Anhang ALSO International Technisch-organisatorische Maßnahmen

Gesellschaft: ALSO International
Standort: Wijchen (Warehouse), Nijmegen (Netherlands), Krefeld (Germany)
Amersham (United Kingdom)

1.Vertraulichkeit (Art. 32 Abs. 1 lit B EU-DSGVO)
Zutrittskontrolle
Kein Unbefugter Zutritt zu Datenverarbeitungsanlagen.

Zweck: Diese Maßnahmen sollen gewährleisten, dass unbefugten der „körperliche“ Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden verwehrt wird.

Im Unternehmen getroffenen Maßnahmen:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maßnahme
x	x			Zutrittskontrollsystem (Ausweisleser, Schließsystem)
x	x	x	x	Maßnahmen zur Objektsicherung
x	x			Zaunanlagen
x	x	x	x	Sicherheitstüren, Sicherheitsfenster
				Gitter vor Fenstern und Türen
				Werkschutz, Pförtner
				Personenkontrolle beim Pförtner, Empfang
	x			Protokollierung der Besucher
x	x			Videoüberwachung
x	x	x	x	Lichtschranken, Bewegungsmelder
x	x			Türsicherung (Schließsystem, Codesperre, biometrische Zugangssperre, Sicherheitsschlösser)
x	x	x	x	Schlüsselverwaltung / Dokumentation der Schlüsselvergabe
x	x			Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz
x	x			Regelung für Gäste / Besucher / Firmenfremde Personen
				Besucherausweise
NVT	x	NVT	NVT	Spezielle Schutzvorkehrungen des Serverraums
				Mitarbeiter- und Berechtigungsausweise (Tragepflicht)
x	x	x	x	Sperrbereiche
x	x	x	x	Sorgfältige Auswahl des Reinigungspersonals

Zugangskontrolle:
Kein unbefugter Systemzugang.

Zweck: Diese Maßnahmen sollen gewährleisten, dass nur befugte Personen die Datenverarbeitungssysteme zugänglich sind und ausschließlich von Ihnen benutzt werden können.

Im Unternehmen getroffene Maßnahmen:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maßnahme**
x	x	x	x	Persönlicher und individueller User-Log-In bei Anmeldung am System, bzw. Unternehmensnetzwerk
x	x	x	x	Kennwortverfahren (Kennwortrichtlinie)
				Multi-Faktor Anmeldung
x	x			BIOS-Passwortschutz
x	x	x	x	Zusätzlicher System-Log-in für bestimmte Anwendungen
x	x	x	x	Zuordnung einzelner Clients und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen
x	x	x	x	Automatische Sperrung des Clients nach gewissem Zeitablauf ohne Useraktivität (auch Passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
				Elektronische Dokumentation sämtlicher Passwörter (keine User-Passwörter) und Verschlüsselung dieser Dokumentation zum Schutz vor unbefugtem Zugriff
				Personalisierte Chipkarten
				Biometrische Login-verfahren
x				Gehäuseverriegelung
				Sperren von externen Schnittstellen (z.B. USB)
x	x	x	x	Einsatz von Intrusion-Detection-Systemen
x	x	x	x	Einsatz von Anti-Viren-Software/Anti-Malware-Software
x	x	x	x	Einsatz von Firewall-Systemen
x	x	x	x	Netzwerkzugangskontrolle (Network-Access-Control)
x	x	x	x	Zuordnung von Benutzerprofilen zu IT-Systemen
x	x	x	x	Einsatz von VPN-Technologie
x	x	x	x	Einsatz von Verschlüsselungsmechanismen für Dateien
x	x	x	x	Verschlüsselung von Mobilen Datenträgern
x	x	x	x	Datenträger in Mobilen Geräten (Notebooks, Smartphones, etc.)
				Externe Speichermedien (USB-Sticks, Memory-Cards, etc)
x	x	x	x	Kein Gerät ohne Passwort oder Sperrcode mit Zugriff auf Firmendaten
				Verpflichtung auf das Datengeheimnis nach Art 28 Abs. 3 lit. b EU-DSGVO
x	x	x	x	Ordnungsgemäße Vernichtung von Datenträgern
x	x	x	x	Richtlinie zur privaten Nutzung des IT-Equipments
x	x	x	x	Richtlinie zu BYOD (Bring your own device)
x	x	x	x	Richtlinie mobiler Arbeitsplatz (z.B. Notebook)

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.
Z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Zweck:
Diese Maßnahmen sollen gewährleisten das nur die zur Nutzung des Datenverarbeitungssystems Berechtigten den Zugriff haben und der Zugriff sich ausschließlich auf diese Personenbezogenen Daten beschränkt die dieser Zugriffsberechtigung unterliegen, so das Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Im Unternehmen getroffenen Maßnahmen:.

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maßnahme**
x	x	x	x	Verwaltung von Berechtigungen
x	x	x	x	Differenzierte Berechtigungen
x	x	x	x	Profile
x	x	x	x	Rollen
x	x	x	x	Dokumentation von Berechtigungen
x	x	x	x	Genehmigungsverfahren zur Berechtigungsvergabe
				Auswertungen/Protokollierung
				Prüfung/Auditierung
				Verschlüsselung von CD/DVD-ROM, externen Festplatten und oder Laptops (z.B. per Betriebssystem, Safeguard, PGP, Veracrypt, etc.)
x	x	x	x	Vier-Augen-Prinzip
x	x	x	x	Segregation of Duties
x	x	x	x	Aufgabenbezogene Berechtigungsprofile
x	x	x	x	Reduzierung der Personen mit Administratorenberechtigungen auf ein Minimum
x	x	x	x	Löschung von Datenträgern vor Wiederverwertung
x	x	x	x	Einsatz von Aktenvernichtern bzw. Dienstleistern zur Aktenvernichtung
x	x	x	x	Sichere Aufbewahrung von Datenträgern
x	x	x	x	Ordnungsgemäße Vernichtung von Datenträgern
x	x	x	x	Protokollierung der Vernichtung
				Regelmäßige Überprüfung der Berechtigungen
x	x	x	x	Aufzeichnung und Auswertung von Protokollen (erfolglose und erfolgreiche Authentifizierungsversuche)
				Richtlinien zur Pseudonymisierung von pers. Daten
x	x	x	x	Abwesenheitsregelung (Zugang zum Datenbestand des Abwesenden)

Trennungskontrolle:
Getrennte Verarbeitung von daten, die zu unterschiedlichen Zwecken erhoben wurden. (Z.B. Sandboxing, Mandantenfähigkeit)

Zweck:
Zweckbezogenen Verarbeitung personenbezogener Daten soll technisch sichergestellt werden. D.h. zu unterschiedlichen Zwecken erhobene Daten sollen auch entsprechend getrennt verarbeitet werden.

Im Unternehmen getroffene Maßnahmen:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maßnahme
x	x	x	x	Getrennte Systeme
x	x	x	x	Getrennte Datenbanken
x	x	x	x	Zugriffsberechtigungen
x	x	x	x	Trennung durch Zugriffsregelungen

Sonstiges:
Pseudonymisieren: (Art. 32 Abs. 1 lit a DSGVO, Art 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzliche Information gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterlag.

2. Integrität (Art. 32 Abs. 1 lit B EU-DSGVO
Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen während des Transportes oder Elektronischer Übertragung. (Z.B Verschlüsselung, VPN, Signatur, etc.)

Zweck:
Diese Maßnahmen sollen gewährleisten das Datenträger während des Transportes oder elektronischer Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, bzw. soll durch die Maßnahmen überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Insofern werden die Transport- und Datenträgerkontrollen durch die Weitergabekontrolle zusammengefasst.

Im Unternehmen getroffene Maßnahmen:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Maßnahme**
				Verschlüsselung von email
				Verschlüsselung von CD/DVD-ROM, externen Festplatten und oder Laptops (z.B. per Betriebssystem, Safeguard, PGP, Veracrypt, etc.)
x	x	x	x	Verschlüsselte Datenverbindungen (VPN)
x	x	x	x	Protokollierung (Auditlogging)
				Transportsicherung von Datenträgern und Transportbehältern
x	x	x	x	Gesichertes WLAN
x	x	x	x	SSL-Verschlüsselung bei Web-Access
				Regelung zur Datenträgervernichtung
x	x	x	x	Ordnungsgemäße Vernichtung von Datenträgern
x	x	x	x	Sorgfältige Auswahl beim Transportpersonal bei manuellem Transport
				Weitergabe in Pseudonymisierter oder Anonymisierter Form
				Übersicht über regelmäßige Abruf- und Übermittlungsvorgänge
x	x	x	x	Keine Software die pers. Daten ohne vertragliche Regelungen auf Fremde Server transferiert. (Facebook, WhatsApp, …)
x	x	x	x	Verfahren zu Erkennung und Schutz von Schadsoftware
x	x	x	x	Gesicherter Datacenter-Eingang
				Datenträger-Verwaltung
				Gesonderter Verschluss vertraulicher Datenträger
x	x	x	x	Kontrollierte Vernichtung von Datenträgern (z.B. Fehldrucke,)
				Löschung von Datenträgern vor Austausch
				Gesicherter Ausdruck

Eingabekontrolle:
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement

Zweck:
Durch diese Maßnahmen soll die Nachprüfbarkeit eines Verarbeitungsvorgangs (Eingabe, Änderung, Entfernung) personenbezogener Daten gewährleistet werden. D.h. Urheber, Inhalt und Zeitpunkt der Datenspeicherung sollen ermittelt werden.

Im Unternehmen getroffenen Maßnahmen:.

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maßnahme
x	x	x	x	Zugriffsrechte / Berechtigungskonzept
x	x	x	x	Systemseitige Protokollierungen
				Sicherheits-/Protokollierungssoftware
x	x	x	x	Funktionelle Verantwortlichkeiten
				Mehraugenprinzip
				Verpflichtung auf das Datengeheimnis

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit b EU-DSGVO)
Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backupkonzept (online/offline, onsite/offsite), unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege, Notfallpläne.

Zweck:
Es muss sichergestellt sein, dass die personenbezogenen Daten nicht zufällig zerstört werden und vor Verlust geschützt sind. Es muss gewährleistet sein, das eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Im Unternehmen getroffene Maßnahmen:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maßnahme
x	x	x	x	Backupstrategie
x	x	x	x	Aufbewahrungskonzept von Backups
	x			Serverräume nicht unterhalb von wasserführenden Anlagen/Einrichtungen
x	x	x	x	Unterbrechungsfreie Stromversorgung (Batterie, Diesel)
x	x	x	x	Temperatur- und Feuchtigkeitsüberwachung in Serverräumen
x	x	x	x	Viren/Bedrohungsschutz, Firewall
x	x	x	x	Klimaanlage in IT Räumen
x	x	x	x	Brand- und Löschschutz (Brandmeldeanlagen, Feuerlöscheinrichtungen)
x	x	x	x	Alarmanlage
				Geeignete Archivierungsräumlichkeiten
x	x	x	x	Notfallplan
x	x	x	x	Notfallübung
				Katastrophenpläne, BCM
x	x	x	x	Ausfall- und Wiederherstellungspläne, etc.
x	x	x	x	Redundantes Datacenter (inhouse/extern)
x	x	x	x	Redundante Datenanbindung der Datacenter an das Corporate Network
x	x	x	x	Redundante Hardware
				Spiegeln von Daten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

Auftragskontrolle:
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 EU-DSGVO ohne entsprechende Weisung des Auftraggebers, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Zweck:
Der Auftragnehmer hat zu gewährleisten das die im Auftrag zu bearbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Mittelbar damit verbunden ist die Pflicht des Auftraggebers, Weisungen an Auftragnehmer zu erteilen.

Im Unternehmen gelten folgende Maßnahmen:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Maßnahme
x	x	x	x	Schriftlicher Vertrag zur Auftragsdatenverarbeitung gem. EU-DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
x	x	x	x	Schulungen aller zugriffsberechtigten Mitarbeiter
x	x	x	x	Regelmäßig stattfindende Nachschulungen
x	x	x	x	Verpflichtung der Mitarbeiter zur Geheimhaltung und auf das Datengeheimnis
x	x	x	x	Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
				Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag
x	x	x	x	Sorgfältige Auswahl des Auftragnehmers