Contrat de sous-traitance selon la LPD ou par analogie avec le RGPD

entre ALSO Suisse SA

- responsable / sous-traitant - ci-après dénommé le donneur d'ordre

et

les fournisseurs

- sous-traitant - ci-après dénommé le contractant

1. Objet et durée du mandat

(1) Objet

L'objet du contrat de traitement des commandes est l'exécution des tâches par le contractant conformément au contrat individuel, en particulier:

- assistance technique et maintenance
- exécution des commandes
- prestations informatiques
- service à la clientèle comme la réparation et les éventuelles prestations de garantie
- les services de cloud computing, chacun dans le cadre du contrat de produit, de service, d'achat et/ou d'entreprise correspondant.

(2) Durée

La durée du présent contrat de sous-traitance (durée) correspond à la durée du contrat individuel (ci-après contrat individuel).

(3) Conclusion

Le présent contrat de traitement des données à caractère personnel entre en vigueur dès sa signature, avec effet rétroactif au 1er septembre 2023.

(4) Étendue

Le présent contrat de sous-traitance s'applique exclusivement au cas où le sous-traitant traite des données personnelles pour le compte du client en tant que sous-traitant. C'est exclusivement le cas en relation avec les activités mentionnées au ch. 1 (1).

Pour les autres traitements, lorsqu'il n'y a pas de sous-traitance, le contractant publie ses principes de traitement des données personnelles ainsi que les éventuelles mises à jour sur Internet sous Insérer URL (Déclaration de protection des données du contractant).

Lors du traitement des données personnelles (telles que définies dans la LPD), le contractant et le donneur d'ordre respectent le droit suisse applicable en matière de protection des données (loi suisse sur la protection des données, LPD et ses ordonnances d'exécution). Lorsque la législation européenne sur la protection des données (Règlement (UE) 2016/679 (Règlement général sur la protection des données, RGPD)) s'applique aux clients finaux du donneur d'ordre, le contractant respecte le RGPD par analogie.

2. Concrétisation de la teneur du mandat

(1) Nature et but du traitement de données prévu
La nature et la finalité du traitement des données à caractère personnel par le contractant pour le compte du donneur d'ordre découlent concrètement du contrat individuel conclu et de ses annexes.

Nature du traitement de données	But du traitement de données
Assistance technique, traitement des tâches, prestations informatiques, service clients, services cloud	Traitement des tâches, assistance technique, prestations informatiques, service clients, services cloud

L'exécution du traitement de données convenu contractuellement a lieu exclusivement en Suisse ou dans un État membre de l'Union européenne ou dans un autre État partie à l'accord sur l'Espace économique européen ou dans un pays pour lequel il existe une décision d'équivalence de la Commission européenne ou du Conseil fédéral suisse, conformément à l'annexe 1 de l'OPDo.

(2) Nature des données

Les types/catégories de données suivants constituent l'objet du traitement des données à caractère personnel (énumération/description des catégories de données):

☒ données de base des personnes

☒ coordonnées (par ex. téléphone, e-mail)

☒ données de base du contrat (relation contractuelle, intérêts contractuels ou pour le produit)

☒ historique du client

☒ données de facturation et de paiement du contrat

☒ données de planification et de contrôle

☒ renseignements donnés (par des tiers, par ex. des sociétés de renseignement ou des répertoires publics)

(3) Catégories de personnes concernées

☒Les catégories de personnes concernées par le traitement comprennent:

- ☒ les collaborateurs du donneur d'ordre
- ☐ les fournisseurs du donneur d'ordre
- ☒ les clients du donneur d'ordre

☐ les agents commerciaux/revendeurs

☐ les interlocuteurs

☐ ……

3. Obligations du donneur d'ordre

(1) Le donneur d'ordre est responsable de l'adoption de règles appropriées en matière de protection des données dans les relations contractuelles avec des tiers et avec ses clients finaux et d'informer les tiers concernés du traitement, de l'enregistrement et de la transmission de données et, le cas échéant, du traitement de données par le contractant. Le donneur d'ordre est responsable de l'obtention des autorisations nécessaires à cet effet auprès des tiers concernés, dans la mesure où la loi l'exige, et de les présenter au contractant sur demande.
(2) Le donneur d'ordre autorise le contractant à traiter les données personnelles du donneur d'ordre et/ou de ses clients finaux qui sont traitées dans le cadre de la convention individuelle, qu'elles proviennent du donneur d'ordre ou de tiers, au sens des lois sur la protection des données.
(3) Le donneur d'ordre prend connaissance du fait que, pour remplir ses obligations contractuelles, le contractant peut transmettre à ses fournisseurs des informations détaillées sur les produits, les quantités, les chiffres d'affaires ainsi que les données relatives aux noms et adresses du client et de ses clients finaux (Sell-Out-Reporting).

4. Mesures techniques et organisationnelles

(1) Le donneur d'ordre et le contractant garantissent, par des mesures techniques et organisationnelles appropriées, une sécurité des données adaptée au risque. Celle-ci se base sur l'annexe 1, qui correspond aux directives selon l'art. 3 LPD ou par analogie à l'art. 28, al. 3, let. c, 32 RGPD, en particulier en relation avec l'art. 1- 4 OPDo ou par analogie à l'art. 5, al. 1, al. 2 RGPD.
(2) Pour garantir une sécurité adéquate des données, le donneur d'ordre et le contractant doivent déterminer le besoin de protection des données personnelles et définir les mesures techniques et organisationnelles appropriées au regard du risque (art. 1 OPDo et par analogie à l'art. 32, al. 1, du RGPD). Le donneur d'ordre et le contractant doivent prendre des mesures techniques et organisationnelles afin que les données traitées ne soient accessibles qu'aux personnes autorisées (confidentialité), qu'elles soient disponibles en cas de besoin (disponibilité), qu'elles ne puissent être modifiées sans droit ou par mégarde (intégrité), qu'elles soient traitées de manière à être traçables (traçabilité) en fonction de leur besoin de protection. Les détails figurent à l'annexe 1.
(3) Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement. Dans la mesure où il est possible au contractant de mettre en œuvre des mesures alternatives adéquates. Dans ce cadre, le niveau de sécurité ne peut pas être inférieur aux mesures fixées. Les modifications importantes sont documentées.

4. Correction, limitation et suppression des données personnelles
(1) Le contractant ne peut pas corriger, supprimer ni limiter le traitement des données traitées dans le cadre du mandat de son propre chef, mais uniquement sur instruction documentée du donneur d'ordre. Dans la mesure où une personne concernée s'adresse directement au contractant à ce sujet, le

contractant transmettra immédiatement cette requête au donneur d'ordre, s'il est évident pour le contractant que le client doit être attribué au donneur d'ordre.

5. Assurance qualité et autres devoirs du contractant

Le contractant garantit notamment le respect des directives suivantes (par analogie avec l'art. 28 à 33 du RGPD):

a) Le contractant a désigné un conseiller à la protection des données. Ses coordonnées actuelles sont indiquées sur la page d'accueil du contractant de façon à être facilement accessibles.

b) Le contractant garantit le respect de la confidentialité entre les parties conformément à l'art. 3 al. 1 OPDo ou par analogie à l'art. 28, al. 3, p. 2, let. b, 29, 32, al. 4 RGPD. Le contractant n'a recours lors de la réalisation des travaux qu'à des employés qui s'engagent à respecter la confidentialité et ayant été préalablement familiarisés avec les dispositions concernant la protection des données pertinentes pour eux. Le contractant et toute personne sous ses ordres ayant accès à des données à caractère personnel peuvent traiter ces données uniquement conformément aux instructions du donneur d'ordre, y compris les attributions consenties dans le présent contrat, à moins qu'ils ne soient légalement tenus de les traiter.

c) Le donneur d'ordre et le contractant collaborent sur demande avec les autorités de surveillance lors de l'accomplissement de leur mission.

d) L'information immédiate du donneur d'ordre au sujet des contrôles et des mesures de l'autorité de surveillance dans la mesure où elles se rapportent au présent mandat, dans la mesure où la loi le permet. Cela s'applique aussi dans la mesure où une autorité responsable enquête, dans le cadre d'une procédure d'infraction administrative ou pénale concernant le traitement des données à caractère personnel lors de la sous-traitance chez le contractant.

e) Dans la mesure où le donneur d'ordre fait l'objet pour sa part d'un contrôle de l'autorité de surveillance, d'une procédure administrative ou pénale, d'une revendication de responsabilité par une personne concernée ou un tiers ou d'une autre revendication en lien avec la sous-traitance chez le contractant, le contractant doit l'aider de son mieux.

f) Le contractant contrôle régulièrement les procédures internes ainsi que les mesures techniques et organisationnelles pour garantir que le traitement sous sa responsabilité est effectué conformément aux exigences de la législation sur la protection des données en vigueur et que la protection des droits de la personne concernée est garantie en fonction du risque.

6. Relations de sous-traitance

(1) Les prestations de services qui se rapportent directement à l'exécution de la prestation principale doivent être considérées comme des relations de sous-traitance au sens du présent règlement. Ne font pas partie de cette catégorie les prestataires accessoires que le contractant fournit, par exemple, en tant que services de télécommunication, services postaux/de transport. En revanche, d'autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résistance du matériel et des logiciels des installations de traitement des données en font partie. Le contractant est toutefois tenu, pour garantir la protection des données et la sécurité des données du donneur d'ordre, également en cas de

prestations accessoires délocalisées, de passer des dispositions contractuelles appropriées et conformes à la législation, et de prendre des mesures de contrôle.

(2) Le donneur d'ordre donne par la présente une autorisation générale pour que le contractant puisse également transférer des données à un tiers, à condition que celui-ci traite les données personnelles en Suisse ou dans un État membre de l'Union européenne, dans un autre État partie à l'accord sur l'Espace économique européen ou dans un pays pour lequel la Commission européenne ou le Conseil fédéral suisse a rendu une décision d'adéquation conformément à l'annexe 1 du RGPD. En l'absence de décision d'équivalence, le contractant prend les mesures appropriées et nécessaires conformément à l'art. 16 al. 2 LPD ou art. 46 RGPD. Le contractant informe le donneur d'ordre de l'identité du tiers et du lieu où le traitement des données a lieu, ainsi que des mesures qu'il a prises s'il a décidé de transférer les données se fonde sur l'art. 16 al. 2 LPD ou art. 46 RGPD.

(3) Le contractant informe le donneur d'ordre de toute modification envisagée concernant l'ajout ou le remplacement d'autres sous-traitants ce qui permet au donneur d'ordre de s'opposer à des modifications de ce type en donnant les raisons dans un délai de 14 jours à partir de la communication, sinon la sous-traitance est considérée comme approuvée. L'information au donneur d'ordre se fait par e-mail. En cas d'opposition du donneur d'ordre et si le choix d'un autre sous-traitant n'est pas possible, le donneur d'ordre peut exceptionnellement mettre un terme au contrat de sous-traitance ainsi qu'au contrat individuel sans aucun droit à remboursement.

(4) Le contractant sélectionnera avec soin des sous-traitants selon leurs aptitudes, en particulier les exigences de la LPD, et effectuera des contrôles réguliers. La transmission de données à caractère personnel du donneur d'ordre vers les sous-traitants et la première intervention de ceux-ci ne sont autorisées qu'à partir du moment où toutes les conditions pour une sous-traitance sont remplies. L'ensemble des dispositions contractuelles dans la chaîne contractuelle doivent être imposées aux autres sous-traitants.

(5) Cela n'affecte pas la transmission de données à des responsables indépendants (comme les concédants de licence) au sens de la LPD, notamment lorsque vous concluez votre propre contrat avec des clients finaux.

7. Droits de contrôle du donneur d'ordre

(1) Le donneur d'ordre a le droit, en commun accord avec le contractant, de vérifier les prestations conformément à l'étendue des prestations du contrat principal ou de faire effectuer des vérifications par un contrôleur soumis au secret professionnel ou à désigner au cas par cas une fois par an pendant 2 jours au maximum durant les heures habituelles de bureau (audit). Il a le droit de s'assurer, par des contrôles par sondage, qui doivent être notifiés au moins 10 jours à l'avance, du respect de la présente convention par le contractant dans son activité commerciale.

(2) La preuve du respect des mesures techniques et organisationnelles, qui ne concernent pas uniquement le mandat concret, peut être apportée par une certification selon une procédure de certification approuvée, des attestations actuelles, des rapports ou des extraits de rapports d'audits réalisés par des instances indépendantes (p. ex. commissaires aux comptes, auditeurs, délégués à la protection des données, service de sécurité informatique, auditeurs chargés de la protection des

données, auditeurs qualité) ou une certification appropriée par un audit de sécurité informatique ou de protection des données.
(3) pour permettre la réalisation de contrôles par le donneur d'ordre, le contractant peut faire valoir un droit à rémunération. Dans la mesure où une vérification/un audit du donneur d'ordre entraîne un besoin d'adaptation, celui-ci doit être appliqué à l'amiable. Les coûts sont alors à la charge du contractant s'il ne s'agit pas de directives spécifiques à la branche.

8. Communication en cas d'infraction

(1) Les deux parties s'aident mutuellement à respecter les obligations légales en matière de sécurité des données à caractère personnel, les obligations de notification en cas de pannes ou de perte de données, les évaluations d'impact sur la protection des données et les consultations préalables. Elles comprennent entre autres:

a) l'obligation de notifier sans délai à l'autre partie les violations de données à caractère personnel, le plus rapidement possible à compter de leur découverte, au moyen du formulaire de notification figurant à l'annexe 2;
b) l'obligation de soutenir l'autre partie dans le cadre de son devoir d'information vis-à-vis des personnes concernées et, dans ce contexte, de mettre immédiatement à disposition de celui-ci l'ensemble des informations pertinentes;
c) le soutien du donneur d'ordre pour son évaluation d'impact sur la protection des données; et
d) le soutien du donneur d'ordre dans le cadre de consultations préalables avec l'autorité de surveillance.

(2) Pour les services d'assistance qui ne font pas partie du cahier des charges du contrat individuel ou qui ne sont pas imputables à un manquement du contractant, ce dernier peut demander une rémunération.

9. Autorité du donneur d'ordre

(1) Le donneur d'ordre donne ses instructions par écrit. Le contractant doit informer sans délai le donneur d'ordre lorsqu'il est d'avis qu'une instruction enfreint des dispositions de protection des données. Le contractant est habilité à suspendre la réalisation des instructions correspondantes jusqu'à ce qu'elles soient confirmées ou modifiées par le donneur d'ordre.

10. Suppression et restitution de données à caractère personnel

(1) Des copies ou des duplicatas des données ne sont pas établis sans que le donneur d'ordre en ait connaissance. Les copies de sécurité, dans la mesure où elles sont nécessaires pour garantir un traitement correct des données et où elles ont fait l'objet d'un mandat à cet effet, ainsi que les données

nécessaires en vue de respecter les obligations légales de conservation, ne sont pas concernées par ce point.

(2) Après la clôture des travaux convenus contractuellement ou plus tôt sur instruction du donneur d'ordre (au plus tard à l'expiration du contrat individuel), le contractant doit remettre au donneur d'ordre l'ensemble des documents étant entrés en sa possession, des résultats de traitement et d'utilisation créés ainsi que les bases de données qui sont en lien avec le mandat spécifique, ou, après accord préalable, les détruire irrévocablement. Il en va de même pour les documents de tests et à jeter. Le procès-verbal de suppression doit être présenté au donneur d'ordre.
(3) Les documentations et correspondances servant de preuve au bon traitement des données conformément au mandat doivent être conservées par le contractant conformément aux délais d'archivage ou de conservation légaux correspondants après l'échéance du contrat.

11. Stipulations finales

(1) La responsabilité du contractant est exclusivement régie par l'accord de prestation dans le cadre du contrat individuel correspondant.

(2) Toute compensation est exclue.

(3) Seul le droit matériel suisse est applicable, à l'exclusion du droit international privé (LDIP, RS 291) et des conflits de lois multinationaux.

(4) Le tribunal d'Emmen est seul compétent.

_____, le _____ _____, le _____

Donneur d'ordre: **Contractant:**

_____ _____

(signature / cachet de l'entreprise) (signature / cachet de l'entreprise)

_____ _____

(fonction du signataire) (fonction du signataire)

_____ _____

(Nom du signataire en clair) (Nom du signataire en clair)

Annexe 1 – Mesures techniques et organisationnelles

1. Confidentialité (art. 2 let. a OPDo, par analogie avec l'art. 32, al. 1, let. b RGPD)

Contrôles d'accès physiques

Pas d'accès non autorisé aux systèmes de traitement des données.

But: Ces mesures visent à garantir que les personnes non autorisées se voient refuser l'accès «physique» aux installations de traitement des données utilisées pour traiter des données à caractère personnel.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Système de contrôle d'accès (lecteur de badge, système de fermeture)
X	Mesures de sécurité des locaux
X	Portes de sécurité, fenêtres de sécurité
X	Enregistrement des visiteurs
X	Surveillance
X	Barrières lumineuses, détecteurs de mouvement
X	Sécurité des portes (système de fermeture, serrure à code, serrure d'accès biométrique, serrures de sécurité)
X	Gestion des clés / documentation de l'affectation des clés
X	Sécurité également en dehors des heures de travail grâce à un système d'alarme et/ou à la sécurité des installations
X	Règles pour les invités / visiteurs / personnes extérieures à l'entreprise
X	Badges visiteurs
X	Mesures de protection particulières de la salle des serveurs (système d'alarme-eau)
X	Cartes de collaborateur et de légitimation (port obligatoire)
X	Zones restreintes pour les visiteurs externes et le personnel interne
X	Sélection rigoureuse du personnel de nettoyage
X	Documentation des mesures de contrôle d'accès
X	Surveillance des accès

Contrôle d'accès physique: pas d'accès non autorisé au système.

But: Ces mesures visent à garantir que seules les personnes autorisées peuvent accéder aux systèmes de traitement des données et qu'elles sont les seules à pouvoir les utiliser.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Authentification personnelle et individuelle des utilisateurs lors de la connexion au réseau du système ou de l'entreprise
X	Procédure de mot de passe (règles concernant les mots de passe)
X	Authentification multifactorielle
X	Protection du BIOS par mot de passe
X	Login système supplémentaire pour des applications spécifiques

X	Attribution de clients individuels et d'identifiants uniquement pour certaines fonctions
X	Verrouillage automatique du client après un certain temps d'inactivité de l'utilisateur (également écran de veille protégé par un mot de passe ou commutation automatique en mode pause)
X	Documentation électronique de tous les mots de passe (pas de mots de passe utilisateur) et chiffrement de cette documentation pour éviter tout accès non autorisé
X	Cartes à puce personnalisées
X	Verrouillage du boîtier
X	Utilisation de systèmes de détection d'intrusion
X	Utilisation d'un logiciel antivirus/anti-malware
X	Utilisation de systèmes de pare-feu
X	Contrôle d'accès au réseau
X	Attribution de profils d'utilisateurs aux systèmes informatiques
X	Utilisation de la technologie VPN
X	Utilisation de mécanismes de chiffrement des fichiers
X	Chiffrement des disques durs mobiles Supports de données dans les terminaux mobiles (ordinateurs portables, smartphones, etc.) Supports de stockage externes (clés USB, cartes mémoire, etc.)
X	Pas d'appareil sans mot de passe ou code de verrouillage avec accès aux données de l'entreprise
X	Obligation de respecter la confidentialité des données conformément à la nLPD
X	Destruction en bonne et due forme de disques durs
X	Guide pour l'utilisation privée des équipements informatiques
X	Directive BYOD (Bring your own device)
X	Directive pour les stations de travail mobiles (par ex. ordinateur portable)
X	Vérification des antécédents des collaborateurs ayant un accès privilégié à l'information
X	L'accès aux sites Internet externes est surveillé
X	Accès limité aux informations d'archives
X	Contrôle d'accès au code source des logiciels
X	Contrôles d'accès documentés

Contrôle d'accès aux données

Pas de lecture, de copie, de modification ou de suppression non autorisées au sein du système.
E.B. Concepts d'autorisation et droits d'accès adaptés aux besoins, journalisation des accès.

But:
Ces mesures visent à garantir que seules des personnes ont accès au système de traitement des données et que l'accès est limité exclusivement aux données à caractère personnel soumises à cette autorisation d'accès, de sorte que les données ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le traitement, l'utilisation et après le stockage.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Gérer les autorisations

X	Autorisations finement graduées
X	Profils
X	Rôles
X	Documentation des autorisations
X	Procédures d'approbation pour l'octroi des autorisations
X	Évaluations/consignation
X	Audit/contrôle
X	Chiffrement des CD/DVD-ROM, des disques durs externes et/ou des ordinateurs portables (par ex. via le système d'exploitation, Safeguard, PGP, Veracrypt, etc.)
X	Principe du double contrôle
X	Séparation des responsabilités
X	Profils d'autorisation liés aux tâches
X	Réduction au minimum des personnes détenant des droits d'administrateur
X	Effacement des supports de données avant leur recyclage
X	Utilisation de destructeurs de documents ou de prestataires de services pour la destruction de documents
X	Conservation sûre des supports de données
X	Destruction en bonne et due forme de disques durs
X	Consignation de la destruction
X	Vérification régulière des autorisations
X	Enregistrement, évaluation et surveillance des fichiers journaux (tentatives d'authentification infructueuses et réussies)
X	Onboarding et offboarding documentés des collaborateurs
X	Contrôle des absences (accès aux données de la personne absente)
X	Contrôles d'accès documentés

Contrôle de la séparation:
Traitement séparé des données collectées à des fins différentes. (P. EX. Sandboxing, multi-mandants)

But:
Le traitement des données à caractère personnel dans un but précis devrait être garanti sur le plan technique. Cela signifie que les données collectées à des fins différentes doivent également être traitées séparément.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Systèmes séparés
X	Bases de données séparées
X	Autorisations
X	Séparation par des règles d'accès
X	Séparation des systèmes de test, de production, de développement et d'archivage

Autres:

Le traitement des données à caractère personnel est effectué de sorte que les données ne puissent plus être associées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient stockées séparément et que des mesures techniques et organisationnelles appropriées aient été prises.

2. Intégrité (art. 2 let. b OPDo, par analogie avec l'art. 32, al. 1, let. b RGPD)
Contrôle de validation

Pas de lecture, de copie, de modification ou de suppression non autorisée pendant le transport ou la transmission électronique. (par ex. chiffrement, VPN, signature, etc.)

But:
Ces mesures visent à garantir que le support de données ne puisse pas être lu, copié, modifié ou retiré sans autorisation pendant le transport ou la transmission électronique, ou à vérifier et constater où la transmission de données à caractère personnel est prévue au moyen des possibilités de transmission de données. Dans cette mesure, les contrôles du transport et des supports de données sont combinées par le biais du contrôle du transfert.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Classification des informations
X	Chiffrement des e-mails
X	Chiffrement des CD/DVD-ROM, des disques durs externes et/ou des ordinateurs portables (par ex. via le système d'exploitation, Safeguard, PGP, Veracrypt, etc.)
X	Connexions de données chiffrées (VPN)
X	Consignation (consignation des audits)
X	Wi-Fi sécurisé
X	Chiffrement SSL pour l'accès au web
X	Ordonnance portant sur la destruction de supports de données
X	Destruction en bonne et due forme de disques durs
X	Sélectionner soigneusement le personnel de transport pour le transport manuel
X	Aperçu des opérations régulières de retrait et de distribution
X	Procédures de détection et de protection contre les logiciels malveillants
X	Saisie sécurisée dans le centre de calcul
X	Gestion des supports de données
X	Blocage séparé des supports de données confidentiels
X	Destruction contrôlée des supports de données (p. ex. erreurs d'impression,)
X	Effacement des supports de données avant leur remplacement
X	Impression sécurisée
X	Maintenance des logiciels, du matériel + des appliances

Contrôle de la saisie de données:
Déterminer si des données à caractère personnel ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données et par qui, grâce à la journalisation et à la gestion des documents

But:
Ces mesures visent à garantir la traçabilité d'une opération de traitement (saisie, modification, suppression) de données à caractère personnel. Cela signifie que l'auteur, le contenu et le moment du stockage des données doivent être déterminés.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Droits d'accès / Concept d'autorisation
X	Journalisation au niveau du système
X	Sécurité/logiciel de journalisation
X	Responsabilités fonctionnelles
X	Principe des «yeux multiples»
X	Obligation de respecter la confidentialité des informations et des données, ainsi que les secrets commerciaux et professionnels.

3. Disponibilité et capacité de résistance

Contrôle de la disponibilité des quantités

Protection contre la destruction ou la perte accidentelle ou intentionnelle, par ex: concept de sauvegarde (en ligne/hors ligne, sur site/hors site), alimentation électrique ininterrompue, protection antivirus, pare-feu, canaux de notification, plans d'urgence.

But:
Il convient de s'assurer que les données à caractère personnel ne sont pas détruites par inadvertance et qu'elles sont protégées contre tout risque de perte. Il faut s'assurer que les systèmes utilisés puissent être restaurés en cas de panne.

Mesures prises au sein de l'entreprise:

Existantes	Mesures
X	Stratégie de sauvegarde
X	Concept de rétention de sauvegarde
X	Locaux de serveurs qui ne sont pas situés sous des systèmes/équipements conducteurs d'eau
X	Alimentation électrique sans coupure (batterie, diesel)
X	Surveillance de la température et de l'humidité dans les salles de serveurs
X	Protection contre les virus/menaces, pare-feu
X	Climatisation dans les salles informatiques
X	Protection contre l'incendie et l'extinction (systèmes d'alarme incendie, appareils d'extinction)
X	Alarme
X	Possibilités d'archivage appropriées
X	Plan alternatif
X	Exercice d'urgence
X	Plans de catastrophe, BCM
X	Plans d'erreurs et de restauration, etc.

X	Centre de données redondant (interne/externe)
X	Connexion redondante des données des centres de données au réseau de l'entreprise
X	Matériel redondant
X	Mise en miroir des données
X	Maintenance des logiciels, du matériel + des appliances

4. Procédures de contrôle, d'évaluation et de suivi réguliers

Gestion de la sous-traitance:

Pas de sous-traitance du traitement des données sans instructions correspondantes du donneur d'ordre, par ex. rédaction claire du contrat, gestion formalisée de la sous-traitance, sélection stricte du prestataire de services, obligation de paiement préalable, vérifications.

But:
Le contractant doit veiller à ce que les données à traiter dans le cadre de la sous-traitance ne soient traitées que conformément aux instructions du donneur d'ordre. L'obligation du donneur d'ordre de donner des instructions aux contractants y est indirectement liée.

Les mesures suivantes s'appliquent dans l'entreprise:

Existantes	Mesures
X	Contrat écrit de sous-traitance du traitement des données avec des sous-traitants, contenant des dispositions sur les droits et obligations du contractant et du donneur d'ordre.
X	Contrôle régulier du respect par les sous-traitants des obligations découlant des contrats de sous-traitance du traitement des données.
X	Formation de tous les collaborateurs autorisés
X	Recyclage régulier
X	Respect de la confidentialité et du secret des données par les collaborateurs
X	Audits réguliers de la protection des données par le délégué à la protection des données de l'entreprise
X	Identification des interlocuteurs et des chefs de projet responsables pour la mission concrète.
X	Sélectionner soigneusement le contractant

Annexe 2 – au contrat de sous-traitance: Formulaire de notification

Notification à: la personne responsable de la protection des données ou de la protection des informations du donneur d'ordre / CONTRACTANT

CONTRACTANT / DONNEUR D'ORDRE	
Période/date de l'incident	
Date et heure de la constatation	
Description de l'incident	
Catégories de données concernées	
Nombre de personnes concernées	
Systèmes informatiques concernés	
Service responsable chez le SOUS-TRAITANT	
Nom et coordonnées du délégué à la protection des données ou du conseiller en la matière	
Auteur + date de la notification	
Qui a été informé par qui (autorités de protection des données, personnes concernées, autorités de contrôle) et, dans l'affirmative, quelle a été la teneur de la communication	
Source de l'information sur la violation de la protection des données	
Description des conséquences de l'incident	
Description des mesures éventuellement déjà prises par le SOUS-TRAITANT (en tenant compte du fait qu'aucune preuve n'est détruite)	
Une procédure pénale a-t-elle été engagée?	
Description des mesures techniques et organisationnelles supplémentaires futures	
Mesures d'atténuation des dommages causés par l'incident	
Évaluation globale des risques	