

Overeenkomst inzake bescherming van persoonsgegevens conform art. 28 AVG

m.b.t. het uitvoeren van IT-diensten

tussen

(hierna te noemen **Verwerkingsverantwoordelijke**)

en

Hogrefe Uitgevers B.V., Weteringschans 128, 1017 XV Amsterdam
(hierna te noemen **Verwerker**)

Preambule

Deze overeenkomst concretiseert de verplichtingen van de Verwerkingsverantwoordelijke en de Verwerker inzake de verwerking van persoonsgegevens bij het uitvoeren van IT-diensten conform art. 28 van de Verordening van de EU 2016/679 (hierna te noemen AVG).

Deze overeenkomst is van toepassing op alle activiteiten waarbij medewerkers van de Verwerker of een door hem belaste derde in aanraking kunnen komen met persoonsgegevens van de Verwerkingsverantwoordelijke. De looptijd van deze bijlage richt zich naar de looptijd van de hoofdovereenkomst tussen beide partijen inzake het gebruik van het HTS online testsysteem van Verwerker.

1. Definities

De definities van art. 4 AVG zijn van toepassing.

2. Onderwerp, omvang, wijze en doel van het gegevensgebruik, kring van betrokkenen

(1) Doel van de verwerking is de tussen de Verwerkingsverantwoordelijke en Verwerker bestaande overeenkomst omtrent het uitvoeren van IT-diensten, die bij verwerving van toegang tot het online-portaal HTS in werking treedt. Bij het uitvoeren van IT-diensten is er sprake van een aan voorschriften gebonden verwerking van persoonsgegevens door de Verwerker voor de Verwerkingsverantwoordelijke.

(2) Onderwerp van deze overeenkomst is daarbij met name het verrichten van de volgende diensten door de Verwerker:

- Hosten van het HTS online portaal en garanderen van de operationaliteit
- Verzorgen van de serverinfrastructuur voor het uitvoeren van online testen
- Ter beschikking stellen van de testresultaten in PDF-formaat in het online portaal, voor de duur van de overeenkomst of tot de Verwerkingsverantwoordelijke betreffende bestanden zelf verwijderd

(3) In het kader van de uitvoering van de diensten hebben de medewerkers van de Verwerker toegang tot de volgende persoonsgegevens:

- naam
- leeftijd
- geslacht
- e-mailadres (bij uitzondering)
- testresultaten en analyses

(4) Beperkt tot het doel van de correcte vervulling van bovengenoemde diensten mag de Verwerker persoonsgegevens voor de Verwerkingsverantwoordelijke verzamelen, opslaan, wijzigen, overdragen en gebruiken.

(5) Personen van wie de persoonsgegevens mogelijk worden verwerkt kunnen zijn (afhankelijk van het werkgebied van de Verwerkingsverantwoordelijke):

- medewerkers
- sollicitanten
- coachees
- patiënten
- studenten
- leerlingen
- overigen:

3. Verantwoording voor de wettelijke toelaatbaarheid

(1) De Verwerkingsverantwoordelijke is op grond van zijn hoedanigheid ingevolge van art. 4, lid 7 AVG alleen verantwoordelijk voor de beoordeling van de wettelijke toelaatbaarheid van de in het kader van de verwerkingsrelatie uitgevoerde verwerking en gebruik van persoonsgegevens door de Verwerker, met het oog op de regelingen van de AVG en andere voorschriften omtrent bescherming van persoonsgegevens.

(2) Op basis van deze verantwoordelijkheid kan de Verwerkingsverantwoordelijke tijdens de looptijd van deze overeenkomst en na afloop van de overeenkomst verwijdering, blokkering en teruggave van persoonsgegevens eisen.

(3) Alleen de Verwerkingsverantwoordelijke is verantwoordelijk voor het controleren van de wettelijke toelaatbaarheid van bepaalde door hem uitgevoerde of voorgenomen verwerkingsactiviteiten.

4. Opvolgen van instructies door Verwerker

- (1) De Verwerker verwerkt en gebruikt de persoonsgegevens van de Verwerkingsverantwoordelijke uitsluitend in het kader van de vervulling van overeengekomen diensten en de speciale opdrachten van de Verwerkingsverantwoordelijke. Het is de Verwerker niet toegestaan de persoonsgegevens van de Verwerkingsverantwoordelijke op een andere dan de aangegeven in artikel 2 genoemde wijze te vergaren, verwerken of te gebruiken.
- (2) De Verwerkingsverantwoordelijke of een gemachtigde van de Verwerkingsverantwoordelijke zal opdrachten, die afwijken van de overeenkomsten conform artikel 2, schriftelijk mededelen per e-mail, brief of fax. Mondelinge instructies worden onmiddellijk per e-mail, brief of fax bevestigd.
- (3) De Verwerker is niet gerechtigd tot het corrigeren, verwijderen of blokkeren van gegevens, tenzij hiervoor een schriftelijke instructie is gegeven door de Verwerkingsverantwoordelijke.

5. Functionaris voor gegevensbescherming

De Verwerker heeft binnen het bedrijf een functionaris voor gegevensbescherming benoemd. De contactgegevens van de functionaris voor gegevensbescherming zijn:

Felix Hudy
Functionaris Bescherming persoonsgegevens
Merkelstraße 3
D-37085 Göttingen - Duitsland
E-mail: datenschutz@hogrefe.de

6. Technische en organisatorische veiligheidsmaatregelen

- (1) De Verwerker garandeert de toepassing van de in het kader van de correcte uitvoering van de verwerkingen vereiste veiligheidsmaatregelen. Hij treft gepaste technische en organisatorische maatregelen voor de juiste persoonsgegevensbeveiliging, die voldoen aan de eisen van de Algemene Verordening Gegevensbescherming, met name art. 32 AVG. Hiervoor dient de Verwerker:
 - de vertrouwelijkheid, integriteit, beschikbaarheid en belastbaarheid van de systemen en diensten met betrekking tot de verwerking duurzaam te garanderen,
 - de capaciteit te garanderen om de beschikbaarheid van persoonsgegevens en de toegang tot deze gegevens bij een fysiek of technisch incident snel weer te herstellen alsmede
 - de in de bijlage van deze overeenkomst vermelde maatregelen te treffen.
- (2) De Verwerker zorgt voor een procedure voor het regelmatig testen, analyseren en evalueren van de effectiviteit van de technische en organisatorische maatregelen teneinde de veiligheid van de verwerking te garanderen.

(3) De vereiste technische en organisatorische maatregelen zijn afhankelijk van de technische vooruitgang en de verdere ontwikkeling. Op basis hiervan is Verwerker gerechtigd om alternatieve, adequate maatregelen te gebruiken. Daarbij mag het veiligheidsniveau van de vastgelegde maatregelen niet worden onderschreden. Wezenlijke wijzigingen dienen te worden gedocumenteerd en aan de Verwerkingsverantwoordelijke te worden medegedeeld.

(4) De Verwerkingsverantwoordelijke is bekend met de door de Verwerker uitgevoerde technische en organisatorische maatregelen. De Verwerkingsverantwoordelijke is ervoor verantwoordelijk, het beveiligingsniveau passend is met betrekking tot de risico's van de te verwerken gegevens.

(5) De Verwerker ondersteunt de Verwerkingsverantwoordelijke bij de documentatie van de door Verwerker getroffen technische en organisatorische maatregelen.

7. Geheimhoudingsplicht

(1) De Verwerker is verplicht, bij de verwerking van de persoonsgegevens van de Verwerkingsverantwoordelijke geheimhouding te betrachten conform art. 28, lid 3b AVG. Met name dient hij te garanderen, dat de persoonsgegevens afkomstig van de Verwerkingsverantwoordelijke niet aan derden worden doorgegeven of op andere wijze gebruikt worden. Hij mag bij de verwerking en het gebruik van de persoonsgegevens van de Verwerkingsverantwoordelijke alleen gebruik maken van gemachtigde personen, die zich conform art. 28, lid 3 b AVG schriftelijk tot geheimhouding hebben verplicht.

(2) De Verwerker dient medewerkers, die zich bezighouden met de uitvoering van werkzaamheden, vertrouwd te maken met de voor hen van belang zijnde bepalingen van de gegevensbescherming en erop toe te zien dat de medewerkers de voorschriften met betrekking tot gegevensbescherming in acht nemen. De regelmatige scholing van de medewerkers moet door hem worden gedocumenteerd en op verzoek van de Verwerkingsverantwoordelijke ter beschikking worden gesteld.

8. Informatieplichten

(1) De Verwerker stelt de Verwerkingsverantwoordelijke alle informatie ter beschikking, welke deze nodig heeft om het voldoen aan de voorschriften inzake de Verwerking van persoonsgegevens conform art. 28 AVG te documenteren en aan te tonen.

(2) De Verwerker informeert de Verwerkingsverantwoordelijke onverwijld omtrent bedrijfsstoringen die relevant zijn voor de gegevensbeveiliging, bij indicaties van mogelijke of vaststaande schendingen van de gegevensbeveiligingen, bij andere onregelmatigheden in verband met de verwerking van persoonsgegevens alsmede bij schendingen van de bepalingen van deze overeenkomst door de Verwerker of een onderaannemer van de Verwerker. Mogelijke gebreken bij de verwerking van persoonsgegevens dienen onverwijld door de Verwerker te worden verholpen. Hiervan dient schriftelijk bewijs te worden overlegd.

(3) De Verwerker stelt de Verwerkingsverantwoordelijke de noodzakelijke informatie ter beschikking ten behoeve van het register van de verwerkingsactiviteiten conform art. 30 AVG.

(4) Indien persoonsgegevens bij de Verwerker door verpanding of inbeslagname, door een insolventieprocedure of door andere gebeurtenissen of maatregelen van derden worden bedreigd, dient de Verwerker de Verwerkingsverantwoordelijke hierover onverwijld te informeren. De Verwerker dient de hierbij betrokken personen onverwijld er over te informeren, dat de rechten op de persoonsgegevens bij de Verwerkingsverantwoordelijke liggen.

9. Overige plichten van de Verwerker

(1) Voor andere dan de onder 2 van deze overeenkomst vastgelegde doelen mogen de persoonsgegevens alleen met schriftelijke toestemming van de Verwerkingsverantwoordelijke worden verwerkt. Dit geldt met name voor de overhandiging aan derden.

(2) Als de Verwerker van mening is, dat een instructie van de Verwerkingsverantwoordelijke een inbreuk vormt op de AVG of andere voorschriften van de Europese Unie of de lidstaten met betrekking tot gegevensbescherming, wijst de Verwerker de Verwerkingsverantwoordelijke hier onverwijld op.

(3) Bij wettelijke uitzonderingen op de gezagsverhouding van de Verwerker conform art. 28, lid 3 AVG informeert de Verwerker de Verantwoordelijke omtrent de op basis van wettelijke voorschriften uitgevoerde of achterwege gebleven verwerking van gegevens, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

(4) De Verwerker volgt de voor hem geldende bepalingen met betrekking tot gegevensbescherming op. Met name is het de Verwerker niet toegestaan om gegevens die niet algemeen toegankelijk zijn, onbevoegd te verwerken, voor opvraging door middel van geautomatiseerde procedures ter beschikking te houden, op te vragen of zichzelf of een ander toegang te verschaffen tot automatische verwerkingen of niet geautomatiseerde bestanden.

(5) Gedurende de gehele looptijd van de overeenkomst bewaakt de Verwerker regelmatig het toezicht op het opvolgen van de voorschriften met betrekking tot gegevensbescherming van deze overeenkomst evenals de instructies van de Verwerkingsverantwoordelijke.

(6) De Verwerker zorgt voor een correcte controle op de persoonsgegevens en toezicht door de verantwoordelijke toezichthoudende autoriteit. In het bijzonder informeert hij de toezichthoudende autoriteit op de juiste wijze, volledig en tijdig, staat hij testen en controlemaatregelen toe en voert hij opdrachten van de toezichthoudende autoriteit uit. De Verwerker informeert de Verwerkingsverantwoordelijke onverwijld, indien de toezichthoudende autoriteit zich in het kader van zijn controle op de persoonsgegevens en toezicht direct tot de Verwerker dient te wenden.

(7) De Verwerker zorgt ervoor, dat de Verwerkingsverantwoordelijke kan voldoen aan de wettelijke aanspraken van de betrokkenen op grond van art. 12 tot en met 22 AVG. De Verwerker dient de juiste technische en organisatorische maatregelen te nemen om de

Verwerkingsverantwoordelijke bij het voldoen aan betreffende eisen van de betrokkenen te ondersteunen. Met name dient de Verwerker de Verwerkingsverantwoordelijke te ondersteunen bij het inwilligen van de eisen van de betrokkenen met betrekking tot het wissen van hun persoonsgegevens conform art. 17 AVG. De Verwerker informeert de Verwerkingsverantwoordelijke onverwijld, indien een betrokkene zich voor informatie, correctie, verwijderen, beperking van de verwerking of overdracht van zijn gegevens direct tot de Verwerker dient te richten.

(8) De Verwerker verbindt zich ertoe de Verwerkingsverantwoordelijke bij te staan bij de te treffen maatregelen met betrekking tot de bescherming van persoonsgegevens conform art. 32 AVG, bij eventuele noodzakelijk meldingen aan de toezichthoudende autoriteit (art. 33 AVG) of bij het informeren van betrokkenen (art. 34 AVG), bij het uitvoeren van gegevensbeschermingseffectbeoordelingen (art. 35 AVG) alsmede bij het overleg met de toezichthoudende autoriteiten (art. 36 AVG). Met name bij het voldoen aan de meld- en informatieverplichtingen (art. 33, 34 AVG) zal de Verwerker de noodzakelijke informatie onverwijld ter beschikking stellen van de Verwerkingsverantwoordelijke.

10. Toezicht door Verwerkingsverantwoordelijke

(1) De Verwerkingsverantwoordelijke vormt zich een oordeel over naleving door Verwerker van deze voorwaarden en van de technische en organisatorische maatregelen van de Verwerker.

(2) De Verwerker verbindt zich ertoe de Verwerkingsverantwoordelijke alle informatie te verstrekken, die noodzakelijk is voor het uitvoeren van toezicht.

(3) In geval van gegronde twijfel aan de gepresenteerde documenten of bij een voorval met betrekking tot de gegevensbescherming kan Verwerkingsverantwoordelijke de naleving door onafhankelijke deskundigen laten vaststellen (audit), mits na tijdige melding en onder opgaaf van redenen, op de gebruikelijke bedrijfstijden en zonder de bedrijfsactiviteiten te storen. De kosten voor de uitvoering van de audit komen voor rekening van de Verwerkingsverantwoordelijke.

11. Inschakelen derden (sub-verwerkers)

(1) De Verwerker mag opdrachten geven aan andere Verwerkers (sub-verwerkers) zonder dat hiervoor voorafgaande separate toestemming van de Verwerkingsverantwoordelijke vereist is.

(2) De sub-verwerkers dienen zorgvuldig te worden geselecteerd, met name voor wat betreft de door hen getroffen technische en organisatorische maatregelen ter bescherming van de persoonsgegevens in de zin van art. 32 AVG. Ze dienen voorafgaand aan het verlenen van de opdracht en tijdens de looptijd van de overeenkomst te worden gecontroleerd op het voldoen aan de wettelijke en verdragsrechtelijke voorschriften met betrekking tot gegevensbescherming. Dit geldt ook voor de overeengekomen technische en organisatorische veiligheidsmaatregelen. De resultaten van deze controle moeten worden gedocumenteerd en op verzoek van de Verwerkingsverantwoordelijke worden overhandigd.

(3) Contractuele overeenkomsten tussen de Verwerker en de onderaannemer dienen te voldoen aan de vereisten met betrekking tot geheimhouding, gegevensbescherming en gegevensbeveiliging van deze overeenkomst. De overdracht van persoonsgegevens aan de onderaannemer is pas toegestaan op het moment dat de onderaannemer voldoet aan de verplichtingen op grond van art. 28 AVG.

(4) De Verwerker zorgt ervoor, dat de Verwerkingsverantwoordelijke de toezichtrechten overeenkomstig artikel 8 van deze overeenkomst ook heeft jegens sub-verwerkers, ingezet door de Verwerker.

(5) De Verwerkingsverantwoordelijke komt het recht toe, bij de Verwerker inzicht te verkrijgen in zijn overeenkomsten met sub-verwerkers.

12. Verwijdering en publicatie

(1) De Verwerker bewaart de persoonsgegevens slechts gedurende de tijd, die door de Verwerkingsverantwoordelijke wordt aangegeven. Voor zover er geen concrete instructies zijn, worden de persoonsgegevens slechts zolang bewaard, als noodzakelijk is voor het uitvoeren van de betreffende verwerking van persoonsgegevens op grond van deze overeenkomst.

(2) Op verzoek van de Verwerkingsverantwoordelijke alsmede na beëindiging van deze overeenkomst, zal de Verwerker alle persoonsgegevens die in verband staan met de verwerking van persoonsgegevens, alsmede alle kopieën daarvan, onverwijld doch uiterlijk binnen 14 dagen na verzoek en instructie van de Verwerkingsverantwoordelijke respectievelijk na beëindiging van de verwerking van persoonsgegevens wissen, met inachtneming van de van toepassing zijnde bepalingen met betrekking tot bescherming van persoonsgegevens.

(3) Documentatie, die dient ten bewijze van de volgens opdracht en correct uitgevoerde gegevensverwerking, moet door de Verwerker overeenkomstig de van toepassing zijnde wettelijke of bij overeenkomst bepaalde bewaartermijn na beëindiging van de overeenkomst worden bewaard. Hij kan dit, te zijner ontlasting, bij beëindiging van de overeenkomst, aan de Verwerkingsverantwoordelijke overhandigen.

(4) Op verzoek verstrekt de Verwerker aan de Verwerkingsverantwoordelijke schriftelijk bewijs van de verwijdering.

13. Aansprakelijkheid

(1) De Verwerker is jegens de Verwerkingsverantwoordelijke aansprakelijk voor directe schade die de Verwerker, zijn medewerkers sub-verwerkers veroorzaken bij het uitvoeren van de contractuele prestatie. Dit geldt niet, indien de Verwerker, zijn medewerkers of sub-verwerkers geen nalatigheid kan worden verweten. Dit geldt eveneens niet, indien de Verwerker, zijn medewerkers of sub-verwerkers geen invloed hadden op de veroorzaakte schade.

(2) Om te bewijzen dat hij, conform art. 82 lid 3 AVG, op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit, is de Verwerker bevoegd tot het openbaren van details van

instructies van de Verwerkingsverantwoordelijke en de uitgevoerde gegevensverwerking. De Verwerkingsverantwoordelijke is verplicht om de Verwerker zo goed mogelijk te steunen, zodat de Verwerker tegenover derden conform art. 82 lid 3 AVG kan bewijzen dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

(3) Verwerkingsverantwoordelijke is verantwoordelijk voor vergoeding van de schade, die een betrokkene lijdt wegens een op grond van de wet of ander voorschrift voor de gegevensbescherming ontoelaatbare of onjuiste gegevensverwerking dan wel gegevensverwerking die niet correct is binnen het kader van de verwerkingsverhouding.

14. Overige bepalingen

(1) Indien de EU-commissie of de verantwoordelijke toezichthoudende autoriteiten standaardclausules voor overeenkomsten tot verwerking van persoonsgegevens vast zouden leggen, overleggen de partijen voor zover nodig omtrent een mogelijke aanpassing van de overeenkomst aan de standaardclausules.

(2) Indien er sprake is van contradictie tussen de hoofdovereenkomst en deze overeenkomst, gaat deze overeenkomst voor, voor zover de contradictie betrekking heeft op de verwerking van persoonsgegevens.

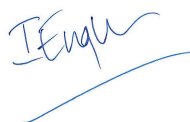
(3) Indien afzonderlijke of meerdere bepalingen van deze overeenkomst ongeldig zijn of worden, blijft de geldigheid van de overeenkomst voor het overige onaangetast. In de plaats van de ongeldige regeling(en) dient steeds een bepaling te worden opgenomen, die in zijn economische resultaat zo dicht mogelijk ligt bij hetgeen partijen beoogden met de ongeldige regeling. Dit geldt eveneens bij lacunes in de overeenkomst.

Plaats, datum



Handtekening

Amsterdam, 17 april 2018



Ilse Engwirda, Hogrefe Uitgevers, Verwerker

Naam, Organisatie, Verwerkingsverantwoordelijke

Technische en organisatorische maatregelen HTS 5 in het kader van de privacy

1. Fysieke toegangscontrole

Het voorkomen van fysieke toegang door ongeautoriseerde personen.

- Toegangspassen / Toegangscontrole transponders
- Toegangsautorisatie concepten
- Bewakingsapparatuur (video bewaking)
- Regulering omtrent de verschaffing van sleutels
- Toezicht op bezoekers door personeel
- Buiten kantooruren beveiliging door middel van een alarmsysteem
- Aangewezen (veiligheids)gebieden met gecontroleerde toegang
- Entreebeveiliging
- Veiligheidsmaatregelen voor het gebouw en terrein (alarmsysteem)
- Beveiligde toegang tot IT- en computercentra
- Datacentra ondergebracht in afsluitbare ruimten
- Back-up data (bijv. CD's) opgeslagen in een kluis met beperkte toegang

2. Toegangscontrole van het systeem

Toegang van ongeautoriseerde personen tot gegevensverwerkingsystemen moet voorkomen worden.

- Encryptie van netwerken
- Afsluitbare dataverwerkingsystemen
- Beveiliging van computerwerkplekken
- Regulatie van gebruikersautorisatie
- Gebruik van individuele paswoorden
- Automatisch blokkeren van gebruikersaccounts na het invoeren meerdere foutieve paswoorden
- Automatische, met paswoord-beschermd, schermbeveiliging van computers na inactiviteit
- Wachtwoord beleid met minimale eisen voor paswoord complexiteit:
 - Op zijn minst 8 tekens
 - Op zijn minst gebruik van twee van de volgende: Hoofd- en kleine letters, speciale tekens, cijfers
- Processen voor het toewijzen van toegangsrechten voor nieuwe werknemers
- Processen voor het terugtrekken van toegangsrechten van werknemers die van afdeling wisselen
- Processen voor het terugtrekken van toegangsrechten van werknemers die uit dienst treden
- De verplichting om te voldoen aan geheimhoudingsvoorzieningen voor gegevens op grond van de AVG
- Vastleggen en analyseren van systeemgebruik
- Vertrouwelijke vernietiging van gegevens

3. Toegangscontrole voor gegevens

Activiteiten in gegevenssystemen door personen zonder toestemming moet voorkomen worden.

- Specificatie van toegangsrechten, autorisatie concepten
- Definiëren van toestemmingen om gegevens toe te voegen, te veranderen of te verwijderen
- Scheiding van organisatorische en technische procedures voor het verlenen van toestemmingen
- Aanwezigheid van een concept voor het gebruik en toewijzing van harde schijven
- Een plan voor het herstellen van gegevens van back-ups
- Controleren van toegang
- Vastleggen van datatoegang

4. Controle van gegevensverschaffing

De overdracht van persoonlijke gegevens moet gereguleerd worden: elektronische overdracht, gegevenstransport en het monitoren daarvan.

- Ontvangt de leverancier gegevens van de cliënt?
- Welke middelen voor gegevensoverdracht zijn er tussen cliënt en leverancier?
 - Uitwisseling van gegevens via een https verbinding
- Er is een autorisatieconcept
- Verwijderen van gegevens: veilige manieren voor het verwijderen van data van mediadragers
- Afvoer van papier: er zijn er afgesloten containers beschikbaar

5. Invoercontrole

Het updaten en het beheer van gegevens moet gedocumenteerd worden en traceerbaar zijn.

- Identificatie/labels van ingevoerde gegevens
- Definities van de verantwoordelijkheden omtrent gegevensinvoer
- Vastleggen van invoer/verwijdering
- Er bestaat er een procedurele-, programma- en workfloworganisatie
- Controle van gegevensinvoer
- De verplichting om te voldoen aan de wet bescherming persoonsgegevens
- Controle over de toegangspermissies

6. Taakcontrole

Verzekerd moet worden dat de gegevens die verwerkt worden door serviceverleners namens de leverancier (subcontractoren) alleen worden verwerkt zoals voorgeschreven door de leverancier.

- Contracten dienen opgemaakt te worden overeenkomstig met de wetgeving
- Gecentraliseerde registratie van bestaande serviceverleners (geünificeerd contractmanagement)
- Inspecties ter plekke bij de serviceverlener voor aanvang van de start van het contract
- Regelmatige inspecties ter plekke bij de serviceverlener gedurende de looptijd van het contract
- Beoordelen van het gegevensbeveiligingsplan van de serviceverlener
- Het toetsen van de bestaande gegevensbeveiligingscertificaten van de serviceverlener
- Verschaffen van instructies aan de serviceverlener voor verbeteringen in de gegevensbeveiliging

7. Beschikbaarheidscontrole

Gegevens moeten beveiligd worden tegen onopzettelijk verlies of vernietiging.

- Data back-up plannen
- Toegangsrechten tot serverruimtes beperkt tot het noodzakelijk personeel
- Installatie van brandalarmen in de serverruimtes
- Airconditioning van de serverruimtes
- Opslag van back-up systemen in aparte panden en op brandveilige afdelingen
- Opslag van archiefgegevens onder geschikte omstandigheden (air conditioning, beveiliging, etc.)
- CO₂ brandblussers in nabijheid van de serverruimtes
- Implementatie van plannen omtrent gegevensbescherming en back-ups
- Opslag van data in datakasten en kluisen
- Noodstroomvoorzieningen
- Wordt ongeautoriseerde gebruikers de toegang geweigerd?

8. Scheidingscontrole

Gegevens die verzameld worden voor verschillende doeleinden moeten gescheiden verwerkt worden.

- Scheiding van klanten
- Er is een autorisatieconcept voor de gescheiden verwerking van gegevens van de cliënt en gegevens van andere klanten
- Scheiding van ontwikkelings-, test- en livesystemen