Verwerkersovereenkomst

tussen

……

- de controleur - hierna verwezen als de klant

en

ALSO Nederland B.V.

- de verwerker - hierna verwezen als de leverancier

1. Onderwerp en duur van de bestelling of overeenkomst

(1) Onderwerp

Het onderwerp van de bestelling of overeenkomst betreffende de verwerking van gegevens is de uitvoering van de volgende diensten of opdrachten door de leverancier: technische ondersteuning, bestellingverwerking, IT-diensten, klantendienst, clouddiensten.

(2) Duur

De duur van deze bestelling (termijn) stemt overeen met de termijn van de dienstovereenkomst binnen het kader van het respectieve product, dienst, aankoop en/of arbeidscontracten.

2. Specificatie van de bestelling- of overeenkomst-details

(1) Aard en doel van de bedoelde verwerking van gegevens

Gedetailleerde beschrijving van het onderwerp met betrekking tot de aard en het doel van de diensten geleverd door de leverancier:

Aard van de gegevens	Doel van de verwerking	Gegevens onderwerp
Persoonsgegevens naam, adres, contactgegevens, details van bankrekening.	Verwerking van bestellingen, technische steun, IT-diensten, klantendiensten, clouddiensten.	Tewerkgestelden van gegevenscontroleur, zakenpartner, klant, verkoper, geïnteresseerde personen.

De uitvoering van de contractueel aanvaarde verwerking van gegevens zal worden gedaan uitsluitend binnen een Lidstaat van de Europese Unie (EU), binnen een Lidstaat van de Europese Economische Zone (EEZ) of in een land dat opgenomen is in de beslissing van adequaatheid van de Europese Commissie. Elke en alle gegevenstransfer(s) naar een staat die geen Lidstaat is noch van de EU noch van de EEZ vereist de voorafgaande toestemming van de klant en zal slechts gebeuren indien de specifieke voorwaarden van artikel 44 en volgende van de AVG worden vervuld. Het adequate niveau van bescherming in een land dat geen lid is van de EU dient te worden gegarandeerd door standaard contractuele clausules van de EU. (Art 46 Abs 2 lid c en d EU-AVG)

(2) Type gegevens

Het onderwerp van de verwerking van persoonsgegevens omvat de volgende gegevenstypes/categorieën: persoonlijke mastergegevens (persoonlijke sleutelgegevens), contactgegevens, contract sleutelgegevens (contractuele/wettige relaties, contractueel of productbelang), klantenhistoriek, contract facturatie en betalingsgegevens, openbaar gemaakte Informatie (van derde partijen, vb. Krediet-Agenturen of openbare directories), informatie betreffende systeemconfiguratie en klantenomgeving.

(3) Categorieën van gegevens onderwerpen

De categorieën van gegevens onderwerpen omvatten: tewerkgestelden van de gegevenscontroleur, zakenpartner, klanten, potentiële klanten, inschrijvers, tewerkgestelden, leveranciers, contactpersonen.

3. Technische en organisatorische maatregelen

(1) Vóór het begin van de verwerking, zal de leverancier de uitvoering documenteren van de nodige technische en organisatorische maatregelen [Details in bijvoegsel 1], uitgestippeld vóór de toekenning van de bestelling of overeenkomst, specifiek met betrekking tot de gedetailleerde uitvoering van de overeenkomst, en zal deze gedocumenteerde maatregelen voorstellen aan de klant voor inspectie. Na aanvaarding door de klant, worden de gedocumenteerde maatregelen de basis van de overeenkomst. Voor zover de inspectie/audit door de klant de noodzaak aantoont van wijzigingen, zullen dergelijke wijzigingen worden doorgevoerd in onderlinge overeenstemming.

(2) De Leverancier zal de veiligheid instellen overeenkomstig artikel 28 paragraaf 3 punt c, en artikel 32 AVG (Algemene Verordening Gegevensbescherming) in het bijzonder in samenhang met artikel 5 paragraaf 1, en paragraaf 2 AVG. De te nemen maatregelen zijn maatregelen voor gegevensbeveiliging en maatregelen die een beschermingsniveau verzekeren aangepast aan het risico met betrekking tot vertrouwelijkheid, integriteit, beschikbaarheid en herstellingsvermogen van de systemen. Het technische peil, de kosten van implementatie, de aard, reikwijdte en doeleinden van de verwerking alsmede de waarschijnlijkheid van gebeuren en de ernst van het risico voor de rechten en vrijheden van natuurlijke personen in de zin van artikel 32 paragraaf 1 AVG moeten in rekening genomen worden. [Details in bijvoegsel 1]

(3) De technische en organisatorische maatregelen zijn onderworpen aan technische vooruitgang en verdere ontwikkeling. In dit verband, is het de leverancier toegelaten om alternatieve aangepaste maatregelen te treffen. In dit geval, mag het veiligheidsniveau van de bepaalde maatregelen niet verminderd worden. Substantiële wijzigingen dienen te worden gedocumenteerd.

4. Correctie, beperking en wissen van gegevens

(1) De leverancier mag niet op eigen initiatief de verwerking van gegevens corrigeren, wissen of beperken die worden verwerkt namens de klant, maar alleen op uitdrukkelijke instructie van de klant. Voor zover de persoon/ het bedrijf van de gegevens de klant rechtstreeks contacteert betreffende een correctie, verwijdering of beperking van de verwerking, zal de leverancier onmiddellijk de aanvraag van de gegevens doorsturen naar de klant.

(2) Voor zover dit is inbegrepen in de draagwijdte van diensten, de uitwispolitiek, het 'recht om vergeten te worden', rectificatie, gegevensdraagbaarheid en -toegang zullen worden verzekerd door de leverancier overeenkomstig de gedocumenteerde instructies van de klant zonder onnodig uitstel.

5. Kwaliteitsverzekering en andere verplichtingen van de Leverancier

Behalve het naleven van de regels opgesteld in deze bestelling of overeenkomst, zal de leverancier de statutaire vereisten vervullen waarnaar verwezen wordt in artikels 28 tot en met 33 AVG; tegelijkertijd, verzekert de leverancier, in het bijzonder, de naleving van de volgende vereisten:

a) Aangeduide Functionaris Gegevensbescherming (Data Protection Officer), die zijn/haar taken vervult in overeenstemming met de artikelen 38 en 39 AVG.
   - ☐ De klant zal worden ingelicht over zijn/haar contactdetails met het oog op direct contact. De klant zal onmiddellijk worden ingelicht over enige verandering van Functionaris Gegevensbescherming (Data Protection Officer).
   - ☐ De leverancier heeft aangeduid meneer Jens Hagen, ALSO Nederland, +31(0)24 3333 250, privacy.nl@also.com als Functionaris Gegevensbescherming (Data Protection Officer). De klant zal onmiddellijk worden ingelicht over enige verandering van Functionaris Gegevensbescherming (Data Protection Officer).
   - ☐ Zijn/haar huidige contactdetails zijn altijd beschikbaar en makkelijk toegankelijk op de website van de leverancier.

b) Vertrouwelijkheid in overeenstemming met artikel 28 paragraaf 3 zin 2 punt b, artikels 29 en 32 paragraaf 4 AVG. De leverancier vertrouwt slechts die tewerkgestelden toe met de gegevensverwerking beschreven in deze overeenkomst en die gebonden zijn geweest aan

vertrouwelijkheid en voorheen vertrouwd werden gemaakt met de gegevensbeschermingsvoorwaarden die belangrijk zijn voor dit werk. De Leverancier en eender welke persoon die handelt onder zijn/haar gezag en die toegang heeft tot persoonsgegevens, zal deze gegevens niet verwerken tenzij in opdracht van de klant, wat de bevoegdheden inhoudt verleend in deze overeenkomst, tenzij dit dient te gebeuren om wettelijke redenen.

c) De implementatie van en het overeenstemmen met alle technische en organisatorische maatregelen nodig voor deze bestelling of overeenkomst in overeenstemming met artikel 28 paragraaf 3 zin 2 punt c, artikel 32 AVG [details in bijvoegsel 1].
d) De klant en de leverancier zullen samenwerken, op verzoek, met de toezichthoudende autoriteit in de uitvoering van zijn/hun opdrachten.
e) De klant zal onmiddellijk worden ingelicht over enige inspectie en maatregelen uitgevoerd door de controlerende overheid, voor zover als deze betrekking hebben op deze bestelling of deze overeenkomst. Dit is tevens geldig voor zover de leverancier onder instructie staat of deel is van een onderzoek door een bevoegde overheid in verband met overtredingen op eender welke burgerlijke of strafrechtelijke wet, of administratieve regel of regeling betreffende de verwerking van persoonsgegevens in verband met de verwerking van deze bestelling of overeenkomst.
f) Voor zover de klant onderworpen is aan een inspectie door de toezichthoudende autoriteit, een administratief of samenvattend misdrijf of strafrechtelijke procedure, een aansprakelijkheidsvordering door een gegevens onderwerp of door een derde partij of enige eis in verband met de bestelling of de overeenkomst van gegevensverwerking door de leverancier, zal de leverancier alle mogelijk inspanningen leveren om de klant te ondersteunen.
g) De leverancier zal periodiek de interne processen controleren en de technische en organisatorische maatregelen om te verzekeren dat de verwerking binnen deze zone in overeenstemming is met de vereisten van de wet op toepasbare gegevensbescherming en de bescherming van de rechten van het gegevens onderwerp.
h) De controleerbaarheid van de technische en organisatorische maatregelen gevoerd door de klant als onderdeel van de toezichthoudende bevoegdheden van de klant zoals vermeld in item 7 van deze overeenkomst.

6. Onderaanneming

(1) Onderaanneming in de zin van deze overeenkomst dient opgevat te worden als diensten die rechtstreeks verband houden met de levering van de hoofddienst. Dit omvat geen aanvullende diensten, zoals diensten van telecommunicatie, post/transportdiensten, onderhoud en gebruikersondersteuningsdiensten of de verwijdering van gegevensdragers, evenals andere diensten om de vertrouwelijkheid, beschikbaarheid, integriteit en herstelvermogen te verzekeren van de hardware en de software van de gegevensverwerkende uitrusting. De leverancier zal, niettemin, verplicht zijn om aangepaste en wettig bindende contractuele akkoorden te sluiten en om de gepaste inspectiemaatregelen te treffen om de gegevensbeveiliging en de gegevensbescherming te verzekeren van de gegevens van de klant, zelfs in het geval van bijkomende diensten die in onderaanneming zijn gegeven.

(2) Bestellingen mogen worden doorgegeven aan onderaannemers binnen het kader van de activiteiten die zijn overeengekomen in de bestelling. De onderaannemers zullen worden meegedeeld aan de klant op verzoek. De leverancier zal zorgvuldig de onderaannemers selecteren overeenkomstig hun geschiktheid, in het bijzonder betreffende de vereisten van de EU-AVG, en zal hen regelmatig controleren. Bovendien, zal de leverancier met de onderaannemers een overeenkomst aangaan over de bestellingverwerking in overeenstemming met deze overeenkomst.
(3) De transfer van persoonsgegevens van de klant naar de onderaannemer en de aanvang van de gegevensverwerking door de onderaannemer zal slechts worden aangegaan na vervulling van alle vereisten.
(4) Indien de onderaannemer de overeengekomen dienst buiten de EU uitvoert, zal de leverancier de naleving verzekeren van de Europese privacy verordening algemene verordening gegevensbescherming door middel van passende maatregelen. Hetzelfde geldt indien dienstenleveranciers worden gebruikt binnen de betekenis van paragraaf 1 zin 2.
(5) Verdere onderaanneming door de onderaannemer vereist het akkoord van de leverancier (op zijn minst in tekstvorm). Alle contractuele voorschriften in de contractenketting moeten tevens opgelegd worden aan de andere onderaannemer.

7. Controlerende machten van de Klant

(1) De klant heeft het recht, na consultatie met de leverancier, inspecties uit te voeren door een persoon die gebonden is door beroepsgeheim of om deze te laten uitvoeren door een auditeur die moet worden benoemd in elk individueel geval. Deze heeft het recht om zichzelf te overtuigen van de naleving van deze overeenkomst door middel van steekproeven, die gewoonlijk tijdig moeten worden aangekondigd.
(2) De leverancier zal ervoor zorgen dat de klant in staat is om de naleving van de verplichtingen van de leverancier na te gaan in overeenkomst met artikel 28 AVG**.** De leverancier geeft de klant de noodzakelijke informatie op aanvraag, en, in het bijzonder, bewijst de uitvoering van de technische en organisatorische maatregelen.
(3) Het bewijs van dergelijke maatregelen, die niet alleen betrekking hebben op de bestelling of de overeenkomst, mag worden geleverd door vervulling van de aangenomen gedragscodes volgens artikel 40 AVG; certificatie volgens een aangenomen certificatieprocedure overeenkomstig artikel 42 AVG; geldige certificatie, rapporten of uittreksels van huidige auditeurs uit rapporten geleverd door onafhankelijke instanties (vb. auditeur, Functionaris Gegevensbescherming (Data Protection Officer), IT-beveiligingsdepartement, auditeur voor gegevensbescherming, kwaliteitsauditeur). Een gepaste certificatie door IT-beveiliging of gegevensbeschermingsauditing.
(4) De leverancier kan een vergoeding eisen voor het mogelijk maken van de klant-inspecties.

8. Communicatie in het geval van overtredingen door de leverancier

(1) De leverancier zal de klant bijstaan in het naleven van de verplichtingen betreffende de veiligheid van de persoonsgegevens, door het rapporteren van vereisten voor gegevensschendingen, gegevensbescherming impactraadgevingen en voorafgaande consultaties, waarnaar wordt verwezen in artikels 32 tot 36 van de AVG. Deze omvatten:

a) Het verzekeren van een aangepast beschermingsniveau doorheen technische en organisatorische maatregelen die rekening houden met de omstandigheden en doeleinden van de verwerking alsmede de geprojecteerde waarschijnlijkheid en ernst van een mogelijke overtreding van de wet ten gevolge van kwetsbaarheden en die een onmiddellijke detectie toelaten van relevante schendingsgebeurtenissen.
b) De verplichting om onmiddellijk aan de Klant een inbreuk op persoonsgegevens te rapporteren.
c) De plicht om de klant bij te staan in verband met de verplichting van de klant om informatie te verschaffen aan het betrokken gegevens onderwerp en om onmiddellijk aan de klant alle relevante informatie te bezorgen in dit verband.
d) De klant ondersteunen met zijn raadgevingen op de gegevensbescherming impact.
e) De klant ondersteunen betreffende de voorafgaande consultatie van de toezichthoudende overheid.

(2) De leverancier kan vergoeding eisen voor ondersteuningsdiensten die niet inbegrepen zijn in de beschrijving van de diensten en die niet te wijten zijn aan fouten vanwege de leverancier.

9. Gezag van de klant om instructies uit te vaardigen

(1) De klant zal onmiddellijk mondelinge instructies bevestigen (ten minste in tekstvorm).

(2) De leverancier zal de klant onmiddellijk inlichten indien hij oordeelt dat een instructie de AVG overtreedt. De leverancier heeft alsnog het recht de uitvoering op te schorten van de relevante instructies totdat de Klant deze bevestigt of wijzigt.

10. Uitwissen en terugbezorgen van persoonsgegevens

(1) Kopieën of duplicaten van de gegevens zullen nooit worden gecreëerd zonder medeweten van de Klant, met uitzondering van back-up Kopieën voor zover deze noodzakelijk zijn om een ordelijke gegevensverwerking te garanderen, evenals gegevens die vereist zijn om te voldoen aan de wettelijke vereisten om gegevens te bewaren.

(2) Na beëindiging van de gecontracteerde taak, of eerder op verzoek van de klant, ten laatste bij het beëindigen van de dienstenovereenkomst, zal de leverancier alle documenten, verwerkings- en gebruiksresultaten, en gegevenssets overhandigen aan de klant of -mits voorafgaandelijke overeenkomst - vernietigen, die in verband staan met de overeenkomst, en die in zijn bezit zijn gekomen, op een wijze die conform is met de gegevensbescherming. Hetzelfde geldt voor elk verbonden test, afval, overbodig en afgedankt materiaal. De registratie van de vernietiging of vernietiging zal op verzoek worden overgedragen.

(3) Documentatie die gebruikt wordt voor het aantonen van ordelijke gegevensverwerking in overeenstemming met de bestelling of de overeenkomst, zal worden bewaard na de contractduur door de leverancier in overeenstemming met de respectievelijke bewaartermijnen. Deze kan dergelijke documentatie overhandigen aan de Klant op het einde van de contractduur om de Leverancier te ontslaan van zijn contractuele verplichting.

Klant: _____	**Leverancier:_____**
_____ (plaats / datum)	_____ (plaats / datum)
_____ (Handtekening / stempel)	_____ Handtekening / stempel)
_____ (Naam / functie van de ondergetekende)	_____ (naam / functie van de ondergetekende)

Bijvoegsel 1 Technische en organisatorische maatregelen

Maatschappij: ALSO Nederland
Plaats: Nijmegen en Nieuwegein

1.Vertrouwelijkheid (Art. 32 Paragraaf 1 Punt B EU-AGV)
Controle over Fysieke Toegang
Geen fysieke toegang zonder toelating tot de systemen van gegevensverwerking.

Doeleinden: Deze maatregel dient om te garanderen dat geen onbevoegde persoon fysieke toegang heeft tot de systemen van gegevensverwerking, die persoonlijke gegevens verwerken.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	Maatregel
x	x	Systeem van Toegangscontrole (ID-kaartlezer, Systeem met toetsvergrendeling)
x	x	Maatregelen voor gebouwbeveiliging veiligheid
x	x	Hekwerk
x	x	Veiligheidsdeuren, Veiligheidsvensters
		Rooster voor vensters en deuren
	x	Beveiliging, poortwachter
x	x	Controle van personen, Receptie
x		Documentatie van bezoekers
x	x	Videobewaking
x	x	Foto-elektrische, Bewegingssensoren
x	x	Deurveiligheid (Vergrendelingssysteem, Slotcode, Biometrische toegangscontrole, Veiligheidssleutels)
x	x	Fysieke sleutelcontrole / Documentatie van de fysieke-sleutelverdeling
x	x	Veiligheid vereist buiten de kantooruren door de fabrieksveiligheidsdienst en/of alarmsysteem.
x	x	Richtlijn voor gasten / bezoekers / externe personen
		ID-kaarten van bezoekers
x	x	Speciale veiligheidsmaatregelen voor server-ruimtes.
		Werknemers identiteitskaarten en autorisatiekaarten (met verplichting)
x	x	Afgebakende zones
x	x	Zorgvuldige selectie van schoonmaakpersoneel

Toegangscontrole:
Geen toegang zonder toelating tot de systemen van gegevensverwerking.

Doeleinden: Deze maatregel zou moeten garanderen dat alleen bevoegde personen toegang bekomen tot de gegevensverwerkingssystemen en slechts door hen kunnen gebruikt worden.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	Maatregel
x	x	Persoonlijke en individuele aanmelding van gebruiker bij het inloggen van gegevensverwerkingssystemen en maatschappij-netwerk.
x	x	Wachtwoordpolitiek
		Multi-Factor Authenticatie
x	x	BIOS-Wachtwoordbescherming
x	x	Bijkomend systeem-log-in voor bepaalde toepassingen
x	x	Toewijzing van bepaalde klanten uitsluitend voor bepaalde functies.
x	x	Automatische afsluiting van klanten wegens inactiviteit zonder interactie van gebruikers. (Wachtwoord beschermde screensaver of automatische breuktolerantie)
		Elektronische documentatie van wachtwoorden (geen gebruikerswachtwoorden) en encryptie van deze documentatie om een niet-toegelaten toegang te voorkomen
		Individuele chipkaarten
		Biometrische login optie
	x	Kluisjes
		Ontmantelen van external-interfaces (vb.: USB)
x	x	Gebruik van Intrusie-Detectie-Systemen
x	x	Gebruik van Anti-Virus-Software/Anti-Malware Software
x	x	Gebruik van Firewalls
x	x	Network-Access-Controle (NAC)
x	x	Toewijzing van gebruikersprofielen voor IT-systemen
x	x	Gebruik van VPN-technologie
x	x	Gebruik van encryptie-mechanismen voor bestanden
x	x	Encryptie van mobiele informatiedragers

x	x	Informatiedrager in mobiele apparaten (Notebooks, Smartphones, enz.)
		Externe gegevensdragers (USB-sticks, Geheugenkaarten, enz.)
x	x	Geen instrumenten zonder wachtwoord of afsluitcode met toegang tot maatschappijgegevens.
		Verplichting van gebruikers voor gegevensbescherming. Art. 28 Paragraaf 3 Punt B EU-AGV
x	x	Voldoende vernietiging van gegevensdragers.
x	x	Richtlijn voor privaat gebruik van de maatschappij-apparaten.
x	x	Richtlijn voor BYOD (Bring your own device)
x	x	Richtlijn voor mobiele werker (vb. Notebook)

Controle over Gegevens-Toegang

Geen ongeoorloofd lezen, kopiëren, wijzigen of uitwissen van persoonsgegevens binnen een systeem van gegevensverwerking.
Voorbeeld: Concept van toelating, rechten van toegang gebaseerd op behoefte, loggen voor toegang.

Doeleinden: Deze maatregelen moeten garanderen dat slechts bevoegde personen toegang krijgen tot het systeem van gegevensverwerking en dat de toegang tot persoonsgegevens beperkt blijft tot de toegangsrechten van de gebruiker. Persoonsgegevens kunnen niet verwerkt of gebruikt worden en na opslag kunnen de gegevens niet worden gelezen zonder toelating, noch gekopieerd, gewijzigd of uitgewist.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	**Maatregel**
x	x	Administratie van rechten en rollen
x	x	Gedifferentieerde toegangsrechten
x	x	Profielen
x	x	Rollen
x	x	Documentatie van toegangsrechten
x	x	Aannemingsprocedure voor toegangsrechten
		Nabespreking / loggen
		Inspectie
		Encryptie van CD/DVD-ROM, externe aandrijvingen van Notebooks (vb. Door operatiesysteem, Safeguard, PGP, Veracrypt, enz.)
x	x	4 ogen principe wordt toegepast
x	x	Segregatie van Verplichtingen
x	x	Taakverwante toegangsprofielen
x	x	Verlagen van aantal personen met administratieve privilegies tot een minimum
x	x	Verwijderen van gegevens-media vóór hergebruik
x	x	Gebruik van dienstverlener voor documentendestructie
x	x	Veilige bewaring van gegevensmedia
x	x	Correcte vernietiging van gegevensmedia
x	x	Loggen van destructie
		Regelmatige audit van toegangsrechten
x	x	Registratie en analyse van log-bestanden (al dan niet succesvolle pogingen van login)
		Richtlijn tot het geven van een pseudoniem van de persoonsgegevens
x	x	Afwezigheidsregeling /richtlijn (Toegang tot gegevens van afwezige tewerkgestelde)

Scheidingscontrole:
Gescheiden verwerking van de gegevens, die worden verzameld voor verschillende doeleinden. (Voorbeeld Sandboxing, Multi-cliënt capable)

Doeleinden: Doelgerichte verwerking van persoonsgegevens dient te worden toegepast op een technisch niveau. Gegevens die verzameld worden voor verschillende doeleinden dienen apart te worden verwerkt.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	**Maatregel**
x	x	Gescheiden Systemen
x	x	Gescheiden databases
x	x	Rechten van Toegangscontrole
x	x	Scheiding door de Rechten op Toegangscontrole

Pseudoniem-gebruik: (Artikel 32 Paragraaf 1 Punt a EU-AGV, Artikel 25 Paragraaf 1 EU-AGV)
De verwerking van persoonsgegevens gebeurt op een dergelijke wijze dat, zonder bijkomende informatie, deze gegevens niet kunnen worden toegeschreven aan een specifieke persoon, in zoverre de bijkomende informatie apart wordt gestockeerd en gebonden aan technische en organisatorische maatregelen.

2. Integriteit (Art. 32 Paragraaf 1 Punt B EU-AGV)

Transfer-controle

Geen niet toegelaten lezen, kopiëren, wijzigen of verwijderen gedurende het transport of de elektronische transmissie. (Encryptie, VPN, Handtekening, enz.)

Doeleinden: Deze maatregelen dienen te waarborgen dat de gegevensmedia niet worden gelezen, gekopieerd, gewijzigd of uitgewist tijdens het transport. De maatregelen moeten controleren en ontdekken waar persoonsgegevens worden getransfereerd of voorbereid voor transfers. Controle van transport en gegevensmedia wordt gecombineerd in Transfer control

Aangenomen maatregelen:

Nijmegen	Nieuwegein	**Maatregel**
		Email-Encryptie
		Encryptie van CD/DVD-ROM, externe aandrijvingen van Notebooks (vb. Door operatiesysteem, Safeguard, PGP, Veracrypt, enz.)
x	x	Encryptie-verbindingen (VPN)
x	x	Loggen (Auditlogging)
		Transportvergrendeling van gegevensmedia en transport-containers
x	x	Beveiligde WLAN
x	x	SSL-Encryptie voor Web-Toegang
		Handleiding voor Gegevensdestructie
x	x	Correcte vernietiging van gegevensmedia
x	x	Zorgvuldige selectie van personeel indien manueel transport
		Transport via pseudonieme of anonieme weg
		Register van regelmatige gegevenstransmissies
x	x	Geen Software die persoonlijke gegevens doorgeeft zonder contractuele clausules aan een vreemde server. (Facebook, WhatsApp…)
x	x	Procedures om kwaadaardige programmatuur te ontdekken en beschermen.
x	x	Beveiligde toegang tot gegevenscentrum
		Beheer van gegevensmedium
		Aparte opslag voor vertrouwelijke Gegevensmedia
x	x	Vernietiging van gegevensmedia (vb. valse afdrukken, magneetschijven, enz.
		Uitwissen van Gegevensmedia vooraleer uit te wisselen
		Veilig afdrukken

Input controle:
Bepalen of en door wie gegevens worden ingebracht, gewijzigd of verwijderd in de gegevensverwerkingssystemen, vb. loggen, documentenbeheer

Doeleinden: Deze maatregelen zijn ontworpen om de controleerbaarheid van een verwerkingsoperatie te waarborgen (invoer, wijziging, verwijdering) van persoonsgegevens. Dit betekent dat de auteur, inhoud en tijd van gegevensopslag dienen bepaald te worden.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	**Maatregel**
x	x	Toegangsrechten /Concept van Toelating
x	x	Systeemzijde loggen
		Veiligheids- of loggingprogramma
x	x	Functionele verantwoordelijkheden
		4 ogen principe
x	x	Verplichting tot gegevensbescherming

3. Integriteit en veerkracht (Art. 32 Paragraaf 1 Punt B EU-AGV)
Controle van Beschikbaarheid
Bescherming tegen accidentele of bewuste vernietiging of verlies, bv Concept van Back-up (online/offline, onsite/offsite), niet-onderbreekbare stroomvoorziening, virusbescherming, firewall, rapporterende kanalen, rampenplannen.

Doeleinden: Er dient gegarandeerd te worden dat de persoonsgegevens niet accidenteel worden vernietigd en beschermd worden tegen verlies. Er dient gegarandeerd te worden dat de gebruikte systemen kunnen hersteld worden in geval van een verkeerde werking.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	**Maatregel**
x	x	Strategie van back-up
x	x	Opslagconcept voor Back-ups
x		Serverskamers niet onder water dragende systemen/inrichtingen
x	x	Niet uitschakelbare stroomvoorziening (batterij, diesel)
x	x	Temperatuur- en vochtigheidscontrole in de server-ruimtes
x	x	Virus-/bedreigingsbescherming, firewall
x	x	Air-conditioning in IT-kamers
x	x	Brand- en blusbescherming (systemen van brandalarm, blusuitrustingen)
x	x	Alarmsystemen
		Aangepaste archiefkamers
x	x	Noodplan
x	x	Rampenoefening
		Falings- en herstelplannen
x	x	Redundante Gegevenscentrum (in-huis/extern)
x	x	Redundante Gegevensconnectie van Gegevenscentrum met bedrijfsnetwerk
x	x	Redundante Hardware
x	x	Datamonitoring

4. Procedure voor regelmatig nazicht, benchmark en evaluatie (Art. 32 Paragraaf 1 Punt d EU-AGV; Art. 25 Paragraaf 1 EU-AGV)

Controle van bestelling:
Geen gegevensverwerking binnen in de zin van Art. 28 EU-AGV zonder overeenkomstige instructies van de contracterende autoriteit, vb. duidelijk contractontwerp, geformaliseerde bestellingbeheer, strikte selectie van de dienstverlener, verplichting om vooraf te overtuigen, opvolgingscontroles.

Doeleinden: De aannemer dient te verzekeren dat de gegevens die moeten worden verwerkt in de bestelling slechts zullen worden verwerkt overeenstemmend met de instructies van de klant. Onrechtstreeks verbonden hiermee, is de verplichting van de klant om instructies te geven aan de aannemer.

Aangenomen maatregelen:

Nijmegen	Nieuwegein	**Maatregel**
x	x	Geschreven contract voor verwerking van bestellinggegevens overeenkomstig EU-AGV met regelingen over de rechten en verplichtingen van de aannemer en opdrachtgever.
x	x	Opleiding van alle bevoegde tewerkgestelden
x	x	Regelmatige opvolging van de opleidingscursussen
x	x	Verplichting van de tewerkgestelden om de vertrouwelijkheid te bewaren en de geheimhouding van gegevens.
x	x	Regelmatige audits van gegevensbescherming door de verantwoordelijke voor de bescherming van de bedrijfsgegevens
x	x	Aanduiding van contactpersonen en verantwoordelijke projectbeheerders voor de specifieke bestelling
x	x	Zorgvuldige selectie van de aannemer