Bijvoegsel 1 Technische en organisatorische maatregelen

Maatschappij: ALSO International
Plaats: Wijchen (Warehouse), Nijmegen (Netherlands), Krefeld (Germany)
Amersham (United Kingdom)

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:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maatregel
x	x			Systeem van Toegangscontrole (ID-kaartlezer, Systeem met toetsvergrendeling)
x	x	x	x	Maatregelen voor gebouwbeveiliging veiligheid
x	x			Hekwerk
x	x	x	x	Veiligheidsdeuren, Veiligheidsvensters
				Rooster voor vensters en deuren
				Beveiliging, poortwachter
				Controle van personen, Receptie
	x			Documentatie van bezoekers
x	x			Videobewaking
x	x	x	x	Foto-elektrische, Bewegingssensoren
x	x			Deurveiligheid (Vergrendelingssysteem, Slotcode, Biometrische toegangscontrole, Veiligheidssleutels)
x	x	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
NVT	x	NVT	NVT	Speciale veiligheidsmaatregelen voor server-ruimtes.
				Werknemers identiteitskaarten en autorisatiekaarten (met verplichting)
x	x	x	x	Afgebakende zones
x	x	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:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maatregel**
x	x	x	x	Persoonlijke en individuele aanmelding van gebruiker bij het inloggen van gegevensverwerkingssystemen en maatschappij-netwerk.
x	x	x	x	Wachtwoordpolitiek
				Multi-Factor Authenticatie
x	x			BIOS-Wachtwoordbescherming
x	x	x	x	Bijkomend systeem-log-in voor bepaalde toepassingen
x	x	x	x	Toewijzing van bepaalde klanten uitsluitend voor bepaalde functies.
x	x	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	x	x	Gebruik van Intrusie-Detectie-Systemen
x	x	x	x	Gebruik van Anti-Virus-Software/Anti-Malware Software
x	x	x	x	Gebruik van Firewalls
x	x	x	x	Network-Access-Controle (NAC)
x	x	x	x	Toewijzing van gebruikersprofielen voor IT-systemen
x	x	x	x	Gebruik van VPN-technologie

x	x	x	x	Gebruik van encryptie-mechanismen voor bestanden
x	x	x	x	Encryptie van mobiele informatiedragers
x	x	x	x	Informatiedrager in mobiele apparaten (Notebooks, Smartphones, enz.)
				Externe gegevensdragers (USB-sticks, Geheugenkaarten, enz.)
x	x	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	x	x	Voldoende vernietiging van gegevensdragers.
x	x	x	x	Richtlijn voor privaat gebruik van de maatschappij-apparaten.
x	x	x	x	Richtlijn voor BYOD (Bring your own device)
x	x	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:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maatregel**
x	x	x	x	Administratie van rechten en rollen
x	x	x	x	Gedifferentieerde toegangsrechten
x	x	x	x	Profielen
x	x	x	x	Rollen
x	x	x	x	Documentatie van toegangsrechten
x	x	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	x	x	4 ogen principe wordt toegepast
x	x	x	x	Segregatie van Verplichtingen
x	x	x	x	Taakverwante toegangsprofielen
x	x	x	x	Verlagen van aantal personen met administratieve privilegies tot een minimum
x	x	x	x	Verwijderen van gegevens-media vóór hergebruik
x	x	x	x	Gebruik van dienstverlener voor documentendestructie
x	x	x	x	Veilige bewaring van gegevensmedia
x	x	x	x	Correcte vernietiging van gegevensmedia
x	x	x	x	Loggen van destructie
				Regelmatige audit van toegangsrechten
x	x	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	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:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maatregel**
x	x	x	x	Gescheiden Systemen
x	x	x	x	Gescheiden databases
x	x	x	x	Rechten van Toegangscontrole
x	x	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:

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

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maatregel**
x	x	x	x	Toegangsrechten /Concept van Toelating
x	x	x	x	Systeemzijde loggen
				Veiligheids- of loggingprogramma
x	x	x	x	Functionele verantwoordelijkheden
				4 ogen principe
				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:

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

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maatregel
x	x	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	x	x	Opleiding van alle bevoegde tewerkgestelden
x	x	x	x	Regelmatige opvolging van de opleidingscursussen
x	x	x	x	Verplichting van de tewerkgestelden om de vertrouwelijkheid te bewaren en de geheimhouding van gegevens.
x	x	x	x	Regelmatige audits van gegevensbescherming door de verantwoordelijke voor de bescherming van de bedrijfsgegevens
				Aanduiding van contactpersonen en verantwoordelijke projectbeheerders voor de specifieke bestelling
x	x	x	x	Zorgvuldige selectie van de aannemer