarin zij aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.
3. De maatregelen, bedoeld in het eerste lid, zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:
   a. beleid inzake risicoanalyse en beveiliging van informatiesystemen;
   b. incidentenbehandeling;
   c. bedrijfscontinuïteit, zoals back-upbeheer en herstelplannen, en crisisbeheer;
   d. de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen de entiteit en haar rechtstreekse leveranciers of dienstverleners; e. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
   e. beleid en procedures om de effectiviteit van maatregelen voor het beheersen van cyberbeveiligingsrisico's te beoordelen;
   f. basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
   g. beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
   h. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets; en
4. wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.
   a. Wanneer de entiteit overweegt welke maatregelen als bedoeld in het derde lid, onderdeel d, passend zijn, houdt zij rekening met:
      b. de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener;
      c. de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van haar leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures; en
      d. de resultaten van de door de samenwerkingsgroep op grond van artikel 22, eerste lid, van de NIS2-richtlijn uitgevoerde gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.
5. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de maatregelen, bedoeld in het eerste lid, en kunnen met betrekking tot die maatregelen eisen worden gesteld aan entiteiten, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten.

Artikel 25 Meldplicht significante incidenten

1. De essentiële entiteit of belangrijke entiteit meldt overeenkomstig de artikelen 26 tot en met 29 ieder significant incident.
2. Een incident is een significant incident als het:
   a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of
   b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.
3. Bij of krachtens algemene maatregel van bestuur worden de criteria vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in het tweede lid, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en soorten entiteiten.

Artikel 26 Vroegtijdige waarschuwing

1. De essentiële entiteit of belangrijke entiteit geeft ten behoeve van de melding, bedoeld in artikel 27, eerste lid, een vroegtijdige waarschuwing over het significante incident aan haar CSIRT en haar bevoegde autoriteit. Dit doet zij onverwijld of, indien dat niet mogelijk is, binnen 24 uur nadat zij kennis heeft gekregen van het significante incident.
2. Bij de vroegtijdige waarschuwing, bedoeld in het eerste lid:
   a. geeft de entiteit aan of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt;
   b. geeft de entiteit aan of het significante incident grensoverschrijdende gevolgen kan hebben; en
   c. verstrekt de entiteit de contactgegevens van de functionaris die verantwoordelijk is voor de melding.

Artikel 43 Nationaal register van entiteiten

1. In het belang van de goede uitvoering van deze wet beheert Onze Minister een nationaal register van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen.
2. Onze Minister evalueert het nationale register en past het indien nodig aan, ten minste elke twee jaren, of vaker indien daartoe aanleiding bestaat.
3. Onze Minister wijzigt, weigert of beëindigt in overeenstemming met de bevoegde autoriteit die het aangaat een in het eerste lid bedoelde registratie, indien de grond voor registratie is gewijzigd, vervallen of ontbreekt.

Artikel 44 Informatieverstrekking ten behoeve van nationale register

1. Een essentiële entiteit, belangrijke entiteit en een entiteit die domeinnaamregistratiediensten verleent verstrekt ten behoeve van de registratie in het nationale register, bedoeld in artikel 43, aan Onze Minister de volgende informatie middels het daarvoor opgezette mechanisme:
   a. de naam van de entiteit;
   b. het adres en de actuele contactgegevens van de entiteit, met inbegrip van e-mailadressen, IP-bereiken en telefoonnummers;
   c. indien van toepassing, de sectoren en subsectoren, bedoeld in bijlage 1 of 2 van deze wet, waartoe de entiteit behoort;
   d. indien van toepassing, een vermelding van de lidstaten van de Europese Unie waar de entiteit haar diensten als bedoeld in bijlage 1 of bijlage 2 van deze wet verleent;
   e. indien van toepassing, de deelname aan en terugtrekking uit een informatie-uitwisselingsregeling als bedoeld in artikel 62, tweede lid; en
   f. indien van toepassing, de andere bij of krachtens algemene maatregel van bestuur genoemde gegevens.
2. De entiteiten, bedoeld in het eerste lid, melden Onze Minister onverwijld of in elk geval binnen twee weken na de datum van de wijziging, elke wijziging van de informatie die zij op grond van het eerste lid hebben verstrekt.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de informatieverstrekking, bedoeld in het eerste lid, waaronder regels over de wijze waarop de informatie wordt verstrekt.

(Deel) Bijlage 1 Cyberbeveiligingswet

Sector	Soort entiteit
Gezondheidszorg	▪ Een zorgaanbieder als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg ▪ EU-referentielaboratoria als bedoeld in artikel 15 van Verordening IEUI 2022/2371[18] ▪ Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen als bedoeld in artikel 1, onderdeel 2, van Richtlijn 2001/83/EG[19] ▪ Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 vervaardigen ▪ Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd (”de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen”) in de zin van artikel 22 van Verordening (EU) 2022/123[20]
Digitale infrastructuur	▪ Aanbieders van internetknooppunten ▪ DNS”dienstverleners ▪ Register voor topleveldomeinnamen ▪ Aanbieders van cloudcomputingdlensten ▪ Aanbieders van datacentrumdiensten ▪ Aanbieders van netwerken voor de levering van inhoud ▪ Verleners van vertrouwensdiensten ▪ Aanbieders van openbare elektronische communicatienetwerken ▪ Aanbieders van openbare elektronische communicatiediensten

7.4 NIS2- Richtlijn

Richtlijn 2022/2555 van het Europees parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS2- richtlijn).

8. Praktijknormen cloud en beveiliging

8.1 ISAE 3402

De ISAE 3402-standaard bevat richtlijnen voor het afgeven van een 'third party mededeling' (TPM). Een TPM is een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de maatregelen die de verwerker heeft getroffen. De TPM wordt opgesteld in opdracht van de verwerker, en wordt verstrekt aan de verwerkingsverantwoordelijke die gebruik maakt van de diensten van de verwerker. Op die manier krijgt de verwerkingsverantwoordelijke inzicht in de getroffen maatregelen, zonder dat iedere verwerkingsverantwoordelijke daarnaar zelf onderzoek hoeft te (laten) doen.

Binnen ISAE 3402 is de basis voor de TPM een beschrijving door de bewerker van de maatregelen die voor de doelgroep van de TPM relevant zijn. De externe deskundige toetst deze beschrijving onder meer op volledigheid en stelt vervolgens vast of de bewerker de beschreven maatregelen daadwerkelijk heeft getroffen. Afhankelijk van het type TPM doet de externe deskundige een uitspraak over de aanwezigheid van de beschreven maatregelen op een bepaalde datum (type 1) of gedurende een bepaalde periode (type 2).

Een TPM kan een goed middel zijn om vast te stellen of de cloudleverancier de noodzakelijke organisatorische en technische beveiligingsmaatregelen daadwerkelijk getroffen heeft.

8.2 ISO/IEC 27017:2015

De ISO/IEC 27017:2015-norm geeft, uitgaande van ISO/SEC 27002, richtlijnen voor informatiebeveiliging bij het gebruik van clouddiensten. Certificering voor de ISO/IEC 27017:2015-norm is mogelijk in combinatie met ISO/IEC 27001.

ISO/IEC 27001
(Nederlandse versie NEN-ISO/IEC 27001nl)
Deze standaard bevat eisen waaraan het management-systeem voor informatiebeveiliging aan moet voldoen. Met de standaard kunnen leveranciers aantonen dat zij aan de vereiste informatiebeveiligingsnormen voldoen. Bij certificering wordt ook tegen deze norm ge-audit.

De standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) voor de algemene bedrijfsrisico's van een organisatie. Het ISMS, het managementsysteem voor informatiebeveiliging, is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatievoorziening beveiligen.

ISO/SEC 27002
(Nederlandse versie NEN-ISO/IEC 27002nl)
Deze standaard is een 'best practice' van beveiligings-maatregelen ('*controls*') om beveiligingsrisico's aan te pakken voor de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de NEN-ISO/IEC 27001.

ISO 27002 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

8.3 NEN 7510

NEN 7510 is een Nederlandse, sectorspecifieke uitwerking van ISO/SEC 27002 voor de zorg. NEN 7510 verwijst naar ISO/IEC 27001 voor het bijbehorende management-systeem. In de NEN 7510-norm wordt bijzondere aandacht besteed aan het beveiligen van informatie die externe partijen verwerken of beheren. Sinds 2016 kan geaccrediteerde certificering plaatsvinden op basis van NEN 7510.

Eindnoten

1 Onder gezondheidsgegevens verstaan wij alle informatie die over de (lichamelijke of geestelijke) gezondheidstoestand gaat van een persoon in het verleden, het heden en de toekomst. Dit is inclusief informatie over een persoon bij de registratie voor of de verlening van gezondheidszorgdiensten aan de desbetreffende persoon. Wordt aan de persoon een cijfer, symbool of kenmerk toegekend dat als unieke identificatie geldt van die natuurlijke persoon voor gezondheidsdoeleinden? Dan is dit ook een gezondheidsgegeven. Voorbeelden zijn informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stoffen, inclusief genetische gegevens en biologische monsters en informatie over de medische voorgeschiedenis, ziekte, het ziekterisico en de klinische behandeling van de persoon.

2 Zie artikel 4, lid 15 AVG.

3 Zie artikel 4, lid 2 AVG.

4 Volgens Overweging 33 van de NIS2- richtlijn wordt een clouddienst als volgt gedefinieerd: "Cloudcomputingdiensten moeten digitale diensten omvatten die beheer op verzoek en brede toegang op afstand ('broad remote access') tot een schaalbare en elastische pool van deelbare computercapaciteit mogelijk maken, ook wanneer deze over verschillende locaties is gedistribueerd. Computercapaciteit omvat middelen zoals netwerken, servers of andere infrastructuur, besturingssystemen, software, opslag, toepassingen en diensten". Zie ook ISO/IEC 22123-1:2023, onder 3.1.1.

5 De leverancier heeft de benodigde capaciteit al gereserveerd, de klant doet de initiële configuratie.

6 Er zijn Europese alternatieven voor verschillende soorten cloudoplossingen. Hierbij kunt u bijvoorbeeld denken aan de leveranciers Cyso cloud, IONOS, UpCloud, en Scaleway.

7 Een platform in deze context is een voorgeconfigureerde omgeving die alle benodigde software en hardware bevat om applicaties te bouwen en te draaien. Het biedt een hogere mate van abstractie dan IaaS, waardoor u zich als afnemer kunt focussen op het ontwikkelen van de functionaliteiten van het systeem in plaats van infrastructuurbeheer.

8 Onder 'telehealth' verstaan wij het gebruik van digitale technologie en telecommunicatie om gezondheidszorg te leveren op afstand.

9 Een private cloud biedt een infrastructuur die slechts door één organisatie geëxploiteerd kan worden en die in beheer is van de eigen of een externe organisatie.

10 Een publieke cloud biedt een infrastructuur voor een groot publiek, waar verschillende organisaties gebruik van kunnen maken. De eigenaar van de middelen is hier de leverancier.

11 Een community-cloud biedt een infrastructuur voor een specifieke groep van organisaties die gezamenlijk werkt aan één doel, project of product. Deze vorm van een cloudinfrastructuur is in beheer bij een van de deelnemende organisaties of bij een externe partij. De middelen zijn eigendom van een of meerdere deelnemende partijen of een externe partij.

12 Een hybride cloudmodel bestaat uit een of meerdere cloudmodellen die afzonderlijk van elkaar bestaan en die verbonden zijn via technologieën die de interoperabiliteit van de gegevens en applicaties mogelijk maken.

13 Zie voor dit begrip hoofdstuk 3 'Verwerkingsverantwoordelijke en verwerker'.

14 Zie artikelen 5, lid 2 AVG, 24 en 28 AVG.

15 Zie ook *Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG,* versie 2.0, vastgesteld op 7 juli 2021, raadpleegbaar via: https://www.edpb.europa.eu/system/files/202310/edpb_guidelines_202007_controllerprocessor_final_nl.pdf.

16 Artikel 4 lid 7 AVG.

17 Artikel 26 AVG.

18 Artikel 4, lid 8 AVG.

19 Artikel 28, lid 3, onder a AVG.

20 Zoals bepaald in artikel 28 lid 10 AVG, schendt een verwerker de AVG door verder te gaan dan de instructies van de verwerkingsverantwoordelijke. Oftewel: de verwerker mag niet eigen doeleinden nastreven en hiervoor middelen bepalen.

21 Conform artikel 28, lid 3, onder d van de AVG moet de verwerker voldoen aan de voorwaarden uit artikel 28, lid 2 en artikel 28 lid 4 om een andere verwerker in dienst te nemen.

22 Artikel 28 lid 2 AVG.

23 Let op: u moet hierbij rekening houden met de bijzondere aard van de persoonsgegevens en het beroepsgeheim dat mogelijk op de persoonsgegevens rust. Op basis hiervan kunt u overwegen om alleen subverwerkers in te schakelen wanneer de verwerker hiervoor van te voren toestemming aan u vraagt. Hiermee kunt u voorafgaand aan de verwerking bij een subverwerker hierop controle uitoefenen.

24 Zie hierover *EDPB Advies 22/2024 over bepaalde verplichtingen die van toepassing zijn wanneer een beroep wordt gedaan op verwerkers en subverwerkers*, vastgesteld op 7 oktober 2024, vindbaar via:

https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202422_relianceonprocessors-sub-processors_nl_0.pdf.

[25] Onder artikel 9 lid 1 van de AVG is het in beginsel verboden om bijzondere gegevens zoals gezondheidsgegevens te verwerken. De uitzonderingen op dit verbod en de grondslag voor de verwerking van deze gegevens zijn specifiek aan de verwerkingsverantwoordelijke. Verwerkt de leverancier de gezondheidsgegevens ook voor andere doeleinden? Of bepaalt de leverancier overige wezenlijke aspecten voor de verwerking? Dan moet u bepalen in hoeverre er een legitieme grondslag is voor de verwerking van deze gegevens door de leverancier. Bovendien moet u rekening houden met sectorale wetgeving die voor u van toepassing kan zijn, zoals de geheimhoudingsverplichting op basis van de Wet op de geneeskundige behandelingsovereenkomst (WGBO).

[26] Artikel 28, lid 3, onder c AVG.

[27] Zie voor de definitie van 'betrokkene' artikel 4, lid 1 AVG.

[28] Artikel 28, lid 1, en Overweging 81 AVG.

[29] Artikel 5, lid 2 en 24 lid 1 AVG.

[30] Voor het gebruik van clouddiensten door zorgaanbieders bestaan verschillende normen. De relevantste normen zijn ISAE 3402, ISO 27017 en NEN 7510. Daarnaast spelen de algemene beveiligingsnormen ISO 27001 en ISO 27002 een rol.

[31] Artikel 28, lid 3 onder h AVG.

[32] Artikelen 5, lid 1, onder a, 6 en 9 AVG.

[33] Artikel 5 lid 2 AVG.

[34] Deze handreiking biedt u handvaten om een weloverwogen keuze te maken om de gezondheidsgegevens in de cloud te verwerken. Globaal krijgt u inzicht in de aspecten die u minstens zou moeten betrekken bij de overstap naar de cloud. In dit document wordt niet expliciet ingegaan op het verrichten van een *data protection impact assessment* (DPIA) op grond van artikel 35 AVG. Als u op grote schaal gezondheidsgegevens verwerkt, dan houdt de verwerking van deze bijzondere persoonsgegevens waarschijnlijk een hoog risico in voor de rechten en vrijheden van de betrokkenen. Daarvoor moet u als verwerkingsverantwoordelijke een DPIA uitvoeren. Zie hierover meer op onze website: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia#wanneer-een-dpia. De aspecten die in deze handreiking worden beschreven, bieden u voldoende input om een verplichte DPIA te verrichten. Als u verplicht bent op grond van artikel 35 AVG om een DPIA uit te voeren, dan moet u de informatie die u heeft verkregen door de stappen in deze handreiking te volgen, aanvullen met wat van u wordt gevraagd op grond van artikel 35 lid 7-11 AVG. Zie hierover ook de *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679*, vindbaar via: https://ec.europa.eu/newsroom/article29/items/611236/en.

[35] Is er binnen uw organisatie niet de juiste kennis om deze beoordeling uit te voeren? Dan moet u daar mogelijk hulp voor inschakelen.

[36] Inclusief de technische en organisatorische maatregelen om de persoonsgegevens, zoals gezondheidsgegevens, te beschermen.

[37] Een voorbeeld hiervan is dat betrokkenen een beroep doen op het recht van verwijdering van hun gegevens. Een leverancier moet in dat geval de gegevens onherroepelijk kunnen verwijderen.

[38] Metadata wordt door het Nationaal Instituut voor Standaarden en Technologie (NIST) gedefinieerd als "informatie die de kenmerken van data beschrijft waaronder bijvoorbeeld structurele metagegevens die gegevensstructuren beschrijven (denk bijvoorbeeld aan gegevensformaat) en beschrijvende metagegevens die de inhoud van data beschrijven." Vindbaar via https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf, NIST SP 800-150, onder metadata. Voorbeelden van metadata zijn locatie data, IP-adres, etc. Soms kan metadata informatie bevatten die gevoelig en persoonlijk van aard is. Zoals de datum, tijd, duur en locatie waarvan er toegang is verkregen tot de cloud. Op basis van dergelijke informatie kunnen er conclusies worden getrokken over het privéleven van de desbetreffende persoon. Zie hierover onder meer in de zaken HvJ C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Secretary of State for the Home Department, ECLI:EU:C:2016:970.

[39] Artikel 28, lid 10 AVG.

[40] Artikel 5 AVG.

[41] Artikel 5, lid 1, f en artikel 32 AVG.

[42] Artikel 32 AVG.

[43] Een voorbeeld van een risicobeoordelingsmethode is de EBIOS-methode. Deze methode staat voor Expression of Needs and Identification of Security Objectives, en maakt het mogelijk dat persoonsgegevens worden beschouwd als een eigendom dat beschermd moet worden en waarbij de impact op de privacy van de betrokkenen in overweging wordt genomen. Deze methode sluit goed aan op de ISO:27001:2022 en ISO:27005:2022 en kan bijdragen aan het treffen van effectieve beveiligingsmaatregelen die in overeenstemming zijn met de NIS2-richtlijn. Meer over deze

methode kunt u nalezen op https://cyber.gouv.fr/publications/ebios-risk-manager-method.

44 Volgens de Internationale Organisatie voor Standaarden (ISO) wordt een virtueel systeem (*virtual machine*) gedefinieerd als een geïsoleerde omgeving voor het uitvoeren van software die gebruikmaakt van gevirtualiseerde fysieke bronnen, zoals processors, geheugen opslag en netwerkverbindingen. Zie ISO/IEC 22123-1:2023(en), onder 3.12.2.

45 Met 'verzoeken van autoriteiten van derde landen' wordt bedoeld een verzoek dat afkomstig is van allerlei overheidsinstanties, waaronder instanties die toezicht houden op de particuliere sector, zoals banken-toezichthouders en belastingdiensten, maar ook instanties die zich bezighouden met rechtshandhaving en nationale veiligheid van een derde land zoals bedoeld onder de AVG. Zie hierover '*EDPB Richtsnoeren 02/2024 betreffende artikel 48 AVG*', versie 2.1. vastgesteld 4 juni 2025, vindbaar via: https://www.edpb.europa.eu/system/files/2025-11/edpb_guidelines_202402_article48_v2_nl_0.pdf.

46 Zie artikel 32, lid 1, onder b en c AVG.

47 Overname of faillissement van de leverancier kan ertoe leiden dat de cloudleverancier de dienstverlening aanpast. Het gevolg kan onder meer zijn dat de gezondheidsgegevens die de cloudleverancier verwerkte, tijdelijk of permanent niet meer voor u toegankelijk zijn. Ook wanprestatie door de cloudleverancier is een risico voor de continuïteit van de dienstverlening. Om problemen te voorkomen zijn goede contractuele afspraken nodig. Het is daarnaast van groot belang dat u uw gegevens zonder al te veel rompslomp terugkrijgt als u de samenwerking met de cloudleverancier wilt beëindigen. Let erop dat cloudleveranciers niet altijd gebruik maken van standaarddatabasetechnologieën en -oplossingen. De bij hen aanwezige gegevens kunnen daardoor niet altijd zonder meer worden overgebracht naar een database van een andere verwerker of naar uw database. Dit is een belangrijk aandachtspunt bij de selectie van een leverancier.

48 Als u eenmaal voor een cloudleverancier heeft gekozen, kunnen er grote drempels zijn om over te stappen naar een andere leverancier. Dit wordt ook wel *vendor lock-in* genoemd.

49 Houd rekening met dit aandachtspunt bij uw exitstrategie en -plan, zie hiervoor onderdeel 4.6.

50 De locatie van de gegevens ofwel *data residency* gaat over de fysieke of geografische locatie van de opslag en verwerking van gegevens.

51 Leveranciers kunnen onder de reikwijdte vallen van wet- en regelgeving van derde landen (landen buiten de EER) waar het niveau van bescherming van bijzondere persoonsgegevens, zoals gezondheids-gegevens, niet gelijkwaardig is aan dat in de EER. Bovendien kunnen de rechten en fundamentele vrijheden van betrokkenen worden beperkt op grond van de toepasselijke wet- en regelgeving in het derde land. Naast de gegevenbeschermingsaspecten is het mogelijk dat 'uw' gegevens, intellectuele eigendom en operationele continuïteit onderworpen worden aan een dergelijke jurisdictie. Dit kan leiden tot verstoringen (zoals *kill-switch*) of ongeoorloofde toegang tot de persoonsgegevens.

52 Volgens de Internationale Organisatie voor Standaardisatie (ISO) wordt *multi-tenant* gedefinieerd als een allocatie van fysieke of virtuele resources (zoals rekencapaciteit, opslag, geheugen, toepassingen, besturingssysteem, servers en het netwerk) zodat klanten ofwel *tenants* en hun configuraties en data geïsoleerd zijn van de andere klanten en ontoegankelijk zijn gemaakt voor andere klanten. Zie ISO/IEC 22123-1:2023(en), onder 3.4.3. De beveiligingsrisico's bij een multi-tenant omgeving zijn bijvoorbeeld beveiligings-incidenten (inclusief met persoonsgegevens zoals bedoeld in de AVG) en ongeoorloofde toegang tot data (door bijvoorbeeld onvoldoende isolatie van de verschillende klant-omgevingen en/of configuraties).

53 Onder de AVG is een verwerker verplicht om alleen persoonsgegevens te verwerken op instructie van de verwerkingsverantwoordelijke. Zie artikel 28, lid 3, onder a van de AVG.

54 Artikel 28, lid 3 onder b AVG.

55 Artikelen 5, lid 1, onder f, en 32 AVG.

56 Artikel 28, lid 3 onder c AVG.

57 Artikel 28, lid 3 onder d AVG.

58 De termijn die u in de rechtshandeling vastlegt, vloeit voort uit artikel 28, lid 3 onder h AVG.

59 **Let op!** De artikelen 33 en 34 AVG bevatten de regeling omtrent inbreuken in verband met persoonsgegevens (ook wel datalekken genoemd). Artikel 33 behandelt de meldplicht richting de toezichthouder en artikel 34 de meldplicht richting betrokkenen. Zoals reeds aangegeven is het verlenen van bijstand van de verwerker aan de verwerkingsverantwoordelijke bij het nakomen van de verplichtingen uit hoofde van artikel 32 tot en met 36 AVG niet vrijwillig. Toch bevatten enkele verwerkersovereenkomsten geen uitgewerkte regeling hiervoor. Een verwerkingsverantwoordelijke dient bijvoorbeeld een inbreuk te melden conform de in art. 33 lid 1 AVG genoemde termijnen en condities. Zo is er een termijn opgenomen van 72 uur waarbinnen inbreuken, "*nadat hij er kennis van heeft genomen*", door de verwerkingsverantwoordelijke dienen te worden gemeld bij de toezichthouder. De AP signaleert in verwerkersovereenkomsten meerdere termijnen

waarbinnen verwerkers meldingen moeten doen aan de verwerkingsverantwoordelijke. Van "onverwijld", via "binnen vier uur" tot binnen "48 uur", zelfs "72 uur" is voorgekomen. Mogelijk is deze laatste termijn voor verwerkingsverantwoordelijke overgenomen uit de AVG en als maatstaf gekozen voor de termijn die de verwerker richting de verwerkingsverantwoordelijke heeft. Het is verstandig om te overleggen wat een passende termijn zou zijn waarbinnen een melding door de verwerker aan de verwerkingsverantwoordelijke is voorzien en als doelstelling te nemen dat deze termijn zo kort mogelijk is. Lees hierover meer in het onderzoeksrapport 'Werkende verwerkersovereenkomsten: onderzoek naar de toepassing in de private sector', vindbaar via: https://www.autoriteitpersoonsgegevens.nl/uploads/imported/onderzoek_verwerkersovereenkomsten.pdf.

60 Artikel 28, lid 4 AVG.

61 Artikel 28, lid 3 onder a en Hoofdstuk V AVG.

62 Artikel 28, lid 3 onder f AVG.

63 Artikel 28, lid 3 onder f AVG en artikel 28, lid 3 onder h AVG.

64 Artikel 17 en 28, lid 3 onder g en e AVG.

65 Artikel 28 lid 9 AVG.

66 Artikel 28 lid 3 AVG.

67 Artikel 28 lid 3 AVG.

68 Artikel 5, lid 1, onder b AVG. Zie ook onder C-77/21 *Digi*, ECLI:EU:C:2022:805.

69 Zie voor meer informatie *EDBP Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*, versie 2.0. vastgesteld op 7 juli 2021. Vindbaar via: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_nl.pdf.

70 Als beveiligingsmaatregel is het mogelijk dat u ervoor kiest om op de gezondheidsgegevens encryptie toe te passen, de gegevens anderzijds af te schermen of deze ontoegankelijk te maken voor de leverancier. Het is belangrijk dat u over de impact van de genomen beveiligingsmaatregel afspraken maakt met de leverancier. In het bijzonder met oog op de geleverde dienst en ondersteuning door de leverancier.

71 Het is mogelijk om de afspraken in verschillende contracten vast te leggen zoals een overeenkomst, verwerkersovereenkomst, Service Level Agreement, etc. De AP vindt het belangrijk om voldoende aandacht te besteden aan de contractuele afspraken met de leverancier. In het bijzonder is het belangrijk om inzicht te krijgen in de afspraken en om over voldoende kennis te beschikken over die afspraken. De contractuele voorwaarden beheersen immers (mede met andere maatregelen)de risico's van het verwerken van gezondheidsgegevens in de cloud.

72 In de verwerkersovereenkomst kunt u een exitclausule opnemen, die verwijst naar een bijlage van de overeenkomst of naar andere bindende documenten waarin de voorbereiding is vastgelegd op een beëindiging van het contract met de leverancier en/of op uitvoering van de migratie van data naar een nieuwe leverancier.

73 Artikel 28, lid 3, onder h AVG.

74 Met on-premise host en beheert de organisatie in beginsel de IT-infrastructuur binnen de fysieke faciliteiten van de eigen organisatie. Alle hardware- en netwerkcomponenten worden door de organisatie intern onderhouden, waardoor de organisatie de volledige controle heeft over de systemen en daarmee ook over de data.

75 Zie ook de ISO:27001:2022 Annex A 5.23 informatie-beveiliging voor het gebruik van clouddiensten.

76 Zie ook Clouddiensten BIO Thema uitwerking van maart 2023, vindbaar via: https://www.cip-overheid.nl/media/h4lcnhdn/20230322-bio-thema-uitwerking-clouddiensten-v22-def.pdf

77 Een exitplan beschrijft de voorbereiding op een beëindiging van de overeenkomst met de cloudleverancier en/of uitvoering van de migratiewerkzaamheden naar een nieuwe leverancier.

78 Met een escrow-regeling wordt bedoeld een regeling over de voorwaarden waaronder (bedrijfskritische) activa zoals broncode, data en documentatie worden veilig gesteld. De escrow-regeling zorgt ervoor dat u toegang blijft houden tot de activa, zelfs wanneer de leverancier niet meer in staat is om de software te ondersteunen of door te ontwikkelen. Hierdoor voorkomt u dat bedrijfskritische processen stilvallen.

79 De lijst is opgesteld aan de hand van de o.a. de volgende bronnen: Standaarden en standaardisatieactiviteiten voor clouddiensten, Forum Standaardisatie (2024) vindbaar via https://www.forumstandaardisatie.nl/sites/default/files/FS/2024/0619/FS-20240619.5B-rapport-onderzoek-standaardisatie-cloud.html#wat-is-cloud, en *Study presenting assessments of codes of conduct on data porting and cloud switching*, SWIPO (2022) vindbaar via: https://digital-strategy.ec.europa.eu/en/library/study-presenting-assessments-codes-conduct-data-porting-and-cloud-switching.

80 Deze lezing vloeit voort uit artikel 28 lid 3 en 4 AVG.

81 Belangrijk om te vermelden is dat u niet de toestemming van uw patiënt nodig heeft om de gezondheidsgegevens in de cloud te plaatsen. Ook het medisch beroepsgeheim schrijft niet voor dat u hiervoor toestemming moet vragen. Artikel 7:457 Burgerlijk Wetboek (BW) bepaalt namelijk dat patiëntgegevens zonder toestemming mogen worden verstrekt aan 'degenen die rechtstreeks betrokken zijn bij de

uitvoering van de behandelingsovereenkomst'. De AP beschouwt een cloudleverancier die patiëntgegevens verwerkt voor de zorgaanbieder als 'rechtstreeks betrokken bij de uitvoering van de behandelingsovereenkomst'.

82 Zie onder andere het verbod op het verwerken van gezondheidsgegevens in artikel 9 AVG. Verder staat in Overweging 51 van de AVG het volgende over bijzondere persoonsgegevens, zoals gezondheidsgegevens: "*Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en fundamentele vrijheden.*" In Overweging 53 stelt de wetgever dat "*bijzondere categorieën van persoonsgegevens [...] betere bescherming [...] vereist [...]. Derhalve dient deze verordening te voorzien in geharmoniseerde voorwaarden voor de verwerking van bijzondere categorieën van persoonsgegevens over de gezondheid, in geval van specifieke behoeften, met name indien deze gegevens met het oog op bepaalde gezondheidsdoeleinden worden verwerkt door personen die wettelijk aan het beroepsgeheim gebonden zijn.*

83 Zie artikel 28, lid 3, sub h AVG.

84 Een voorbeeld hiervan is de US Cloud-Act. Hierover kunt u meer lezen in het onderzoeksrapport over de Cloud-Act van het NCSC, vindbaar via: https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo.

85 Zie onder andere Tweede Kamer initiatiefnota van de leden Six Dijkstra en Kathmann 'Wolken aan de horizon', vindbaar via: https://open.overheid.nl/documenten/080c489f-4fd8-4755-9b35-02f91c5748c8/file.

86 Zie hierover *EDPB Advies 22/2024 over bepaalde verplichtingen die van toepassing zijn wanneer een beroep wordt gedaan op verwerkers en subverwerkers*, vastgesteld op 7 oktober 2024, vindbaar via: https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202422_relianceonprocessors-sub-processors_nl_0.pdf.

87 Zie hoofdstuk 4.

88 Zie paragrafen 4.5. en 4.6.

89 Zie paragraaf 4.6.

90 Zie paragraaf 2.2.

91 In de tekst worden de zuivere vormen van een 'doorgifte' beschreven zoals bedoeld onder de AVG. Het is mogelijk dat in uw situatie geen sprake is van een doorgifte. Om deze beoordeling te kunnen maken adviseren wij om de *EDPB Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen inzake internationale doorgiften overeenkomstig hoofdstuk V van de AVG*, versie 2.0. door te nemen, vindbaar via: https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_nl.pdf.

92 Kan het beschermingsniveau dat vereist wordt op basis van de AVG en relevante sectorale wet- en regelgeving niet worden gewaarborgd? Dan moet u maatregelen treffen. Bijvoorbeeld als bepaalde wet- en regelgeving in een derde land inbreuk maakt op het beschermingsniveau dat geboden moet worden aan gezondheidsgegevens.

93 Zie hiervoor ook EDPB's *Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen*, versie 2.0, vastgesteld op 18 juni 2021, paragraaf 53.

94 Kiest u ervoor om een leverancier in te schakelen uit een 'derde land' zoals bedoeld in de AVG? Dan is het risico aanwezig dat autoriteiten van derde landen de leverancier om toegang tot de gezondheidsgegevens verzoeken. Dit is een belangrijke factor om mee te wegen in uw risicobeoordeling. Zie hierover ook voetnoot 44.

95 Zie ook paragraaf 4.6.

96 Zie hiervoor onder andere de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en de Regeling gebruik burgerservicenummer in de zorg. Ook stelt de Inspectie Gezondheidszorg en Jeugd (IGJ) eisen aan ziekenhuizen om aantoonbaar te voldoen aan de NEN 7510.

97 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PbEU 2022, L333/80).

98 Zie hierover meer op https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg/achtergrond

99 Zie bijvoorbeeld artikel 2 Regeling gebruik burgerservicenummer in de zorg, artikel 10 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, artikel 9.1.1. lid 4 Wet langdurige zorg, artikel 86, lid 4 en 5, Zorgverzekeringswet, artikelen 28, lid 2 en 29 van het Besluit gebruik Burgerservicenummer in de zorg.

100 Artikel 1 lid 1 Wet kwaliteit, klachten en geschillen zorg definieert een zorgaanbieder als '*een instelling dan wel een solistisch werkende zorgverlener*'. De Wet zorg en dwang sluit aan op deze definitie door in artikel 1 lid 1 sub f een zorgaanbieder te beschrijven als '*een*

natuurlijke persoon of rechtspersoon die beroepsmatig of bedrijfsmatig zorg aanbiedt aan een cliënt'.

[101] Zie hierover meer op: https://www.igj.nl/vraag-en-antwoord/vragen-over-nen-7510

[102] Zie NEN 7510-2:2024, eis 5.23.

[103] De ontwikkelingen rondom de Cyberbeveiligingswet kunt u volgen via https://wetgevingskalender.overheid.nl/Regeling/WGK014627.

[104] Zie artikelen 9 en 10 Cyberbeveiligingswet.

[105] Volgens de Cbw zijn de volgende sectoren 'zeer kritieke sectoren': energie, vervoer, bankwezen en infrastructuur financiële markt, gezondheidszorg, drinkwater, digitale infrastructuur (zoals DNS dienstverleners, aanbieders van cloudcomputingdiensten en aanbieders van datacentrumdiensten), beheer van ICT-diensten, overheid en ruimtevaart. Als 'andere kritieke sectoren' ziet de Cbw: digitale aanbieders (onlinemarktplaatsen, onlinezoekmachines, socialenetwerkdiensten), post- en koeriersdiensten, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek en vervaardiging/manufacturing. Zie Bijlage I en II van de Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet). Zie ook de website van het Nationaal Cyber Security Centrum (NCSC) waar u een zelfevaluatie en flowchart kunt vinden om te beoordelen of u onder de Cbw valt, vindbaar via: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/aan-de-slag.

[106] Zie voor meer informatie de website van het ministerie van Volksgezondheid, Welzijn en Sport (VWS): https://www.datavoorgezondheid.nl/weerbaarheid/cyberbeveiligingswet

[107] Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333) (Cyberbeveiligingswet), p.50.

[108] Het ministerie VWS heeft een interactieve beslisboom Cyberbeveiligingswet beschikbaar gesteld voor de sector gezondheidszorg, zie hiervoor: https://www.datavoorgezondheid.nl/documenten/2025/04/01/beslisboom-cyberbeveilingswet.

[109] Het NCSC heeft een flowchart en zelfassessment-tool beschikbaar gesteld waarvan u kunt bepalen of u moet voldoen aan de eisen uit de Cbw, zie: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/aan-de-slag.

[110] De European Union Agency for Cybersecurity heeft een technische implementatie handreiking opgesteld voor de implementatie van de eisen uit de NIS2-richtlijn,vindbaar via:https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

[111] De maatregelen die in de NIS2/Cbw worden voorgeschreven, moet u opvatten als maatregelen die u ten minste moet nemen. Dit betekent niet dat uw organisatie NIS2/Cbw-compliant is als u voldoet aan deze maatregelen. Uw organisatie moet immers 'een op de risico's afgestemd beveiligingsniveau waarborgen'. Afhankelijk van wat die risico's zijn, moet u bepaalde beveiligingsmaatregelen treffen.

[112] Artikel 21, lid 2, onder a, Cbw.

[113] Artikel 21, lid 2, onder i, Cbw.

[114] Artikel 21, lid 2, onder c, Cbw.

[115] Artikel 21, lid 2, onder b, Cbw.

[116] Artikel 21, lid 2, onder g, Cbw.

[117] Artikel 21, lid 2, onder e, Cbw.

[118] Artikel 21, lid 2, onder d, Cbw.

[119] Artikel 21, lid 2, onder h, Cbw.

[120] Artikel 21. Lid 2, onder j, Cbw.

[121] Artikel 21, Lid 2, onder f, Cbw.

[122] De infosheet is beschikbaar op de website van het NCSC, zie: https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/februari/27/infosheet-nis2-verplichtingen-zorgplicht.

[123] Een incident is een 'significant incident' volgens artikel 25, lid 2 Cbw als het: 'a) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b) andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.' Verder kunnen bij of krachtens algemene maatregel van bestuur criteria worden vastgesteld waarmee bepaald kan worden of er sprake is van een significant incident zoals bedoeld in de Cbw.

[124] Artikel 26 Cbw.

[125] De algemene CSIRT in Nederland is het NCSC en specifiek voor de Nederlandse zorg is Z-CERT, waar een melding gemaakt kan worden.

[126] Zie paragraaf 5.3.

[127] Artikel 27 Cbw.

[128] Artikel 26 Cbw.

[129] Artikel 27 Cbw.

[130] Artikel 28 Cbw.

[131] Uiterlijk één maand na de melding zoals bedoeld in artikel 27 Cbw moet u een eindverslag indienen bij het

CSIRT en de bevoegde autoriteit. Zie artikel 29, lid 1 Cbw. Duurt het incident nog voort op het moment dat u het eindverslag had moeten indienen? Dan moet u het eindverslag indienen binnen één maand nadat het incident is afgehandeld. Zie artikel 29, lid 2 Cbw.

[132] Bij een vroegtijdige waarschuwing dient de entiteit aan te geven of het significante incident vermoedelijk is veroorzaakt door een onrechtmatige of kwaadwillige handeling. Zie artikel 26, lid 2, onder a Cbw.

[133] Artikel 26, lid 2, onder b Cbw en artikel 29, lid 1, onder d Cbw.

[134] Artikel 26, lid 2, onder c Cbw.

[135] Artikel 27, lid 1, onder d Cbw en artikel 29, lid 1 onder a-b Cbw.

[136] Artikel 26, lid 1 Cbw, artikel 27, lid 1 Cbw, artikel 27, lid 1, onder d Cbw, artikel 27, lid 2 Cbw en artikel 29, lid 1, onder a Cbw. Zie ook Flowchart Cyberbeveiligingswet: meldplicht van het NCSC, vindbaar via: https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/oktober/08/infosheet-meldplicht.

[137] Artikel 27, lid 1, onder b Cbw en artikel 29, lid 1, onder a Cbw.

[138] Artikel 29, lid 1, onder c Cbw.

[139] Artikel 27, lid 1, onder b en artikel 29, lid 1, onder a Cbw. Zie ook *Kamerstukken II* 2024/25, 36764, nr. 3, p. 121.

[140] Zie artikel 44 Cbw en checklist Cbw registratie van het NCSC via: https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/oktober/08/checklist-registreren.

[141] Artikel 58 Cbw.

[142] Volgens artikel 33 AVG moet u een 'inbreuk in verband met persoonsgegevens' (datalek) melden bij de toezichthouder zonder onredelijke vertraging en uiterlijk 72 uur nadat u ervan kennis heeft genomen. Tenzij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

[143] Op de website van de AP kunt u meer informatie vinden over wat een 'datalek' is, wat u moet doen, hoe u een datalek meldt, etc. Zie: https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen.

[144] Houdt een datalek waarschijnlijk een hoog risico in voor de rechten en vrijheden van natuurlijke personen? Dan moet u als verwerkingsverantwoordelijke de betrokkene(n) onverwijld op de hoogte stellen. Tenzij er sprake is van een van de voorwaarden uit artikel 34 lid 3 van de AVG.

De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder op persoonsgegevens die mensen beschermt in een digitale wereld.

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ Den Haag

autoriteitpersoonsgegevens.nl