



KONICA MINOLTA

Mesures techniques et organisationnelles



Mesures techniques et organisationnelles

1. Confidentialité

a) Contrôle d'accès physique :

Les mesures permettant d'interdire aux personnes non-autorisées l'accès aux systèmes de traitement des données utilisés pour le traitement des données à caractère personnel sont décrites ci-dessous :

- Détermination des personnes bénéficiant de l'accès au moyen d'exigences organisationnelles
- Documentation de l'attribution et du retrait des droits d'accès
- Audit régulier des droits d'accès
- Contrôle de l'accès au moyen d'une Carte d'accès personnalisée avec photographie d'identité et code PIN (TÜV RZ [Certification informatique])
- Contrôle de l'accès avec jeton personnalisé, contrôle biométrique de l'accès (empreinte digitale) et système de séparation
- Documentation de la présence dans les salles des serveurs
- Règlementation des accès pour les personnes externes
- Zone fermée avec accès réservé aux personnes autorisées uniquement
- Surveillance vidéo de cette zone et à l'intérieur des bâtiments, y compris les salles des serveurs

b) Contrôle de l'accès au système :

Les mesures suivantes sont prises pour empêcher l'intrusion de personnes non-autorisées dans les systèmes de traitement des données :

- L'entrée dans les systèmes n'est possible qu'après authentification au moyen d'un identifiant et mot de passe personnels
- Utilisation de mots de passe complexes comportant au moins huit caractères et qui respectent au moins trois critères sur quatre (lettre majuscule, lettre minuscule, chiffre, caractère spécial) et changement obligatoire du mot de passe tous les 90 jours
- Interdiction de divulguer les mots de passe
- Journalisation des attributions des droits d'accès
- Limitation au minimum des accès en lien avec l'administration
- Protection des systèmes de traitement des données face aux accès non-autorisés au moyen de systèmes de pare-feu pertinents

c) Contrôle de l'accès aux données :

Les activités non-autorisées dans les systèmes de traitement des données et en-dehors du périmètre des droits attribués seront interdites au moyen de droits d'accès et d'un concept d'autorisation fondé sur les besoins et d'inspections de ces systèmes :

- Limitation des droits d'accès aux domaines d'activité
- Séparation des autorisations de droits (organisationnelles) et des attributions de droits (techniques)
- Journalisation des modifications apportées aux droits
- Contrôles des tentatives d'accès non-autorisés (IDS/IPS)

d) Contrôle de la séparation :

- Spécification de différents profils d'utilisateur
- Droits d'accès spécifiques et alignés sur les besoins en matière d'accès aux données
- Séparation des données dans plusieurs applications à l'aide de machines virtuelles (pour les applications individuelles)

e) Pseudonymisation (Art. 32 sec. 1 point a du RGPD ; Art 25 sec. 1 du RGPD)

2. Intégrité

a) Contrôle des transmissions :

- Chiffrement des transferts de données, notamment lors de transferts via des réseaux publics (par ex. SSL, TLS)
Élimination des données respectant la protection des données, supports de données et exemplaires physiques conformes à un concept de classe de protection

b) Contrôle des entrées :

Les droits d'accès sont régulièrement contrôlés et mis à jour
La journalisation du traitement des données (lorsque cela est possible et pertinent) permet ultérieurement de vérifier et de déterminer si des données à caractère personnel ont été saisies, modifiées ou supprimées et le cas échéant, par qui (par ex. journaux de modification des données dans les systèmes ERP centralisés)
Enregistrement et disponibilité selon les besoins des actions correspondantes menées sur les systèmes (par ex. les fichiers de journaux)
Identification et marquage explicites du stockage de données des appareils MFP/PP- pour leur retour

3. Disponibilité et capacité de charge : Contrôle de la disponibilité et de la capacité de restauration :

L'utilisation de deux centres informatiques certifiés, situés à distance l'un de l'autre et empêchant ainsi l'interruption des services grâce à la redondance (c'est à dire grâce à la conservation de données redondantes)
Des précautions techniques prenant la forme de systèmes d'avertissement précoce dans le cadre de la protection face aux perturbations provoquées par le feu/la chaleur, l'eau ou la surcharge et comprenant également une source d'alimentation électrique non-interruptible
Des mesures de protection face aux coupures et surcharges de courant, c'est à dire des systèmes de source d'alimentation non interruptible (UPS)
Réalisation programmée de sauvegardes des données et, si nécessaire, utilisation de procédures de redondance
Architecture d'antivirus/de pare-feu à plusieurs niveaux
Achats centralisés pour le matériel et les logiciels
Capacité à rétablir l'accès dans des délais convenables (Art. 32 sec.1 point. c **du RGPD**)

4. Contrôles des commandes :

Nomination d'un délégué à la protection des données
Accords de niveau de services avec des prestataires de services externes
Formation des employés au traitement des données à caractère personnel
Respect obligatoire de la confidentialité des données par les employés

5. Contrôle de l'organisation (vérification, analyse et évaluation) :

- Mise en place de processus de vérification en continu et si nécessaire, ajustement des mesures de protection des données
Règlement établi par écrit pour les copies des données
Processus permettant de traiter un cas de protection de données
Pour chaque processus pertinent, réalisation d'une étude de risques
Pour chaque processus pertinent, réalisation d'une étude d'impact
Mise en place de paramètres de base favorisant la protection des données
Incident - Réponse - Gestion