Contrat de traitement des données personnelles

VERSION 8 BBE 01.04.2024

§ 1 Objet du contrat

(1) Le sous-traitant fournit des services au Responsable du traitement (ci- également dénommé " le Client ") comme décrit par le contrat principal de location/achat de copieurs multifonctions avec services de maintenance associés (ci-après dénommé " Contrat principal"). Dans la mesure où la fourniture de ces services implique le traitement de données à caractère personnel pour le compte du Responsable du traitement, tel que visé par le Règlement général sur la protection des données entré en vigueur le 25 mai 2018 (ci-après : RGPD), les Parties fixent par la présente leurs droits et obligations respectifs dans le présent contrat de traitement des données personnelles (ci-après : " Contrat ").

(2) Les données à caractère personnel traitées peuvent provenir du Responsable du traitement, ou de responsables du traitement ou sous-traitants associés au Responsable du traitement en vertu des article 26 ou 28 du RGPD, ou avoir été collectées par le Sous-traitant pour le compte des parties susmentionnées (toutes les données à caractère personnel seront ci-après dénommées conjointement "données à caractère personnel du Responsable du traitement").

(3) Le type des données à caractère personnel du Responsable du traitement et les catégories des personnes concernées par le traitement, ainsi que la nature et la finalité du traitement sont spécifiés dans l'Annexe 1 de ce Contrat.

(4) La durée du traitement et la durée du présent Contrat dépendront de la durée du Contrat Principal, sauf si les dispositions suivantes imposent des obligations ou des droits de résiliation allant au-delà de ces durées.

§ 2 Droit d'émettre des instructions

(1) Le Sous-traitant ne peut collecter, traiter ou utiliser des données que dans le cadre du Contrat principal et conformément aux instructions du Responsable du traitement.

(2) Les instructions du Responsable du traitement sont initialement énoncées dans le présent Contrat et peuvent ensuite être modifiées, complétées ou remplacées par des instructions individuelles écrites ou sous forme de texte (instructions individuelles). Les instructions verbales sont confirmées sans délai par le Responsable du traitement (au moins sous forme de texte). Le Responsable du traitement a le droit d'émettre des instructions à tout moment. Cela inclut les instructions relatives à l'effacement, à la rectification et à la limitation du traitement des données. Pour les produits dont l'utilisation l'exige, les personnes autorisées à donner ou à recevoir des instructions sont définies dans l'Annexe 1 de ce Contrat.

(3) Si le Sous-traitant estime qu'une instruction du Responsable du traitement viole les règles de protection des données, il doit en informer le Responsable du traitement dans les plus brefs délais. Le Sous-traitant est en droit de suspendre l'exécution de l'instruction en question jusqu'à ce qu'elle soit confirmée ou modifiée par le Responsable du traitement. Le Sous-traitant peut refuser d'exécuter une instruction qui est manifestement illégale.

(4) Les instructions du Responsable du traitement qui vont au-delà des services dus en vertu du Contrat Principal, et du traitement des données requis à cet effet pourraient faire l'objet d'une rémunération supplémentaire.

§ 3 Mesures de sécurité dans le chef du Sous-traitant

(1) Le Sous-traitant s'engage à respecter les dispositions du RGDP, le Sous-traitant conçoit l'organisation de manière à ce qu'elle réponde aux exigences particulières de la protection des données. Le Sous-traitant prendra toutes les mesures techniques et organisationnelles nécessaires à la protection appropriée des données à caractère personnel du Responsable du traitement conformément à l'art. 32 du RGPD, en particulier et au minimum les mesures spécifiées dans l'Annexe 1 de ce Contrat. Le Sous-traitant se réserve le droit de modifier les mesures de sécurité prises, tout en veillant à ce qu'elles ne soient pas inférieures au niveau de protection convenu dans l'annexe 1 de ce Contrat.

(2) Le Sous-traitant a désigné un délégué à la protection des données de l'entreprise. Les coordonnées du délégué à la protection des données sont publiées sur le site Internet du Sous-traitant.

(3) Le Sous-traitant imposera une obligation de confidentialité (art. 28 point 3 al. b du RGPD) à l'ensemble de son propre personnel chargé du traitement et de l'exécution du présent CTD (ci-après dénommés les employés) et veille au respect de la présente obligation avec toute la diligence requise.

§ 4 Obligations du Sous-traitant

(1) En cas de violation de données à caractère personnel du Responsable du traitement, le Sous-traitant en informera immédiatement le Responsable du traitement par écrit ou sous forme de texte. La notification d'une violation de données à caractère personnel reprendra au minimum :

(a) la nature de la violation des données à caractère personnel, en ce compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de fichiers de données à caractère personnel concernés ;

(b) le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact où de plus amples informations peuvent être obtenues ;

(c) les conséquences probables de la violation des données à caractère personnel ;

(d) les mesures prises ou proposées à prendre par le Responsable du traitement pour remédier à la violation des données à caractère personnel, en ce compris, le cas échéant, les mesures visant à atténuer ses éventuels effets négatifs.

(2) Le Sous-traitant prendra immédiatement les mesures nécessaires pour sécuriser les données à caractère personnel et atténuer toute conséquence négative pour les personnes concernées, en informera le Responsable du traitement et demandera les instructions supplémentaires.

(3) En outre, le Sous-traitant sera tenu de fournir à tout moment des informations au Responsable du traitement si des données à caractère personnel auront été affectées par une violation telle que visée au paragraphe (1).

(4) Si les données à caractère personnel du Responsable du traitement présentes dans les locaux du Sous-traitant sont menacées de saisie ou de confiscation, par le biais d'une procédure d'insolvabilité ou de concordat, ou par d'autres événements ou mesures de tiers, le Sous-traitant en informera immédiatement le Responsable du traitement, à moins que cela ne soit interdit par un tribunal ou une ordonnance officielle. Dans ce contexte, le Sous-traitant informera sans délai toutes les autorités juridictionnelles que le pouvoir de décision ultime sur les données appartient exclusivement au Responsable du traitement en sa qualité de "Responsable du traitement" au sens du RGPD.

(5) Le Sous-traitant tiendra un registre des activités de traitement effectuées pour le compte du Responsable du traitement, contenant toutes les informations requises par l'art. 30 (2) du RGPD.

(6) Le Responsable du traitement et le Sous-traitant assisteront, si on le leur demande, les autorités de contrôle de la protection des données dans l'accomplissement de leurs tâches.

§ 5 Droits du Responsable du traitement

(1) Avant le début du traitement des données, et régulièrement par la suite, le Responsable du traitement s'assurera à sa satisfaction du caractère adéquat des mesures techniques et organisationnelles prises par le Sous-traitant. À cette fin, le Responsable du traitement peut, par exemple, obtenir des informations du Sous-traitant, se faire présenter des certifications ou des attestations d'experts existantes ou, après une coordination en temps utile (au moins trois semaines au préalable), inspecter les mesures techniques et organisationnelles prises par le Sous-traitant. Les inspections peuvent être effectuées pendant les heures normales de travail, en personne ou par une tierce partie compétente. Les inspections par des tierces parties doivent être effectuées avec l'accord du Sous-traitant, les tierces parties dans une relation de concurrence pouvant être rejetées par le Sous-traitant. Le Responsable du traitement n'effectuera les inspections que dans la mesure requise et ne perturbera pas de manière disproportionnée les activités du Sous-traitant. Chaque partie supportera ses propres coûts pour les audits et les inspections.

(2) Le Sous-traitant s'engage à fournir au Responsable du traitement, à la demande écrite de ce dernier et dans un délai raisonnable, toutes les informations et preuves nécessaires pour effectuer un audit ou une inspection sur les mesures techniques et organisationnelles prises par le Sous-traitant.

(3) Le Responsable du traitement consignera le résultat de l'audit ou de l'inspection et le fournira au Sous-traitant. Si le Responsable du traitement découvre des erreurs ou des irrégularités, notamment dans les résultats du traitement des données commandé, le Sous-traitant en sera informé sans délai. Si l'audit ou l'inspection révèle des problèmes dont l'évitement futur nécessite des modifications du traitement commandé, le Responsable du traitement informera le Sous-traitant des résultats et des modifications demandées, par écrit ou sous forme de texte.

§ 6 Engagement de sous-sous-traitants

(1) En signant le présent Contrat, le sous-traitant reçoit une autorisation générale de désigner des sous-sous-traitants pour l'exécution du contrat principal. Une liste des sous-sous-traitants désignés est ajoutée en annexe 1.

(2) Dans le cadre de ses obligations contractuelles, le Sous-traitant sera autorisé à modifier les relations existantes avec des Sous-sous-traitants ou à en établir de nouvelles. Le Sous-traitant en informera le Responsable du traitement dans les plus brefs délais. Le Responsable du traitement peut s'opposer à l'engagement de nouveaux Sous-sous-traitants. Le Responsable du traitement doit émettre toute objection sans délai ; les objections ne peuvent pas être fondées sur des considérations déraisonnables

(3) Le Sous-traitant est tenu de sélectionner soigneusement les Sous-sous-traitants en fonction de leur aptitude et de leur fiabilité. S'il est fait appel à des Sous-sous-traitants, le Sous-traitant les engagera conformément aux dispositions du présent Contrat. Si des Sous-sous-traitants d'un pays tiers doivent être impliqués, le Sous-traitant sera tenu de s'assurer qu'un niveau approprié de protection des données est garanti pour le Sous-sous-traitant concerné (par exemple, en convenant des SCC clauses)

(4) Il n'y aura pas de relation de sous-traitance au sens des présentes dispositions si le Sous-traitant confie à des parties tierces des services qui doivent être considérés comme purement auxiliaires. Il s'agit, par exemple, de services postaux, de transport et d'expédition, de services de nettoyage, de services de télécommunications sans référence spécifique aux services que le Sous-traitant fournit au Responsable du traitement, et de services de sécurité.

§ 7 Requêtes et droits des personnes concernées

(1) Dans la mesure du possible, le Sous-traitant assistera le Responsable du traitement en prenant des mesures techniques et organisationnelles appropriées pour aider à remplir les obligations du Responsable du traitement en vertu des articles 12 à 22 et 32 à 36 du RGPD.

(2) Si une personne concernée doit contacter directement le Sous-traitant afin de faire valoir ses droits en tant que personne concernée, par exemple pour obtenir des informations, la rectification ou l'effacement de ses données, le Sous-traitant ne réagira pas de manière indépendante. Si le Responsable du traitement concerné peut être identifié à partir de la demande de la personne concernée, le Sous-traitant en informera le Responsable du traitement et attendra les instructions de ce dernier.

§ 8 Responsabilité

(1) Le Responsable du traitement assume l'entière responsabilité, dans les limites du Contrat principal, de toute réclamation introduite à l'encontre du Sous-traitant pour toute perte ou tout dommage subi par une personne concernée à la suite d'un traitement de données ou de l'utilisation de données dans le cadre d'un traitement interdit ou incorrect au sens des règles de protection des données, pour autant que l'utilisation ou le traitement de données interdit ou incorrect soit basé sur des instructions émises par le Responsable du traitement.

(2) Chacune des Parties dégagera l'autre Partie respective de toute responsabilité si cette autre Partie peut prouver qu'elle n'était en aucun cas responsable de la circonstance qui a conduit à la perte ou au dommage subi par la personne concernée.

§ 9 Résiliation du ou des Contrat(s)-cadre(s)

(1) Après la résiliation du Contrat Principal, ou à tout moment à la demande de la Partie responsable, le Sous-traitant restituera à la Partie responsable tous les documents, toutes les données et tous les supports de données fournis par le Responsable du traitement ou (à la demande du Responsable du traitement, à moins qu'il n'y ait une obligation de conserver les données à caractère personnel en vertu du droit applicable) les effacera ou écrasera. Cela s'applique également à toute sauvegarde de données dans les locaux du Sous-traitant. Le sous-traitant a le droit de facturer au Responsable du Traitement un effacement ou un écrasement des données à caractère personnel stockées sur le disque dur d'un copieur multifonction.

(2) Le Sous-traitant sera tenu de traiter de manière confidentielle les données dont il a pris connaissance dans le cadre du Contrat Principal pendant et après la fin de la durée du Contrat Principal. Le présent Contrat restera en vigueur après la fin de la durée du Contrat Principal aussi longtemps que le Sous-traitant disposera de données à caractère personnel fournies par le Responsable du traitement ou collectées par le Sous-traitant pour le compte du Responsable du traitement.

§ 10 Dispositions générales

(1) Les changements et les modifications du présent Contrat doivent être effectués par écrit.

(2) Le présent Contrat fait partie intégrante du Contrat Principal. Tous les droits et obligations du Contrat Principal, y compris les limitations de responsabilité, s'appliquent donc également au présent Contrat. En cas de contradiction, d'incohérence ou de doute

entre les conditions du présent Contrat et les conditions du Contrat Principal , les conditions du Contrat Principal auront la priorité sur les conditions de ce Contrat.

(3) Si certaines dispositions du présent Contrat sont ou deviennent invalides ou inapplicables en tout ou en partie, cela n'affectera en rien la validité des autres dispositions.

(4) Le présent contrat est régi par le droit belge et relève, en cas de litige, de la compétence du tribunal de Bruxelles ou Anvers, par choix du sous-traitant.

Annexe au Contrat de traitement des données personnelles

Description des mesures de sécurité techniques et organisationnelles

1. A Description de la nature et de l'objet du traitement dans les systèmes d'impression

Les Systèmes Multifonctions et/ou d'Impression de production Konica Minolta traitent les documents papier et électroniques à des fins d'impression, de numérisation, de copie et de télécopie.

Konica Minolta est tenue de mettre en place et d'assurer la maintenance ou l'entretien des Systèmes susmentionnés conformément au contrat conclu entre Konica Minolta Business Solutions Belgium SA/NV ("Konica Minolta") et le client (ci-après "Contrat-cadre"). La présente annexe au CTD de Konica Minolta décrit le traitement des données à caractère personnel nécessaires à la mise en place, à la maintenance et à l'entretien des Systèmes susmentionnés par Konica Minolta en tant que "Sous-traitant" au sens du RGPD.

Le traitement des données à caractère personnel du Responsable du traitement ou de parties tierces (dénommés conjointement ci-après "données à caractère personnel du Responsable du traitement") par Konica Minolta est exclusivement effectué dans le cadre de la fourniture de services d'entretien et de maintenance pour les Systèmes

Konica Minolta. Les données à caractère personnel ne seront traitées que dans le but d'assurer le service et la maintenance. Aucune autre collecte ou utilisation des données à caractère personnel du Responsable du traitement par Konica Minolta n'a lieu. La nature spécifique du traitement dépendra des options de service et des services à distance décrits dans la présente Annexe, qui ont été choisis par le Responsable du traitement. Le Responsable du traitement peut passer d'une option de service à une autre pendant la durée du ou des Contrat(s)-cadre(s).

Le traitement des données à caractère personnel du Responsable du traitement peut avoir lieu au cours de l'approvisionnement et de la configuration des Systèmes Konica Minolta (en particulier dans le cadre d'une connexion réseau) et au cours de l'entretien physique et des travaux de maintenance sur l'équipement. Dans de très rares cas, il peut être nécessaire pour Konica Minolta de stocker temporairement le contenu d'un dispositif de stockage sur un autre dispositif de stockage afin de pouvoir réparer ou remplacer le dispositif de stockage de l'équipement sans perte de données. Le Responsable du traitement peut choisir de fournir son propre dispositif de stockage externe pour transférer toutes les données.

Les Systèmes Multifonctions et d'Impression de production Konica Minolta sont capables d'enregistrer les processus techniques dans des fichiers journaux cryptés. Konica Minolta ne lance la création de fichiers journaux que lorsque l'analyse d'erreurs devient nécessaire. Les fichiers journaux peuvent être consultés par un technicien Konica Minolta sur place, mais dans la procédure standard, les fichiers journaux sont transférés vers des serveurs appartenant à et exploités par Konica Minolta Europe (en Allemagne) dans le cadre des services à distance de Konica Minolta (Konica Minolta "Remote Service Platform" ("RSP")).

En outre, les services à distance peuvent être utilisés pour créer des copies de sauvegarde de la configuration qui peuvent être stockées sous une forme protégée par mot de passe et cryptée sur les serveurs du Responsable du traitement ou sur les serveurs de Konica Minolta Europe (en Allemagne).

Les fichiers journaux et les copies de sauvegarde de la configuration de l'appareil ne contiennent pas le contenu des opérations d'impression, de numérisation, de copie ou autres opérations similaires effectuées sur les Systèmes.

Le service et la maintenance à distance des Systèmes Konica Minolta seront effectués selon les options de service choisies par le Responsable du traitement. Konica Minolta utilise à cette fin la "Konica Minolta Remote Service Platform" ("RSP"), les connexions "Remote Panel", la solution "Konica Minolta Remote Support Tool" ou des solutions

fonctionnellement comparables. Lors de la maintenance à distance, il n'est pas possible d'éliminer complètement la possibilité de visualiser et donc de traiter des données à caractère personnel du Responsable du traitement.

Dans le cas d'un retour éventuel des Systèmes Konica Minolta au terme de la durée du Contrat-cadre, le dispositif de stockage de l'équipement sera soit détruit, soit effacé, soit retiré et remis au Responsable du traitement conformément à un accord conclu séparément. Konica Minolta est autorisée à traiter les données à caractère personnel du Responsable du traitement, mais uniquement pour le compte et selon les instructions du Responsable du traitement.

Au-delà de ce qui précède, la nature et l'objet du traitement des données par Konica Minolta peuvent être précisés plus avant dans le Contrat-cadre ou dans des accords supplémentaires.

1. B Description de la nature et de l'objet du traitement dans des solutions Safe Q Cloud

SafeQ Cloud est une solution cloud tout-en-un pour la gestion des impressions et le scannage, conçue pour les organisations qui souhaitent se décharger de la gestion d'une infrastructure d'impression informatique complexe tout en bénéficiant de tous les avantages d'une offre SaaS (Software-as-a-Service). Le logiciel est géré et hébergé (hosting) par Konica Minolta Europe dans des centres de données en Allemagne et en Suède appartenant à Konica Minolta Europe

Dans le cadre de la fourniture et du fonctionnement du service Safe Q Cloud, Konica Minolta a accès aux données personnelles du Responsable du traitement et/ou aux données personnelles d'autres tiers, c'est-à-dire d'autres responsable de traitement et personnes concernées.

Il est important de noter que Konica Minolta traite les données personnelles du Responsable du traitement dans le seul but de fournir le service. Il n'y aura pas de collecte, d'utilisation ou de traitement des données personnelles du Responsable du traitement au-delà des objectifs susmentionnés.

2.1 A) Type de données à caractère personnel dans les systèmes d'impression

Type de données à caractère personnel qui peuvent être incluses dans les copies de sauvegarde de la configuration de l'appareil : carnet d'adresses interne de l'équipement (noms d'utilisateurs IT et adresses électroniques), adresses IP, adresses MAC, numéro de série.

Catégories de données à caractère personnel éventuellement contenues dans les fichiers journaux : noms d'utilisateurs IT (p. ex. les noms d'utilisateurs Windows des utilisateurs de l'appareil), adresses e-mail des utilisateurs, adresses IP, adresses MAC, numéro de série, historique du navigateur Internet de l'appareil (URL consultées), historique de l'état d'alimentation de l'appareil, historique des 150 derniers travaux d'impression (propriétaire du travail d'impression, horodatage, nom du document).

Toutes les données enregistrées dans les fichiers journaux ne sont collectées qu'à partir du lancement de l'enregistrement des événements.

Données à caractère personnel susceptibles d'être traitées dans le cadre du service et de la maintenance sur site :
[Le type de données à caractère personnel éventuellement accessibles aux techniciens de Konica Minolta dépend des données traitées sur les Systèmes. Ces contenus ne peuvent être évalués que par le Responsable du traitement.]

☒ Données de base personnelles (p. ex. prénom et nom de famille)
☒ Données de communication (p. ex. téléphone, e-mail)
☐ Données de base des contrats (p. ex. relation contractuelle, produit/intérêt contractuel)
☐ Historique des clients (p. ex. données CRM)
☐ Données de facturation et de paiement des contrats
☐ Données de cartes de crédit et données bancaires (numéros de comptes bancaires)
☐ Données de planification et de contrôle
☐ Informations obtenues auprès de tiers (p. ex. agences de crédit, annuaires publics)
☐ Adresses IP, adresses MAC
☐ Autres :

2.1 B) Type de données à caractère personnel dans les solutions Safe Q Cloud

Lors de la fourniture et de l'utilisation du service Safe Q Cloud, Konica Minolta a accès aux données personnelles du Responsable du traitement, telles que le contenu du document et les métadonnées qu'un utilisateur final traite par le biais de la solution SafeQ Cloud.

Les données se composent de trois catégories principales :

1. Contenu du document

Le contenu du document est le contenu réel du document qu'un utilisateur final traite par le biais de la solution SafeQ Cloud.

via la solution SafeQ Cloud Print. Ce type de données peut contenir des données

personnelles.

2. Métadonnées du document

Les métadonnées du document contiennent des informations sur les travaux d'impression (voir ci-dessous).

3. Données d'application

Les données d'application contiennent les noms des utilisateurs et la configuration spécifique du client de la solution installée.

Les trois catégories principales comprennent les catégories spécifiques suivantes Données personnelles du Responsable du traitement :

☒ métadonnées du document (horodatage du travail, propriétaire du travail, noms des fichiers)
☒ adresses IP, adresses MAC
☒ noms d'utilisateurs informatiques et autres identifiants uniques
☐ Données de base personnelles (par exemple, nom, adresse)
☐ Données de communication (par exemple, téléphone, courrier électronique)
☐ Données de base contractuelles (par exemple, relation contractuelle, intérêt du produit/contrat)
☐ Historique du client (par exemple, données CRM)
☐ Détails de la facturation et du paiement des contrats
☐ Données relatives aux cartes de crédit et coordonnées bancaires (numéros de compte bancaire)
☐ informations obtenues auprès de tiers (par exemple, agences d'évaluation du crédit, bases de données publiques)
☐ Autres:

2.2 Catégories de personnes concernées

[Les catégories suivantes ne peuvent être évaluées que par le responsable du traitement].
☒ Données à caractère personnel des employés du Responsable du traitement (art. 88 GDPR)
☐ Données à caractère personnel du partenaire commercial du Responsable du traitement
☐ Données à caractère personnel des clients du Responsable du traitement
☐ Autres :

3. Sous-sous-traitants engagés

Konica Minolta Business Solutions Europe GmbH
Europaallee 17
30855 Langenhagen
Allemagne

Description du traitement commandé :

- Fournisseur de services IT pour Konica Minolta Business Solutions Allemagne (y compris l'exploitation des serveurs de service à distance et de sauvegarde Konica Minolta).
- Support de 2ème niveau pour les systèmes d'impression et Safe Q (Cloud) pour Konica Minolta Business Solutions Belgium NV
- La solution Safe Q Cloud est gérée et hébergée par Konica Minolta Europe dans des centres de données en Allemagne et en Suède, appartenant à Konica Minolta Europe.

YUSEN LOGISTICS (Benelux) BV

Middenweg 10
4782 PM Moerdijk
Pays-Bas

Description du traitement commandé :

- Fournisseur de services logistiques (livraison et installation des MFP, écrasement et/ou effacement du disque dur à la fin du Contrat-cadre).

FOUNDEVER operating corporation limited

Butts Road 53-55 Coventry Warwickshire CV1 3 BH
England

Description du traitement commandé :

Centre d'appel pour toute demande d'intervention de maintenance ou de livraison de fournitures vers le client

Konica Minolta informe le contrôleur du fait que l'Angleterre, en tant que partie du Royaume-Uni, est considérée comme un pays ayant un niveau adéquat de protection des données conformément à la décision d'adéquation de la Commission européenne (art. 45 GDPR).

I.S.A.B. NV

Huttegem 10,
8570 Anzegem
Belgique

Description du traitement commandé :

- Fournisseur de services de maintenance sur les appareils MFP de certains clients.

4. Mesures techniques et organisationnelles

1. Confidentialité

a) Contrôle de l'accès physique :

- Seules les personnes qui ont besoin de consulter des données à caractère personnel dans le cadre de leurs fonctions sont autorisées à traiter ces données.
- Les fonctions de ces personnes sont enregistrées et font l'objet d'un suivi
- Audits périodiques du contrôle d'accès.
- Contrôle d'accès dans les locaux du sous-traitant avec badge, y compris dans les salles de serveurs.
- Documentation de la présence dans les salles de serveurs

- Contrôle d'accès pour les personnes externes

b) Contrôle de l'accès au système et données:

Les mesures suivantes sont prises pour empêcher toute intrusion non autorisée dans les systèmes de traitement des données :

- l'Accès aux systèmes est possible après multi factor authentication et avec un nom d'utilisateur et un mot de passe
- Utilisation de mots de passe complexes d'au moins huit caractères répondant à au moins trois des quatre critères (majuscules, minuscules, chiffres, caractères spéciaux) et changement obligatoire du mot de passe tous les 90 jours.
- Interdiction de divulguer les mots de passe
- Enregistrement de l'attribution des droits d'accès
- Restriction de l'accès administratif au minimum
- Protection des systèmes de traitement des données contre les accès non autorisés grâce à des système firewall
- Verrouillage automatique des systèmes après une certaine période de mise hors service
- Attribution des droits d'accès sur la base d'un concept d'autorisation en fonction des besoins
- Contrôle régulier des droits d'accès
- Séparation des autorisations de droits (organisationnelles) et des attributions de droits (techniques)

c) Contrôle de la séparation :

- Contrôle des tentatives d'accès non autorisé (IDS/IPS)
- Spécification de différents profils d'utilisateurs (niveaux administrateur/utilisateur)
- Droits d'accès spécifiques et alignés sur les besoins en matière d'accès aux données
- Séparation des environnements de production et de test par des mesures techniques (serveurs virtuels, systèmes séparés, segmentation des adresses IP)

2. Intégrité

a) Contrôle des transmissions :

- Chiffrement des transferts de données, notamment lors de transferts via des réseaux publics (p. ex. SSL, TLS)
- Suppression et/ou destruction respectant la protection des données, des données, dispositifs de stockage de données et copies imprimées conformes à un concept de classe de protection
- Chiffrement des dispositifs de stockage des données
- Option d'effacement à distance pour les appareils mobiles

b) Contrôle de l'input :

- Droits d'accès régulièrement contrôlés et mis à jour
- La journalisation du traitement des données permet ultérieurement de vérifier et de déterminer si et par qui des données à caractère personnel ont été saisies, modifiées ou supprimées (p. ex. journaux de modification des données dans les systèmes ERP centralisés)
- Enregistrement et conservation, selon les besoins, des actions correspondantes menées sur les systèmes (p. ex. les fichiers journaux)
- Excl. pour les systèmes d'impressions : 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 :

- Utilisation de deux centres IT 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)
- Excl. pour les systèmes d'impressions : 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 surchauffe
- Excl. pour les systèmes d'impressions : Mesures de protection face aux coupures et surcharges de courant, p. ex. des systèmes d'alimentation électrique non interruptibles (UPS)
- Excl. pour les systèmes d'impressions : Réalisation programmée de sauvegardes de données et, si nécessaire, utilisation de procédures de redondance
- Architecture d'antivirus/firewall à plusieurs niveaux
- Procédure établie pour l'achat centralisé de matériel et de logiciels
- Capacité à rétablir l'accès dans des délais convenables (art. 32 point 1 al. c du RGPD) via global system-related back-up - concept
- Mises à jour régulières de tous les systèmes utilisés, le cas échéant
- Mise en place de protocoles pour les mesures d'urgence et la récupération des données

4. Contrôle des tâches:

- Nomination d'un délégué à la protection des données
- Accords de niveau de services avec des prestataires de services externes et engagement de ces derniers conformément au RGPD
- Formation des employés au traitement des données à caractère personnel
- Obligation pour les employés de respecter la confidentialité des données
- Protection technique par des mesures de contrôle d'accès, de contrôle de séparation et de contrôle de l'input

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

- Mise en place de processus de vérification en continu et si nécessaire, ajustement des mesures de protection des données
- Mise en place de procédures permettant de traiter un cas/infraction de protection des données
- Mise en place de directives obligatoires de l'entreprise sur le traitement des données à caractère personnel et l'utilisation des systèmes IT
- Formations correspondantes pour les employés
- Gestion des incidents (incident response management)