Appendix Technical and organisational measures

Company: ALSO International
Location: Wijchen (Warehouse), Nijmegen (Netherlands), Krefeld (Germany) Amersham (United Kingdom)

1.Confidentiality (Art. 32 Paragraph 1 Point B EU-GDPR)

Physical Access Control

No unauthorized physical access to data processing systems.

Purpose: This measure should ensure that no unauthorized person has physical access to data processing systems, that process personal data.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Measure
x	x			Access Control System (ID-Card reader, Key locking system)
x	x	x	x	Measures for object security
x	x			Fences
x	x	x	x	Securitydoors, Securitywindows
				Grating for windows and doors
				Factory security service, gatekeeper
				Control of persons, Reception
	x			Documentation of visitors
x	x			Video surveillance
x	x	x	x	Photoelectric beams, Motion sensors
x	x			Door security (Key locking system, Code lock, Biometrical access control, Security locks)
x	x	x	x	Physical Key management / Documentation of physical key distribution
x	x			Securing due out of Office hours by factory security service and / or alarm system.
x	x			Guideline for guests / visitors / external persons
				Visitor ID-cards
NVT	x	NVT	NVT	Special safety measures for serverrooms
				Employee identity cards and authorisation cards (wearing obligation)
x	x	x	x	Restricted areas
x	x	x	x	Careful selection of cleaning staff

Access Control:
No unauthorized access to data processing systems.

Purpose: This measure should ensure that only authorized persons have access to data processing systems and can only be used by them.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	Measure
x	x	x	x	Personal and individual User-Log-In when logging in data processing systems and company network
x	x	x	x	Passwordpolicy
				Multi-Faktor Authentication
x	x			BIOS-Passwortprotection
x	x	x	x	Additional system-log-in for certain applications
x	x	x	x	Assignment of certain clients exclusively for defined roles.
x	x	x	x	Automatic locking of clients due to inactivity without user interaction. (Passwordprotected screensaver or automatic break detection)
				Electronic documentation of passwords (no user-passwords) and encryption of this documentation to prevent unauthorized access.
				Individual Chip-cards
				Biometrically login-option
x				Case-locking
				Disable of external interfaces (e.g. USB)
x	x	x	x	Use of Intrusion-Detection-Systems
x	x	x	x	Use of Anti-Virus-Software/Anti-Malware-Software
x	x	x	x	Use of Firewalls
x	x	x	x	Network-Access-Control (NAC)
x	x	x	x	Assignment of userprofiles to IT-systems
x	x	x	x	Use of VPN-Technology
x	x	x	x	Use of encryption mechanisms for files
x	x	x	x	Encryption of mobile data carriers.
x	x	x	x	Data carrier in mobile devices (Notebooks, Smartphones, etc.)
				External data carrier (USB-Sticks, Memory-Cards, etc)
x	x	x	x	No devices without password or locking code with access to company data.
				Obligation of users to dataprotection. Art 28 Paragraph 3 Point b EU-DSGVO
x	x	x	x	Duly destruction of data carriers.
x	x	x	x	Guideline for private use of company equipment.
x	x	x	x	Guideline for BYOD (Bring your own device)
x	x	x	x	Guideline for mobile worker (e.g. Notebook)

Data Access Control
No unauthorized reading, copying, modifying or deleting of personal data inside a data processing system.
E.g. Authorization concept, needs-based access rights, access-logging.

Purpose: This measure should ensure that only authorized users have access to the data processing system and the access to personal data is limited to the access-rights of this user. Personal data cannot be processed, used and after storing the data cannot unauthorized read, copy, modify or delete.

Adopted measures:

Wijchen (EDC)	**Nijmegen (NL)**	**Krefeld (DE)**	**Amersham (UK)**	**Measure**
x	x	x	x	Administration of rights and roles
x	x	x	x	Differentiated access rights
x	x	x	x	Profiles
x	x	x	x	Roles
x	x	x	x	Documentation of access rights
x	x	x	x	Approval procedure for authorization assignment
				Debriefing / Logging
				Inspection / Auditing
				Encryption of CD/DVD-ROM, external drives or Notebooks (e.g. by operating system, Safeguard, PGP, Veracrypt, etc.)
x	x	x	x	4 eyes principles
x	x	x	x	Segregation of Duties
x	x	x	x	Task-related accessright-profiles
x	x	x	x	Decrease persons with admin privileges to a minimum
x	x	x	x	Erase of data mediums before re-use
x	x	x	x	Use of service provider for document destruction
x	x	x	x	Secure keeping of data mediums
x	x	x	x	Correct destruction of data mediums
x	x	x	x	Logging of destruction
				Regular audit of access rights
x	x	x	x	Record and analyze of logfiles (successful and unsuccessful login attempts)
				Guideline to pseudonymize of personal data
x	x	x	x	Absence regulation/guideline. (Access to data of absent employee)

Separation control:
Separated processing of data, that are collected for different purposes. (e.g. Sandboxing, Multi-client capable)

Purpose: Purpose related processing of personal data should be implemented on a technical level. Data that is collected for different purposes should be processed separated.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Measure**
x	x	x	x	Seperated Systems
x	x	x	x	Seperated Databases
x	x	x	x	Access-control-rights
x	x	x	x	Seperation through Access-Control-Rights

Other:
Pseudonymisation: (Article 32 Paragraph 1 Point a EU-GDPR, Article 25 Paragraph 1 EU-GDPR)
Processing personal data is done in a wise that without additional information this data can not be referred to a specific individual person, insofar as the additional information stored separately and bound to technical and organisational measures.

2. Integrity (Art. 32 Paragraph 1 Point B EU-GDPR)
Transfer control

No unauthorized read, copy, modify or erase during transportation or electronic transmission. (Encryption, VPN, Signature, etc.)

Purpose: These measures should ensure that data mediums cannot be read, copied, modified or erased during transport. The measures should check and find out where personal data is transferred or being prepared for transfer. Transport- and data medium control are combined in transfer control.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Measure**
				Email-Encryption
				Encryption of CD/DVD-ROM, external drives or Notebooks (e.g. by operating system, Safeguard, PGP, Veracrypt, etc.)
x	x	x	x	Encrypted Connections (VPN)
x	x	x	x	Logging (Auditlogging)
				Transportation lock of data mediums and transport containers
x	x	x	x	Secured WLAN
x	x	x	x	SSL-Encryption for Web-Access
				Guideline for data destruction
x	x	x	x	Correct destruction of data mediums
x	x	x	x	Careful selection of transport staff if manually transported
				Transfer in a pseudonymized or anonymized way
				Record of regular datatransmissions
x	x	x	x	No Software that transfers personal data without contractual clauses to foreign server. (Facebook, Whatsapp,…)
x	x	x	x	Procedures to detect and protect against malicious software
x	x	x	x	Secured datacenter-entrance
				Data medium management
				Seperate Storage for confidential Data mediums
x	x	x	x	Destruction of data mediums (e.g. false printouts, disks,…)
				Erase of Data mediums before exchanging
				Secure printing

Inputcontrol:
Determining whether and by whom personal data has been entered, changed or removed in data processing systems, e.g. logging, document management.

Purpose: These measures are designed to ensure the verifiability of a processing operation (entry, modification, removal) of personal data. This means that the author, content and time of data storage should be determined.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Measure**
x	x	x	x	Access Rights / Authorization Concept
x	x	x	x	Systemside logging
				Security or Loggingsoftware
x	x	x	x	Functional responsibilities
				4-eyes principle
				Obligation to data protection

3. Availability and resilience (Art. 32 Paragraph 1 Point b EU-GDPR)
Availability Control:
Protection against accidental or deliberate destruction or loss, e.g.: Backup concept (online/offline, onsite/offsite), uninterruptible power supply, virus protection, firewall, reporting channels, emergency plans.

Purpose: It must be ensured that the personal data is not accidentally destroyed and protected against loss. It must be ensured that the systems used can be restored in the event of a malfunction.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Measure**
x	x	x	x	Backupstrategy
x	x	x	x	Stortage concept for Backups
	x			Server rooms not below water-bearing systems/facilities
x	x	x	x	Uninterruptible power supply (battery, diesel)
x	x	x	x	Temperature and humidity monitoring in server rooms
x	x	x	x	Virus/threat protection, firewall
x	x	x	x	Air conditioning in IT rooms
x	x	x	x	Fire and extinguishing protection (fire alarm systems, fire extinguishing equipment)
x	x	x	x	Alarm systems
				Suitable archiving rooms
x	x	x	x	Emergency Plan
x	x	x	x	Emergency exercise
				Failure and recovery plans
x	x	x	x	Redundant Datacenter (inhouse/extern)
x	x	x	x	Redundant Dataconnection of Datacenter to Corporate Network
x	x	x	x	Redundant Hardware
x	x	x	x	Datamirroring

4. Procedure for regular review, benchmark and evaluation (Art. 32 Paragraph 1 Point d EU-GDPR; Art. 25 Paragraph 1 EU-GDPR)

Order control:
No processing of data within the meaning of Art. 28 EU-GDPR without corresponding instructions from the contracting authority, e.g. clear contract design, formalised order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.

Purpose: The contractor must ensure that the data to be processed in the order will only be processed in accordance with the instructions of the client. Indirectly connected with this is the obligation of the customer to give instructions to contractors.

Adopted measures:

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Measure**
x	x	x	x	Written contract for order data processing according to EU-GDPR with regulations on the rights and obligations of the contractor and principal
x	x	x	x	Training of all authorized employees
x	x	x	x	Regular follow-up training courses
x	x	x	x	Obligation of employees to maintain confidentiality and data secrecy
x	x	x	x	Regular data protection audits by the company data protection officer
				Determination of contact persons and responsible project managers for the specific order
x	x	x	x	Careful selection of the contractor