Annexe ALSO International Mesures techniques et organisationnelles

Société : ALSO International

Lieu : Wijchen , Nijmegen, Krefeld , Amersham

1. Confidentialité (Art. 32 Paragraphe 1 Point B UE-RGPD)

Contrôle d'accès physique

Aucun accès physique non autorisé aux systèmes de traitement de données.

Objet : Cette mesure devrait garantir qu'aucune personne non autorisée n'a physiquement accès à des systèmes de traitement de données qui traitent des données personnelles.

Mesures adoptées :

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
x	x			Système de contrôle d'accès (lecteur de carte d'identité, système de verrouillage à clé)
x	x	x	x	Mesures pour la sécurité du bâtiment
x	x			Clôtures
x	x	x	x	Portes de sécurité, fenêtres de sécurité
				Grille pour fenêtres et portes
				Service de sécurité, portier
				Contrôle des personnes, Réception
	x			Documentation des visiteurs
x	x			Vidéosurveillance
x	x	x	x	Détecteurs de mouvement, photoélectriques
x	x			Sécurité des portes (système de fermeture à clé, verrouillage par code, contrôle d'accès biométrique, verrouillage de sécurité)
x	x	x	x	Gestion des clés physiques/Documentation de la distribution physique des clés
x	x			Sécurisation en dehors des heures de bureau par le service de sécurité d'usine et/ou le système d'alarme.
x	x			Ligne directrice pour les invités/visiteurs/personnes extérieures
				Cartes d'identité de visiteur
	x			Mesures de sécurité spéciales pour les salles de serveurs
				Cartes d'identité des employés et cartes d'autorisation (obligation de port)
x	x	x	x	Zones réglementées
x	x	x	x	Sélection rigoureuse du personnel de nettoyage

Contrôle d'accès :
Aucun accès non autorisé aux systèmes de traitement de données.

Objet : Cette mesure devrait garantir que seules les personnes autorisées ont accès aux systèmes de traitement de données et ne peuvent être utilisées que par elles.

Mesures adoptées :

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
x	x	x	x	Code de connexion personnel et individuel lors de la connexion dans les systèmes de traitement de données et le réseau de l'entreprise
x	x	x	x	Politique de mot de passe
				Authentification Multi-facteur
x	x			Protection par mot de passe BIOS
x	x	x	x	Système de connexion supplémentaire pour certaines applications
x	x	x	x	Affectation de certains clients exclusivement pour des rôles définis.
x	x	x	x	Verrouillage automatique des clients dû à l'inactivité sans intervention de l'utilisateur. (Écran de veille protégé par mot de passe ou détection automatique de rupture)
				Cartes à puce individuelles
				Option de connexion biométrique
				Casier
x				Cartes à puce individuelles
				Disable of external interfaces (e.g. USB)
x	x	x	x	Désactiver des interfaces externes (par exemple USB)
x	x	x	x	Utilisation de systèmes de détection d'intrusion
x	x	x	x	Utilisation de logiciels antivirus/anti-logiciels malveillants
x	x	x	x	Utilisation de pare-feu informatique
x	x	x	x	Contrôle d'accès réseau
x	x	x	x	Affectation de profils utilisateur à des systèmes informatiques
x	x	x	x	Utilisation de la technologie VPN

x	x	x	x	Le support de données dans les appareils mobiles (ordinateurs portables, smartphones, etc.)
x	x	x	x	Cryptage des supports de données mobiles.
				Un support de données externe (clés USB, cartes mémoire, etc.)
x	x	x	x	Pas d'appareils sans mot de passe ou de verrouillage avec accès aux données de l'entreprise
				Obligation pour les usagers de protéger les données. Art. 28 alinéa 3 point b EU-RGPD
x	x	x	x	La destruction des supports de données.
x	x	x	x	Ligne directrice pour l'utilisation privée de l'équipement de l'entreprise.
x	x	x	x	Ligne directrice pour le BOYD (Bring Your Own Device)
x	x	x	x	Ligne directrice pour travailleur mobile (par exemple, ordinateur portable)

Contrôle d'accès aux données

Aucune lecture, copie, modification ou suppression non autorisées de données personnelles à l'intérieur d'un système de traitement de données.
Par exemple : Concept d'autorisation, droits d'accès basés sur les besoins, consignation d'accès.

Objet : Ces mesures devraient garantir que seuls les utilisateurs autorisés ont accès au système de traitement des données et que l'accès aux données personnelles est limité aux droits d'accès de cet utilisateur. Les données personnelles ne peuvent pas être traitées, utilisées et après stockage, les données ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation.

Ces mesures visent à garantir que seules les personnes autorisées à utiliser le système de traitement de données ont accès aux données personnelles faisant l'objet d'une telle autorisation, afin qu'elles ne soient pas lues, copiées, altérées ou stockées sans autorisation.

Mesures adoptées :

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
x	x	x	x	Administration des droits et des rôles
x	x	x	x	Droits d'accès différenciés
x	x	x	x	Profils
x	x	x	x	Rôles
x	x	x	x	Documentation des droits d'accès
x	x	x	x	Procédure d'approbation pour l'attribution d'autorisation
				Compte rendu / Journalisation
				Inspection/Audit
				Cryptage de CD/DVD-ROM, de lecteurs externes ou d'ordinateurs portables (par exemple, par système d'exploitation, sauvegarde, PGP, Veracrypt, etc.)
x	x	x	x	Principes des 4 yeux
x	x	x	x	Séparation des tâches
x	x	x	x	Profils de droits d'accès liés aux tâches
x	x	x	x	Diminuer au minimum les personnes ayant des privilèges d'administrateur
x	x	x	x	Effacement des supports de données avant réutilisation
x	x	x	x	Utilisation du fournisseur de services pour la destruction de documents
x	x	x	x	Maintien sécurisé des supports de données
x	x	x	x	La destruction correcte des supports de données
x	x	x	x	Enregistrement de la destruction
				Audit régulier des droits d'accès
x	x	x	x	Enregistrement et analyse des fichiers journaux (tentatives de connexion réussies et infructueuses)
				Ligne directrice pour la pseudonymie des données personnelles
x	x	x	x	Règlement d'absence/ligne directrice. (Accès aux données de l'employé absent)

Contrôle de séparation :

Traitement séparé des données, recueillies à des fins différentes. (Par exemple, Sandboxing, capacité multi-client)

Objet : Le traitement des données personnelles à des fins spécifiques devrait être mis en œuvre au niveau technique. Les données collectées à des fins différentes doivent être traitées séparément.

Mesures adoptées :

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
x	x	x	x	Systèmes séparés
x	x	x	x	Bases de données séparées
x	x	x	x	Accès-contrôle-droits
x	x	x	x	Séparation grâce aux droits de contrôle d'accès

Autre :
Pseudonymie : (article 32, alinéa 1, point a, de l'accord UE-RGPD, article 25, alinéa 1, de l'accord UE-RGPD).
Le traitement des données personnelles s'effectue de manière à ce que, sans informations supplémentaires, ces données ne puissent pas être transmises à une personne spécifique, dans la mesure où les informations supplémentaires sont stockées séparément et liées à des mesures techniques et organisationnelles.

2. Intégrité (Art. 32 Alinéa 1 Point B UE-RGPD)
Contrôle de transfert

Aucune lecture, copie, modification ou effacement non autorisés pendant le transport ou la transmission électronique. (Chiffrement, VPN, Signature, etc.)

Objectif : Ces mesures doivent garantir que les supports de données ne peuvent pas être lus, copiés, modifiés ou effacés pendant le transport. Les mesures doivent vérifier et savoir où les données personnelles sont transférées ou en cours de préparation pour le transfert. Le transport et le contrôle du support de données sont combinés dans le contrôle de transfert.

Mesures adoptées :

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
				Cryptage d'email
				Cryptage de CD/DVD-ROM, de lecteurs externes ou d'ordinateurs portables (par exemple, par système d'exploitation, sauvegarde, PGP, Veracrypt, etc.)
x	x	x	x	Connexions cryptées (VPN)
x	x	x	x	Journalisation (journal d'audit)
				Verrou de transport des supports de données et des conteneurs de transport
x	x	x	x	WLAN sécurisé
x	x	x	x	Cryptage SSL pour l'accès au Web
				Ligne directrice pour la destruction des données
x	x	x	x	La destruction correcte des supports de données
x	x	x	x	Sélection rigoureuse du personnel de transport si transporté manuellement
				Transférer de manière pseudonymisée ou anonymisée
				Enregistrement des transmissions de données régulières
x	x	x	x	Aucun logiciel qui transfère des données personnelles sans clauses contractuelles à un serveur tiers. (Facebook, WhatsApp...)
x	x	x	x	Procédures de détection et de protection contre les logiciels malveillants
x	x	x	x	Entrée sécurisée du centre de données
				Gestion du support de données

				Stockage séparé pour les supports de données confidentielles
x	x	x	x	Destruction de supports de données (par exemple, fausses impressions, disques...)
				Effacement des supports de données avant l'échange
				Impression sécurisée

Contrôle d'entrée :
Déterminer si et par qui des données personnelles ont été saisies, modifiées ou supprimées dans des systèmes de traitement de données, par ex. journalisation, gestion de documents.

Objet : Ces mesures sont destinées à assurer la vérifiabilité d'un traitement (entrée, modification, suppression) de données personnelles. Cela signifie que l'auteur, le contenu et l'heure du stockage des données doivent être déterminés.

Mesures adoptées :

Autre :

Wijchen (EDC)	**Nijmegen (NL)**	**Krefeld (DE)**	**Amersham (UK)**	**Mesure**
x	x	x	x	Droits d'accès/Concept d'autorisation
x	x	x	x	Enregistrement côté système
				Logiciel de sécurité ou de journalisation
x	x	x	x	Responsabilités fonctionnelles
				Principe des 4 yeux
				Obligation de protection des données

3. Disponibilité et résilience (Art. 32 Alinéa 1 Point b UE-RGPD)
Contrôle de disponibilité :
Protection contre la destruction ou la perte accidentelle ou délibérée, par exemple : concept de sauvegarde (en ligne/hors-ligne, sur site/hors site), alimentation ininterrompue, protection antivirus, pare-feu, canaux de signalement, plans d'urgence.

Objet : Il faut s'assurer que les données personnelles ne sont pas accidentellement détruites et qu'elles soient protégées contre les pertes. Il faut s'assurer que les systèmes utilisés peuvent être restaurés en cas de dysfonctionnement.

Mesures adoptées

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
x	x	x	x	Stratégie de sauvegarde
x	x	x	x	Concept de stockage pour les sauvegardes
	x			Salles de serveurs non situées en dessous des systèmes/installations aquifères
x	x	x	x	Alimentation sans interruption (batterie, diesel)
x	x	x	x	Surveillance de la température et de l'humidité dans les salles de serveurs
x	x	x	x	Protection contre les virus/menaces, pare-feu
x	x	x	x	Air conditionné dans les salles informatiques
x	x	x	x	Protection contre l'incendie et l'extinction (systèmes d'alarme incendie, équipement d'extinction d'incendie)
x	x	x	x	Systèmes d'alarme
				Salles d'archivage adaptées
x	x	x	x	Plan d'urgence
x	x	x	x	Exercice d'urgence
				Échec et plans de récupération
x	x	x	x	Centre de données redondant (interne/externe)
x	x	x	x	Connexion de données redondante du centre de données au réseau d'entreprise
x	x	x	x	Matériel redondant
x	x	x	x	Mise en miroir des données

4. Procédure d'examen régulier, de référence et d'évaluation (Art. 32 Alinéa 1 Point d UE-RGPD ; Art. 25 Alinéa 1 UE-RGPD)

Contrôle de commande :
Aucun traitement de données au sens de l'art. 28 UE-RGPD sans instruction correspondante de l'autorité contractante, par ex. conception claire des contrats, gestion des commandes formalisée, sélection stricte du prestataire de service, obligation de convaincre à l'avance, contrôles de suivi.

Objet : L'entrepreneur doit s'assurer que les données à traiter lors de la commande ne seront traitées que conformément aux instructions du client. L'obligation du client de donner des instructions aux entrepreneurs est un lien indirect.

Mesures adoptées :

Wijchen (EDC)	Nijmegen (NL)	Krefeld (DE)	Amersham (UK)	**Mesure**
x	x	x	x	Contrat écrit pour les commandes de traitement des données selon UE-RGPD avec des règlements sur les droits et obligations de l'entrepreneur et du client
x	x	x	x	Formation de tous les employés autorisés
x	x	x	x	Cours de suivi régulier
x	x	x	x	Obligation des employés de maintenir la confidentialité et le secret des données
x	x	x	x	Audits réguliers de protection des données par le responsable de la protection des données de l'entreprise
				Détermination des personnes de contact et des chefs de projets responsables pour la commande spécifique
x	x	x	x	Sélection rigoureuse de l'entrepreneur