Accord de traitement des Données à caractère personnel

La présente Annexe est établie en application de l'article 28.3 du règlement Européen 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« règlement général sur la protection des données » ou (« RGPD »), et de la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée à tout moment (ensemble la « **Réglementation** »).

Elle fait partie intégrante des Condition Générales de Vente CENIT KEONYS FR (le « **Contrat** »).

Les termes utilisés dans la présente Annexe avec une majuscule ont le sens qui leur est attribué dans le RGPD ou dans le Contrat.

1.1. Les Parties reconnaissent que lorsque CENIT KEONYS FR traite des Données à caractère personnel pour le compte du CLIENT dans le cadre de l'exécution du Contrat, il agit en qualité de Sous-traitant et le CLIENT agit en tant que Responsable de traitement.

En tout état de cause, CENIT KEONYS FR s'engage à agir conformément aux instructions documentées du CLIENT (y compris pour le transfert de Données à caractère personnel en dehors de l'U.E.).

Les instructions du CLIENT pour le Traitement des Données à caractère personnel doivent être licites et conformes à la Règlementation ; le CLIENT est seul responsable de l'exactitude, de la qualité et de la légalité des Données à caractère personnel et des moyens par lesquels il a acquis les Données à caractère personnel.
Le détail des traitements de données faisant l'objet de la sous-traitance de données figure en Appendice 1 des présentes.

1.2. Si CENIT KEONYS FR considère qu'une des instructions du CLIENT constitue une violation du RGPD ou de toute autre disposition du droit de l'U.E. ou du droit des Etats-membres relative à la protection des données, il en informera dans les meilleurs délais le CLIENT, sans que cet avis ne constitue un avis ou une consultation juridique. CENIT KEONYS FR est en droit de suspendre l'exécution de cette instruction jusqu'à ce que le CLIENT ne la confirme ou ne la modifie.

1.3. CENIT KEONYS FR s'engage à :

a) Garantir la confidentialité des Données personnelles traitées pour le compte du CLIENT ;
b) Ne pas utiliser les Données à caractère personnel collectées en qualité de Sous-traitant du Client à d'autres fins que celles prévues à la présente Annexe sauf lorsque cela est expressément autorisé par l'Article 28 (3)(a) du RGPD ;
c) Mettre en œuvre les mesures techniques appropriées et raisonnables pour assurer la protection des Données à caractère personnel traitées pour le compte du CLIENT. En particulier, CENIT KEONYS FR s'engage à mettre en œuvre les mesures de sécurité détaillées en Appendice 2 des présentes visant à :
   - protéger la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement ;
   - rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
   - En particulier, CENIT KEONYS FR met en place uUne procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

   Le Client reconnait que ces mesures sont susceptibles d'évoluer en raison des connaissances et des développements techniques futurs, CENIT KEONYS FR est donc expressément autorisé à mettre en place des mesures alternatives à celles décrites tant que ces mesures maintiennent le niveau de sécurité général tel que décrit ci-avant.

   CENIT KEONYS FR s'engage à :
d) S'assurer que l'accès aux Données à caractère personnel est limité au personnel et ses sous-traitants ultérieurs qui ont besoin d'y accéder pour la fourniture des services prévus au Contrat ;
e) Notifier au CLIENT, par courrier électronique ou postal, dans meilleurs délais après en avoir eu connaissance, toute Violation des Données à caractère personnel, lui fournir toutes informations s'y rapportant, et prendre toutes mesures raisonnables à l'effet d'y remédier, ce dont il devra tenir informé le CLIENT. La notification devra être accompagnée de toute documentation utile afin de permettre au CLIENT de notifier cette violation à l'autorité de contrôle compétente ;
f) Aider le CLIENT, dans la mesure du possible, dans la gestion des demandes ou recours introduits par les Personnes Concernées dans l'exercice de leurs droits. Lorsque les Personnes Concernées exercent directement leurs droits auprès de CENIT KEONYS FR, ce dernier devra adresser ces demandes dès leur réception au DPO du CLIENT par courrier électronique.
g) Coopérer avec les autorités compétentes en matière de protection des données.

1.4. Le CLIENT autorise CENIT KEONYS FR à recourir à un ou plusieurs sous-traitants ultérieurs pour le Traitement des Données à caractère personnel. En particulier, le CLIENT autorise CENIT KEONYS FR à recourir à la société CENIT AG (société mère) située 54 Industrie Strasse – Stuttgart – Allemagne, société assurant la sécurité et la sauvegarde des Données hébergées par CENIT KEONYS FR. Le CLIENT accepte que CENIT AG puisse recourir à des sous-traitants ultérieurs listés en Appendice 3 pour l'exécution du Contrat. CENIT KEONYS FR s'engage à informer le CLIENT par écrit de toute modification prévue concernant l'ajout ou le remplacement de sous-traitants ultérieurs en indiquant la référence du Contrat. Le CLIENT peut s'opposer, pour des motifs justifiés et légitimes, au recours à un nouveau sous-traitant ultérieur en avertissant CENIT KEONYS FR par courrier électronique dans les dix (10) jours à compter de la réception de la notification de CENIT KEONYS FR, dans les conditions de l'article 28 paragraphe 3 du RGPD.

En tout état de cause, CENIT KEONYS FR imposera à ses sous-traitants autorisés les mêmes obligations de protection des Données à caractère personnel que celles énoncées à la présente Annexe. CENIT KEONYS FR veillera également à ce que ses sous-traitants ultérieurs ne traitent pas les Données à caractère personnel pour des finalités autres que celles nécessaires à la fourniture des services sous-traités.

1.5. Tout transfert de Donnée à caractère personnel devra être mis en œuvre conformément à la Réglementation.

Si CENIT KEONYS FR ou l'un des sous-traitants ultérieurs traite ou transfère des Données à caractère personnel hors de l'Union Européenne, dans un pays ne disposant pas d'un niveau de protection adéquat tel que défini par la Commission Européenne, le CLIENT donne mandat à CENIT KEONYS FR de signer en son nom et pour son compte avec les entités juridiques concernées un contrat de transfert de données établi sur la base des Clauses Contractuelles Types de la Commission Européenne pour le transfert de Données à caractère personnel vers des entreprises établies dans des pays tiers (les « Clauses Contractuelles pour le Transfert de Données » ou « EUSCC »). Alternativement, les transferts seront encadrés au moyen d'un mécanisme de substitution validé et reconnu par les autorités européennes comme garantissant un cadre légal adéquat pour sécuriser le Traitement de Données à caractère personnel en dehors de l'Union Européenne.

CENIT KEONYS FR précise qu'aucun transfert de Données à caractère personnel n'est réalisé hors de l'UE.

1.6. Le CLIENT pourra vérifier, au plus une fois par an, le respect par CENIT KEONYS FR de l'ensemble des obligations issues du présent accord ou pourra mandater à cet effet un auditeur de son choix pour autant qu'il ne s'agisse pas d'un concurrent de CENIT KEONYS FR.

Cet audit devra être effectué (i) pendant les heures de bureau normales de CENIT KEONYS FR, (ii) sans interférer avec les opérations commerciales de CENIT KEONYS FR, et (iii) moyennant le respect d'un préavis approprié et après consultation avec CENIT KEONYS FR. Etant précisé que la conduite d'un audit par le Client doit se limiter au périmètre des prestations fournies par CENIT KEONYS FR au Client.

Le Client supportera ses propres dépenses dans le cadre de cet audit et dédommagera CENIT KEONYS FR du coût de ses ressources internes requises pour mener l'audit sur site (sur la base du temps et du matériel selon la liste de prix alors en vigueur) si l'audit ne révèle pas un manquement grave de CENIT KEONYS FR à ses obligations en vertu de la présente Annexe (dans cette hypothèse, CENIT KEONYS FR remédiera rapidement à la violation à ses propres frais).

1.7. CENIT KEONYS FR respectera les instructions du CLIENT concernant la conservation des Données à caractère personnel et, au choix et sur demande du CLIENT, s'engage à détruire ou restituer au CLIENT, dans le délai convenu avec lui, toutes les Données à caractère personnel, y compris toutes copies qui en auraient été faites sur quelque support que ce soit, sauf en cas de nécessité de conservation requise par une loi ou réglementation.

En tout état de cause, les Données à caractère personnel traitées par CENIT KEONYS FR dans le cadre du Contrat seront conservées pendant la durée du Contrat augmentée de la durée de la prescription applicable nécessaire à CENIT KEONYS FR afin d'assurer la défense de ses droits.

En cas de suppression, CENIT KEONYS FR devra spécifier préalablement au CLIENT les modalités de suppression des Données à caractère personnel.

1.8. CENIT KEONYS FR précise par ailleurs avoir désigné un Délégué à la Protection des Données à caractère personnel (DPO) dont les coordonnées figurent ci-après : dataprotection @keonys.fr

APPENDICE 1 – DETAILS DU / DES TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

1. Prestations de services d'intégration et/ou de migration

Finalité de traitement	Finalité de traitement prédéfinie par le Client, en qualité de Responsable de traitement
Objet du traitement	Exécution des prestations prévues au Contrat conclu entre le Client et CENIT KEONYS FR
Nature des opérations de traitement	Collecte, enregistrement, structuration, interconnexion, destruction
Personnes concernées	Utilisateurs du Client
Catégories de données à caractère personnel	Données prévues au Contrat
Durée de conservation	Durée définie au Contrat

2. Prestations de services de formation

Finalité de traitement	Gestion des financements et de la prise en charge des formations professionnelles
Objet du traitement	Exécution des prestations prévues au Contrat conclu entre le Client et CENIT KEONYS FR
Nature des opérations de traitement	Collecte, enregistrement, hébergement, modification, communication, destruction
Personnes concernées	Employés du Client
Catégories de données à caractère personnel	Données prévues au Contrat
Durée de conservation	Durée définie au Contrat

3. Prestations de services de support de niveau 1 aux utilisateurs

Finalité de traitement	Gestion et suivi du support aux utilisateurs Gestion de la remontée d'informations à l'éditeur pour le support
Objet du traitement	Exécution des prestations prévues au Contrat conclu entre CENIT KEONYS FR et le Client ou l'éditeur
Nature des opérations de traitement	Collecte, enregistrement, hébergement, modification, communication, destruction
Personnes concernées	Utilisateurs du Client
Catégories de données à caractère personnel	Données prévues au Contrat
Durée de conservation	Durée définie au Contrat

APPENDICE 2 – MESURES DE SECURITE

CENIT KEONYS FR prend toutes les précautions utiles pour préserver la sécurité des données traitées, en particulier leur confidentialité, leur intégrité et leur disponibilité.

CENIT KEONYS FR déclare d'ores et déjà mettre en œuvre les mesures techniques et organisationnelles de sécurité ci-dessous.

Mesures techniques et organisationnelles

1. Mesures pour garantir la confidentialité	
1.1 Accès **Mesures destinées à empêcher les personnes non autorisées d'accéder physiquement aux bâtiments, locaux et données.**	**Disponible**
Système de verrouillage des accès physiques	X
Vitrage spécial (réduction de la visibilité)	
Sélection minutieuse des agents de sécurité externes	X
Vidéosurveillance	X
Contrôle d'accès biométrique	
Service de sécurité y compris en dehors des heures de travail	X
Vérification des passages à la réception	X
Accès limité dans le temps aux zones publiques	X
Badges d'accès (via des puces RFID)	X
Cartes de visiteur	
Enregistrement des accès des visiteurs / registre des visiteurs	X
Accompagnement des visiteurs par le personnel interne	X
Cartes de code d'accès électroniques/transpondeurs d'accès	X
Réglementation des clés	X
Politique d'autorisation d'accès	X
Zones de sécurité différenciées avec accès réglementé	X
Entrée sécurisée pour les arrivées et les livraisons	
Accès séparé et sécurisé à la salle des serveurs	X
Accès séparé et sécurisé au data center	X
Instructions spécifiques relatives à la fermeture des locaux lors du départ ou de la fin du travail	X
Sélection minutieuse du personnel de nettoyage	X
Autres mesures :	

1.2 Contrôle d'accès physique **Afin de prévenir tout accès non autorisé à, et toute utilisation de, systèmes de traitement des données. Protection des systèmes.**	**Disponible**

Attribution des droits des utilisateurs selon le principe du moindre privilège	X
Création de profils utilisateurs	X
Gestion des autorisations	X
Processus documenté pour l'attribution des droits lors de l'arrivée de nouveaux employés dans l'entreprise	X
Processus documenté pour la révocation des droits en cas de changement de département des employés	X
Processus documenté pour la révocation des droits en cas de démission d'un employé	X
Attribution fonctionnelle et/ou limitée dans le temps des autorisations utilisateur	X
Utilisation de mots de passe individuels	X
Connexion avec nom d'utilisateur et mot de passe	X
Verrouillage automatique protégé par mot de passe de l'écran après inactivité (économiseur d'écran)	X
Politique de mot de passe avec des exigences minimales de complexité : • Au moins 12 caractères • Majuscules et minuscules, caractères spéciaux, chiffres (au moins trois critères sur les quatre) • Prévention des mots de passe triviaux (par exemple, password1, password2, 123456, qwerty) • Historique des mots de passe (pas de réutilisation des 13 derniers mots de passe) • Verrouillage automatique des comptes utilisateurs après plusieurs tentatives infructueuses d'entrée de mot de passe • Procédure de réinitialisation de mot de passe raisonnablement sécurisée	X
Chiffrement des réseaux	X
Verrouillage des systèmes de traitement des données (par exemple, cage verrouillée pour les serveurs)	X
Blocage des interfaces externes (par exemple, USB)	X
Procédures d'examen et de validation des programmes pour les nouvelles installations	X
Utilisation de systèmes de prévention des intrusions	X
Utilisation de la technologie VPN	X
Utilisation d'un logiciel antivirus : Serveurs	X
Utilisation d'un logiciel antivirus : Clients	X
Utilisation d'un pare-feu logiciel	X
Utilisation d'un pare-feu matériel	X
Gestion des appareils mobiles (Mobile-Device-Management)	X
Stockage des données personnelles/supports de données dans des armoires de sécurité verrouillables ou dans des locaux sécurisés séparément	X
Encadrement sur le télétravail / travail à domicile	X
Autres mesures :	

1.3 Contrôle d'accès **Destiné à empêcher les activités non autorisées dans les systèmes de traitement des données en dehors des autorisations accordées.**	**Disponible**
Utilisation d'un concept d'autorisation basé sur les rôles	X
Examens réguliers des permissions utilisateurs attribuées	X
Limitation de l'utilisation du compte administrateur.	X
Séparation entre l'autorisation d'approbation (organisationnelle) et l'attribution des autorisations (technique)	X
Encadrement de la restauration des données depuis les sauvegardes (qui, quand, à qui).	X
Stockage des sauvegardes de données (par ex. bandes, CD) dans un coffre protégé par un accès sécurisé Restriction de l'accès libre et non surveillé aux bases de données.	X
Évaluation régulière des logs (fichiers de log)	X
Limitation temporelle des options d'accès	X
Options d'accès restreint aux ensembles de données et aux fonctions (lecture, écriture, exécution)	X
Journalisation des accès aux fichiers Journalisation des suppressions de fichiers Journalisation des modifications de fichiers Détection d'intrusion (IDS)	X
Logiciel de gestion des informations et des événements de sécurité (SIEM)	X
Accès limité aux fichiers de log (administrateur des logs uniquement)	X
Stockage des fichiers logs sur un serveur dédié aux fichiers journaux	X
Stockage chiffré des données	X
Destructeur de documents (découpe croisée, au minimum niveau 3, norme DIN 66399)	X
Conteneurs métalliques scellés (appelés bacs de protection des données), élimination par des prestataires de services	X
Destruction des supports de données - Effacement sécurisé des supports selon la norme DIN 66399.	X
Destruction physique (par exemple, destructeur pour des tailles de particules allant jusqu'à 1000 millimètres carrés maximum)	X
Démagnétisation par destruction thermique (chauffage de la surface du disque magnétique au-delà de la température de Curie du revêtement utilisé)	X
Politique de destruction des données	X
Politique de bureau propre (Clean Desk Policy)	X
Politique d'écran propre (Clean Screen Policy)	X
Autres mesures :	

1.4 Contrôle des commandesGarantir que les données traitées pour le compte de prestataires de services (sous-traitants) ne sont traitées que conformément aux instructions du client.	**Disponible**
Rédaction des contrats conformément aux exigences légales (Art. 28 RGPD)	X
Tenu d'un registre des prestataires de services existants (gestion uniforme des contrats)	X
Vérifications préalables dans les locaux du prestataire avant le début du contrat	X
Inspections régulières chez le prestataire après le début du contrat (pendant la durée du contrat)	X
Inspections sur site dans les locaux du prestataire	X
Etude de la prise en compte de la sécurité des données chez le prestataire	X
Vérification des certificats de sécurité informatique existants des prestataires	X
Le prestataire a désigné un délégué à la protection des données	X
Émission d'instructions aux prestataires pour améliorer la protection des données	X
Autres mesures :	

1.5 Contrôle de séparation **Les données collectées à des fins distinctes doivent être traitées de manière indépendante.**	**Disponible**
Séparation des données clients (capacité multi-clients du système utilisé)	X
Séparation physique des données (par exemple, systèmes ou supports de données différents)	X
Séparation logique des données (par exemple, basée sur les numéros de client ou de contrat)	X
Sauvegardes des données client sur des supports de données distincts (sans données d'autres clients)	X
Concept d'autorisation garantissant la séparation du traitement des données de chaque client de celles des autres clients.	X
Séparation des systèmes de développement, de test et de production	X
Catographie des données avec les attributs de finalités	X
En cas de données pseudonymisées : séparation du fichier de correspondance et stockage sur un autre système	X
Autres mesures :	

2. Mesures pour garantir l'intégrité

2.1 Contrôle des transferts **Garantir la sécurité des données lors de leur transmission électronique et de leur transport, ainsi que la traçabilité des transferts.**	**Disponible**
Comment les données sont-elles transférées entre le responsable du traitement et des tiers ? •Connexion VPN	X
Chiffrement des e-mails	X

•SMIME	X
•OpenPGP	
•Envoi d'e-mails avec des fichiers ZIP chiffrés	X
Échange de données via une connexion HTTPS	X
•Protocole TLS 1.2	X
Autre mode d'envoi : module adHoc de Move-It	X
Utilisation de procédures de signature	X
Méthode de signature utilisée : HSM (Hardware Security Module)	
Signature numérique des macros	X
Gestion documentée des supports de données, contrôle des inventaires	X
Chiffrement des enregistrements de données confidentielles	X
Chiffrement des supports de données mobiles (par exemple, disques durs de portables, disques durs externes, clés USB)	X
Interdiction d'emporter des sacs et autres bagages ainsi que des téléphones portables dans les zones de sécurité	X
Encadrement concernant la réalisation de copies d'enregistrements	X
Sauvegarde des disques nécessitant un transport	X
Documentation des organismes auxquels un transfert est prévu et des canaux de transmission	X
Enlèvement direct, service de messagerie, escorte de transport	X
Vérification de l'exhaustivité et de l'exactitude Autres mesures :	X

2.2 Contrôle des entrées **Pour garantir la traçabilité de qui, quand et comment des données personnelles ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données.**	**Disponible**
Journalisation technique des saisies, modifications et suppressions de données.	X
Évaluation manuelle ou automatisée des logs.	X
Permissions utilisateur différenciées :	X
•Noms d'utilisateur individuels, pas de groupes d'utilisateurs.	X
•Attribution des droits d'entrée, de modification et de suppression de données basée sur un concept d'autorisation.	X
•Accès différencié aux champs des bases de données.	X
Définition organisationnelle des responsabilités de soumission.	X
Serveur de journaux dédié.	X
Encadrement des autorisations d'accès aux serveurs de logs (LogAdmin).	X
Encadrement des périodes de conservation à des fins d'audit/vérification.	X
Autres mesures :	

3. Mesures pour garantir la disponibilité et la résilience	
3.1 Vérification de la disponibilité **Destinée à protéger les données contre une destruction ou une perte accidentelle.**	**Disponible**
Systèmes d'alarme incendie dans les salles serveurs	X
Détecteurs de fumée dans les salles serveurs	X
Portes coupe-feu	X
Systèmes d'extinction d'incendie sans eau dans les salles serveurs	X
Capteurs d'eau dans les salles des serveurs	X
Protection contre la foudre et les surtensions	X
Salles des serveurs climatisées	X
Salles des serveurs dans un compartiment coupe-feu distinct	X
Hébergement des systèmes de sauvegarde dans des pièces séparées et dans un compartiment coupe-feu distinct	X
Salles des serveurs non situées sous ou à côté des installations sanitaires	X
Restriction de l'accès aux salles des serveurs au personnel nécessaire	X
Message d'alarme en cas d'accès non autorisé aux salles serveurs	
Stockage des supports d'archives dans des conditions de conservation nécessaires (climatisation, exigences de protection, etc.)	X
Extincteur au CO2 à proximité immédiate des salles serveurs	X
Système UPS (alimentation sans interruption)	X
Générateur électrique	
Armoires coupe-feu	
Coffre-fort pour la confidentialité	X
Sauvegarde des données documentée et concept de sauvegarde	X
Exécution des sauvegardes de données et création de copies de sauvegarde à l'aide d'un serveur central de sauvegarde	X
Surveillance du processus de sauvegarde par le service d'assistance	X
Tests réguliers de récupération des données	X
Élaboration de documents complets et de plans pour la reprise des activités	X
Miroir des disques durs (par exemple, RAID) en fonction de la classe de protection	X
Partitions distinctes pour le système d'exploitation et les données	X
Archivage externe (externalisation des données)	X
Plan d'urgence en place (Norme BSI 100-4)	X
Garantie de la lisibilité technique à long terme des supports de stockage de sauvegarde	X
Autres mesures :	

3.2 Résilience (résistance et contrôle des défaillances) **Permettre aux systèmes de gérer les changements liés aux risques et de démontrer leur tolérance et leur capacité de compensation face aux perturbations.**	**Disponible**
Alimentation électrique redondante Alimentation sans interruption (UPS) pour pallier les coupures de courant pour tous les systèmes centraux	X
Redondance de la connexion de données	X
Redondance du système de climatisation dans le centre de données.	X
Centres de données alternatifs disponibles (hot ou cold stand-by) : centre de sauvegarde disponible	X
Autres systèmes/procédures redondants : Utilisation d'une solution de réseau de stockage (SAN) haute disponibilité	X
Équipe d'intervention en cas d'urgence informatique (CERT)	X
Utilisation de la répartition de charge (load balancing)	X
Délimitation des composants critiques	X
Réalisation de tests de pénétration	X
Renforcement des systèmes (désactivation des composants inutiles)	X
Activation immédiate et régulière des mises à jour logicielles et des micrologiciels disponibles	X
Sensibilisation régulière des employés (au moins une fois par an)	X
Processus de signalement immédiat des incidents à l'informatique connu de tous les employés	X
Souscription d'une assurance cyber	X
Autres mesures :	

4. Mesures d'examen, d'évaluation et d'analyse périodiques

4.1 Procédures **Pour garantir l'efficacité des mesures de sécurité des données.**	**Disponible**
Registres des traitements (Art. 30 I et II du RGPD) mis à jour chaque année.	X
Notification des nouvelles procédures de traitement des données ou des modifications apportées aux procédures existantes au délégué à la protection des données.	X
Notification des nouvelles procédures de traitement des données ou des modifications apportées aux procédures existantes au responsable de la sécurité informatique.	X
Les processus de signalement des nouvelles procédures ou des modifications sont documentés.	X
Test de l'efficacité des mesures de sécurité au moins une fois par an.	X
En cas de constatations négatives dans le cadre des tests, les mesures de sécurité sont adaptées en fonction des risques identifiés.	X

Un processus de réponse aux violations de sécurité (attaques) et aux perturbations des systèmes est en place (gestion des réponses aux incidents).	X
Documentation des incidents de sécurité et processus documenté pour leur traitement.	X

4.2 Autres éléments de gestion de la protection des données	**Disponible**
Utilisation de paramètres logiciels respectueux de la vie privée	X
Utilisation d'un logiciel de gestion de la protection des données Désignation d'un délégué à la protection des données.	X
Désignation d'un responsable de la sécurité informatique.	X
Processus documenté pour la gestion des incidents liés à la protection des données	X
Responsabilités clairement définies pour le traitement des incidents de confidentialité et de sécurité.	X
Processus documenté pour garantir les droits des personnes concernées	X
Stockage centralisé des directives/procédures accessible à tous les employés	X
Vérifications périodiques par le délégué à la protection des données	X
Coordination régulière entre le Conseil d'administration et le délégué à la protection des données	X
Audits internes et externes réguliers	X
Directives détaillées pour les employés dans le Manuel de protection des données	X
Formation annuelle des employés	X
Certifications pertinentes en matière de protection des données et de sécurité des données conformément aux normes ISO 9001, ISO 27001 et VDA TISAX	X

Autres mesures :

APPENDICE 3 – LISTE DES SOUS-TRAITANTS ULTERIEURS

1. **BMC Software GmbH**

Heriotstrasse 1, 60528 Frankfurt (UE)
Gestion des tickets et support de 1er niveau

2. **Adobe Systems Software Ireland Ltd.**

4-6 Riverwalk, Citywest Business Campus, Dublin (UE)
Signature électronique de documents

3. **Axsos AG**

Konrad-Zuse-Weg 1, 72555 Metzingen (UE)
Plateforme d'outil d'apprentissage en ligne (e-learning)