www.orderbird.com
hello@orderbird.com

Accord sur le traitement des commandes

Entre

_____

(Nom)

_____

(Adresse)

– Donneur d'ordre –

et

orderbird AG

Ritterstraße 12 – 14. ent. 4

10969 Berlin

– Preneuse d'ordre –

Préambule

Par le contrat du _____ (appelé ci-après « contrat principal »), les parties ont créé une obligation de traitement des données de commande. Le présent accord sur le traitement des commandes devrait régler en détail les obligations des parties en matière de protection des données.

Les parties conviennent que le présent accord s'applique à toutes les activités prévues dans le cadre du traitement des données à caractère personnel conformément au contrat principal réalisées par les employés ou les sous-traitants de la preneuse d'ordre.

1. L’objet de l’accord

(1) La preneuse d’ordre traite les données à caractère personnel pour le compte du donneur d’ordre. Cela comprend les données collectées dans le cadre de l’utilisation du logiciel de la preneuse d’ordre et qui sont détenues par le donneur d’ordre.

(2) Une rémunération éventuelle sera ensuite réglée dans le contrat principal sous-jacent.

(3) Pour l’essentiel, la commande du donneur d’ordre comprend la phase du traitement des données « stockage » des données traitées par différents procédés.

(4) En tant que données à caractère personnel, seront traitées les données des clients et des collaborateurs (par exemple, nom, nom de la société, numéro de client, adresse), ainsi que, le cas échéant, les coordonnées (par exemple, l’adresse e-mail, numéro de téléphone) et les données relatives au règlement du contrat et les données de paiement.

(5) La catégorie des personnes concernée par le traitement comprend les clients et les collaborateurs du donneur d’ordre.

2. Mise à la disposition des données par le donneur d’ordre

Le donneur d’ordre met à disposition les données via l’application client orderbird.POS et le module de gestion et de comptabilité « my.orderbird ». Il s’assure que les données d’accès à la base des données sont conservées en sécurité et ne seront pas transmises à des tiers. L’accès n’est alors possible qu’aux données faisant l’objet du contrat. Après la fin du contrat, la preneuse d’ordre détruira les données d’accès.

3. Droits et obligations du donneur d’ordre

(1) Dans le cadre du présent contrat, le donneur d’ordre répond seul de l’évaluation de l’admissibilité du traitement des données ainsi que de la protection des droits des personnes concernées.

(2) Pour ce faire, il convient avec la preneuse d’ordre les mesures techniques et organisationnelles figurant à l’annexe. Il veille à ce qu’elles présentent un niveau de protection approprié contre les risques couru par les données à traiter, notamment que la confidentialité, l’intégrité, la disponibilité et la capacité de charge des systèmes et services en rapport avec le traitement à long terme sont assurées.

(3) Le donneur d’ordre a le droit de donner des instructions concernant la nature, l’étendue et le procédé du traitement des données, sous forme écrite ou électronique. Les instructions seront fixées contractuellement au début de la collaboration. Dans le cadre du mandat, le donneur d’ordre peut donner des instructions individuelles

visant à protéger les données à caractère personnel et contrôler le respect des dispositions en matière de la protection des données et des instructions qu'il a données. Les instructions verbales doivent être immédiatement confirmées par écrit ou sous forme de texte.

(4) Le donneur d'ordre nomme à la preneuse d'ordre une personne habilitée à donner des instructions.

(5) Le donneur d'ordre informe immédiatement la preneuse d'ordre dès qu'il constate des erreurs ou des irrégularités pendant la vérification des résultats de la commande.

(6) Le donneur d'ordre est tenu de traiter confidentiellement tous les secrets commerciaux et les mesures de sécurité des données de la preneuse d'ordre appris dans le cadre de la relation contractuelle.

4. Obligations de la preneuse d'ordre

(1) La preneuse d'ordre traite les données à caractère personnel exclusivement dans le cadre du présent accord et conformément aux instructions du donneur d'ordre, sauf disposition légale contraire.

(2) La preneuse d'ordre informe immédiatement le donneur d'ordre lorsqu'elle considère qu'une instruction porte atteinte aux dispositions légales. La preneuse d'ordre peut suspendre la mise en œuvre de l'instruction jusqu'à sa confirmation ou modification par le donneur d'ordre.

(3) La preneuse d'ordre n'utilise pas les données transférées aux fins du traitement des données à d'autres fins que celles précitées. Il est interdit de produire des copies ou duplicata sans en avertir le donneur d'ordre.

(4) La preneuse d'ordre aménage son organisation de manière à satisfaire les dispositions légales dans le domaine de la protection des données.

(5) Dans son domaine de responsabilité, la preneuse d'ordre veillera à la mise en œuvre et au respect des mesures générales, techniques et organisationnelles jointes en **annexe** du présent contrat pour garantir une protection appropriée des données du donneur d'ordre tout en respectant les dispositions légales. En fait également partie l'utilisation d'un procédé de vérification, estimation et évaluation régulières de l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement conformément aux dispositions légales.

(6) La preneuse d'ordre se réserve le droit à modifier unilatéralement les mesures de sécurités prises afin de garantir que le niveau de protection prévu par le contrat soit maintenu.

(7) Sur demande, la preneuse d'ordre assiste le donneur d'ordre dans l'exécution des obligations en matière de protection des données si les dispositions légales prescrivent une telle assistance de la part de la preneuse d'ordre.

(8) La preneuse d'ordre veille à ce qu'il soit interdit aux collaborateurs et à d'autres personnes employées par la preneuse d'ordre chargés du traitement des données du donneur d'ordre de traiter les données d'une façon contraire aux instructions. En outre, les collaborateurs et les tiers employés par la preneuse d'ordre seront tenus à la confidentialité s'ils ne sont pas soumis à un devoir de confidentialité légal comparable. Ces règles doivent également s'appliquer après la fin du contrat.

(9) La preneuse d'ordre renseigne immédiatement le donneur d'ordre des insuffisances techniques et organisationnelles de la sauvegarde des données en cas de tout soupçon d'atteinte à la protection des données ou d'autres irrégularités lors du traitement des données à caractère personnel. Elle prend des mesures nécessaires pour sécuriser les données et pour réduire les conséquences défavorables possibles des personnes concernées et se concerte immédiatement avec le donneur d'ordre à cet effet.

(10) La preneuse d'ordre doit rectifier, supprimer et bloquer les données à caractère personnel si le donneur d'ordre le demande dans une instruction. Si un effacement conforme aux règles de la protection des données ou une restriction correspondante du traitement des données ne sont pas possibles, la preneuse d'ordre se charge de la destruction des supports de données et d'autres matériaux concernés conforme aux règles de la protection des données sur la base d'un mandat individuel de la part du donneur d'ordre ou rend ces supports de données au donneur d'ordre. Dans des cas particuliers à déterminer par le donneur d'ordre, une conservation a lieu ; la rémunération et les mesures de sécurité doivent alors être convenues séparément.

(11) Après la conclusion de la commande, la preneuse d'ordre doit remettre au donneur d'ordre tous les résultats de traitement et d'utilisation se trouvant en sa possession se trouvant en rapport avec la relation de mandat. Les supports de données de la preneuse d'ordre doivent ensuite être effacés physiquement. Le matériel d'essai et de rebut doit être immédiatement détruit ou rendu au donneur d'ordre. L'effacement ou la destruction doivent être confirmés par écrit au donneur d'ordre. Les obligations de conservation légales ne sont pas affectées par le présent accord.

5. Moyens de preuve

(1) Le donneur d'ordre a le droit d'effectuer, après consultation avec la preneuse d'ordre des contrôles par lui-même ou par un contrôleur mandaté par lui et se convaincre, grâce aux contrôles d'échantillonnage devant être notifiés à temps, du respect du présent accord par la preneuse d'ordre dans ses activités commerciales.

(2) La preneuse d'ordre prouve au donneur d'ordre le respect des obligations fixées dans le présent contrat en réalisant des audits internes. Elle les gardent pour le donneur d'ordre et les transmet, sur demande, à un interlocuteur désigné par le donneur d'ordre.

6. Sous-traitants

(1) Le recours à des sous-traitants pour l'exécution de ses obligations contractuelles par la preneuse d'ordre est autorisé et exige l'information préalable du donneur d'ordre.

(2) La preneuse d'ordre conclura des accords avec ces tiers dans la mesure nécessaire pour assurer les mesures appropriées de protection des données et de sécurité des informations.

(3) Si le sous-traitant fournit ses prestations en dehors de l'UE / de l'EEE, la preneuse d'ordre garantit leur recevabilité du point de vue de la protection des données au moyen des mesures correspondantes.

7. Obligations d'information

Si la protection des données à caractère personnel est menacée par les mesures des tiers, comme par exemple, la procédure d'insolvabilité, ou par d'autres évènements, la preneuse d'ordre doit le signaler immédiatement au donneur d'ordre. La propriété du donneur d'ordre (par exemple, les supports de données, copies de travail, contenants) doit être marquée à temps.

8. Durée du contrat

Le présent accord commence à la conclusion du contrat et se termine à la fin du contrat principal conclu entre les parties.

9. Responsabilité et dommages-intérêts

Le régime de responsabilité convenu entre les parties dans le contrat principal s'applique également au présent accord sur le traitement des commandes, sauf convention expresse contraire.

10. Résiliation

En cas d'atteintes graves ou répétées au présent accord, les parties disposent d'un droit réciproque de résiliation extraordinaire.

11. Clause de la forme écrite, loi applicable

(1) Les modifications et compléments du présent accord et de tous ses éléments exigent un accord écrit pouvant également être conclu sous forme électronique.

(2) En cas de contradictions éventuelles, les règles de la présente annexe sur la protection des données prévalent sur les règles du contrat principal.

(3) Si certaines parties de la présente annexe deviennent inefficaces, la validité du reste de l'annexe n'en sera pas affectée.

_____, le _____	Berlin 22.11.18 _____, le _____
(Lieu et date)	(Lieu et date)
_____	_____
pour le donneur d'ordre	pour orderbird AG

www.orderbird.com
hello@orderbird.com

Mesures techniques et organisationnelles

Les organisations qui traitent, utilisent ou collectent les données à caractère personnel par eux-mêmes ou par des mandataires doivent prendre des mesures techniques et organisationnelles permettant un processus de traitement conforme aux règles de la protection des données. Les mesures ne sont nécessaires que si le caractère raisonnable est préservé en prenant en compte les intérêts de protection.

La société orderbird AG satisfait à cette exigence grâce aux mesures suivantes, étant donné que nous distinguons entre nos propres mesures et les mesures prises dans les centres de données auxquels nous recourons et qui sont exploités par les sous-traitants.

État : le jeudi 2 août 2018

I. Mesures propres

Nous prenons les mesures suivantes dans la mesure où nous ne sous-traitons pas l'activité de traitement.

1. Confidentialité, intégrité, disponibilité (article 32, paragraphe 2, point b RGPD)

a) Contrôle d'entrée

N°	Mesures techniques	Mesures organisationnelles
1.	Système de carte à puce / de transpondeur	Gestion des clés définie par écrit et claire avec la responsabilité précise des collaborateurs nommément désignés
2.	Conservation des clés sûre / coffre à clés	Vérification régulière des droits d'entrée accordés
3.	Serrures de sécurité	Réception / les visiteurs sont accompagnés par des collaborateurs
4.		Sélection et surveillance des services de gardiennage et de nettoyage du point de vue de la protection des données

b) Contrôle d'accès

N°	Mesures techniques	Mesures organisationnelles
1.	Cryptage des ordinateurs portables	Règles concernant les mots de passe, avec des exigences élevées en matière de longueur, complexité et changement
2.	Authentification avec les données d'accès personnalisées	
3.	Verrouillage de l'écran du PC automatique et protégé par le mot de passe	
4.	Verrouillage automatique en cas de tentatives de connexion échouées	

5.	Utilisation des Firewalls pour protéger les systèmes informatiques	
6.	Utilisation du VPN en cas d'accès à distance aux systèmes informatiques	
7.	Système d'effacement des données pour effacer au moyen du programme de disque dur (Mac OS) ou DBAN (serveur)	
8.	Enregistrement des accès aux applications et systèmes informatiques	
9.	Garantie du cryptage du disque dur	
10.	Exigence d'un identifiant de l'écran de veille	
11.	Possibilité de suppression à distance par le Mobile Device Management (MDM)	
12.	Attribution des mots de passe de micrologiciel (mots de passe EFI)	

c) Contrôle d'accès

N°	Mesures techniques	Mesures organisationnelles
1.	Enregistrement des accès aux applications et systèmes informatiques	Groupage des autorisations d'accès en fonction du domaine de responsabilités et de compétences
2.	Enregistrement des tentatives d'accès échouées aux systèmes informatiques	Concept d'autorisations pour les accès aux systèmes informatiques
3.	Destruction des données réglementée et techniquement fiable grâce à l'utilisation d'une « poubelle à données »	Règles concernant les mots de passe et attribution des mots de passe protégée
4.		Gestion des droits des utilisateurs par des administrateurs du système formés

5.		Attribution des droits par un personnel formé
6.		Vérification régulière des droits d'accès aux systèmes informatiques
7.		Concept des autorisations avec le principe minimaliste

d) Contrôle de séparation

N°	Mesures techniques	Mesures organisationnelles
1.	Affectation durable des appareils de traitement à des utilisateurs individuels	Différents postes de travail pour différentes opérations de traitement et catégories de données
2.	Systèmes multi-tenant pour la séparation des fonctions	Commande via le concept des autorisations
3.	Segmentation des réseaux en fonction de la vulnérabilité	Les données de contrat du client sont enregistrées dans un SGC séparé avec un système d'accès conditionnel propre
4.	Séparation des environnements de développement et de test et des systèmes productifs	Des données de test sont générées dans le développement pour ne pas devoir recourir aux données en direct
5.		Détermination des droits sur les bases de données

e) Contrôle de transmission

N°	Mesures techniques	Mesures organisationnelles
1.	Cryptage des e-mails en cas de données sensibles (p. ex., lors de la communication avec le bureau des salaires)	Documentation des destinataires des données ainsi que la durée de la remise et des délais d'effacement prévus
2.	Utilisation de VPN	Dans les cas appropriés, transfert sous forme pseudonomysée ou anonymisée

3.	Mise à disposition des informations sur les connexions cryptées, comme https, sftp	
4.	Utilisation du procédé de signature	

2. Contrôle de disponibilité et de capacité de charge (article 32, point c RGPD)

N°	Mesures techniques	Mesures organisationnelles
1.	Utilisation des systèmes redondants	Conservation des sauvegardes de données dans un endroit externalisé sûr
2.	Présence d'extincteurs dans les bureaux et les locaux d'infrastructure	Supervision de toutes les infrastructures et systèmes informatiques pertinents
3.	Utilisation de miroitage (RAID) pour les systèmes informatiques concernés	Concept de sauvegarde et de restauration (formulé)
4.		Contrôle de l'opération de sauvegarde
5.		Tests réguliers de restauration de données et de documentation des résultats

3. Incident Response Management

N°	Mesures techniques	Mesures organisationnelles
1.	Utilisation de Firewall et sa mise à jour régulière	Processus documenté de détection et de notification des incidents de sécurité / pannes de données (aussi en ce qui concerne l'obligation de notification à l'autorité de surveillance) « Directive sur la gestion des crises »
2.	Utilisation de VPN	Procédure documentée pour traiter les incidents de sécurité
3.	Mise à disposition des informations sur les connexions cryptées, comme https, sftp	Implication du délégué à la protection des données dans les incidents de sécurité et les pannes de données, processus d'amélioration constante

4.	Utilisation du procédé de signature	Processus formel pour le traitement ultérieur des incidents de sécurité
5.		Documentation des incidents de sécurité dans un système de tickets

4. Contrôle des commandes (externalisation à des tiers)

N°	Mesures techniques	Mesures organisationnelles
1.	Cryptage des e-mails en cas de données sensibles	Examen des mesures de sécurité prises par le preneur d'ordre et leur documentation
2.	Utilisation de VPN	Processus formel pour l'examen et la conclusion des accords sur le traitement des commandes ou des clauses contractuelles standard de l'UE
3.	Mise à disposition des informations sur les connexions cryptées, comme https, sftp	Instructions écrites pour le preneur d'ordre
4.	Utilisation du procédé de signature	L'obligation des collaborateurs du preneur d'ordre à la confidentialité des données est garantie
5.		Garantie contractuelle de la destruction des données à la fin de la commande
6.		Processus de contrôle continu des sous-traitants

5. Gestion de la protection des données (article 32, point d RGPD)

N°	Mesures techniques	Mesures organisationnelles
1.	Documentation des procédures consultable électroniquement	Sensibilisation régulière des collaborateurs en matière de protection des données
2.	Documentation technique de la saisie, de la modification et de l'effacement des données	Processus établi de destruction / effacement des données

3.	Contrôle manuel et automatique des fichiers journaux créés à cette fin du côté du logiciel	Vérification régulière de l'actualité et de l'efficacité des directives
4.	Documentation centrale des procédures et instructions de travail relatives à la protection des données ; possibilité d'accès pour les collaborateurs concernés selon la pertinence	Processus de démantèlement en cas de résiliations de produit
5.	Garantie du principe d'économie des données au niveau technique : seules les données nécessaires seront demandées aux collaborateurs lors du processus de demande	Directives d'intégration et de départ pour les nouveaux collaborateurs et les collaborateurs quittant l'entreprise
6.		Surveillance centralisée du respect du niveau de protection des données adéquat par les sous-traitants
7.		Conseil extérieur par un cabinet d'avocats spécialisé
8.		Directives contraignantes en matière de droit de travail « travail mobile » avec des dispositifs particuliers contre la perte des données et l'accès non autorisé des tiers
9.		Directive d'utilisation de l'équipement de travail / des supports de données
10.		Délégué à la protection des données externe
11.		Conservation de formulaires, à partir desquels des données ont été reprises dans les traitements automatisés
12.		Collaborateurs formés et tenus à la confidentialité / secret des données

II. Mesures de nos sous-traitants

Dans le cadre de l'exécution de notre activité principale, nous recourrons aux services des meilleurs fournisseurs de cloud. À cet effet, il s'agit, au moment de la conclusion du présent contrat, des entreprises suivantes, en sachant que les entreprises des États-Unis sont autocertifiées selon l'accord sur le Bouclier de protection des données :

Amazon Web Services, Inc. 410 Terry Ave North Seattle, WA 98109-5210	CloudHare, Inc. 101 Townsend St. San Francisco, CA 94107

Les mesures techniques et organisationnelles suivantes concernent nos sous-traitants impliqués dans le cadre du traitement de la commande. Où les mesures ne sont pas uniformes, cela sera marqué par un sigle pour désigner le sous-traitant concerné (A = Amazon Web Services Inc., C = CloudHare Inc.) :

1. Confidentialité, intégrité, disponibilité (article 32, paragraphe 2, point b RGPD)

a) Contrôle d'entrée

N°	Mesures techniques	Mesures organisationnelles
1.	Système de contrôle d'entrée	Contrôle personnel à l'entrée sur le territoire de l'entreprise et dans les centres de données[A]
2.	Authentification à deux niveaux avec les données d'accès personnalisées[A]	Système d'attribution des cartes d'entrée aux collaborateurs et personnes spécialement autorisées
3.	Système de fermeture avec des serrures de sécurité	Authentification au moins double requise avant l'autorisation d'entrée aux centres de données[A]
4.	Vidéosurveillance des entrées et des sorties[A], alarme anti-intrusion	Attribution des droits d'entrées aux collaborateurs et aux collaborateurs externes selon des critères fixes.
5.		Attribution et documentation des autorisations par la gestion des droits d'entrée
6.		Identification des visiteurs et des collaborateurs externes[A]

7.		Accompagnement des visiteurs et des collaborateurs externes uniquement par des collaborateurs autorisés[A]
8.		Documentation et audit des entrées effectuées[A]

b) Contrôle d'accès

N°	Mesures techniques	Mesures organisationnelles
1.	Utilisation des Firewalls pour protéger les systèmes informatiques	Concept d'autorisation pour les accès aux systèmes de traitement des données, attribution des autorisations selon des critères fixes
2.	Utilisation du VPN en cas d'accès à distance aux systèmes informatiques	Règles concernant les mots de passe et attribution des mots de passe protégée
3.	Documentation des accès au serveur, aux réseaux et aux ports	Verrouillage temporaire automatique du terminal de l'utilisateur en cas de non-utilisation, identification et saisie du mot de passe nécessaires pour une réouverture[C]
4.	Utilisation des procédés de cryptage	Verrouillage temporaire automatique de l'autorisation de l'utilisation en cas de saisie réitérée des mots de passe erronés, documentation de la saisie des mots de passe[C]
5.	Accès à distance aux systèmes informatiques internes uniquement après authentification, utilisation de VPN[A]	
6.		Information des collaborateurs responsables en cas d'accès suspects[A] Utilisation de pagers pour donner l'alerte[A] disponibilité permanente des collaborateurs responsables[A] discussions hebdomadaires sur la mise en place des mesures préventives[A]

7.		Élimination des supports de données usagés selon des règles fixes[A]

c) Contrôle d'accès

N°	Mesures techniques	Mesures organisationnelles
1.	Enregistrement des accès aux applications et systèmes informatiques	Concept des autorisations d'accès en fonction du domaine de responsabilités et de compétences
2.	Documentation des tentatives d'accès suspectes aux systèmes de traitement de l'information, communication aux collaborateurs responsables[A]	Maintien d'une équipe de gestion des incidents[A]
3.	En option : accès uniquement après une authentification multifactorielle[A]	Directives destinées aux collaborateurs et formations individuelles en rapport avec les droits d'accès[C]
4.	SSL-Load Balancer conforme FIPS 140-2[A]	Possibilité de documentation des personnes qui effacent, ajoutent ou modifient les données à caractère personnel[C]
5.	Mise en place des dispositifs de réseau pour gérer la communication de l'interface avec les Internet Service Providers (ISP)[A]	
6.	Connexion redondante aux plusieurs services de communication du réseau[A]	
7.	Utilisation des technologies de cryptage (Security Socket Layers – SSL[A])	

d) Contrôle de séparation

N°	Mesures techniques	Mesures organisationnelles

1.	Séparation entre le réseau opérationnelle et le réseau d'entreprise[A], stockage séparé de données au niveau de base de données en fonction du module, du client ou de la fonction prise en charge[C]	Attribution d'accès aux différents réseaux via le système de tickets[A] et le concept des autorisations
2.	Accès au réseau opérationnel uniquement avec une authentification SSH-Public-Key[A]	Fin d'autorisation automatique après 90 jours ou au départ du collaborateur de l'entreprise[A]
3.	Limitation des interfaces, processus discontinus et rapports pour des objectifs et fonctions déterminés[C]	

e) Contrôle de transmission

N°	Mesures techniques	Mesures organisationnelles
1.	Protection contre l'accès aux systèmes au niveau du site et de l'entreprise[A]	Transmission des données uniquement à des personnes autorisées, Y compris l'attribution des droits d'accès et des rôles différenciés[C]
2.	Utilisation de Firewall, technologies de VPN et de cryptage pour protéger les passerelles et les lignes par lesquelles les données nous sont transmises	Effacement des données contrôlée et documenté[C]
3.	Cryptage de certaines données des collaborateurs (p. ex., informations personnellement identifiables, comme les numéros d'identification nationale, numéros de carte de crédit ou de débit) au sein du réseau[C]	Notification de l'utilisateur en cas de transfert de données incomplet (end-to-end-check)[C]
4.		Documentation du transfert de données (dans la mesure du possible)[C]

2. Contrôle de disponibilité et de capacité de charge (article 32, point c RGPD)

N°	Mesures techniques	Mesures organisationnelles

1.	Alimentation en courant redondante sans coupures des centres de données sans incidence sur les processus en cours[A], Système d'alimentation sans interruption (UPS) en cas d'une panne de courant pour les charges critiques et essentielles dans l'installation[A], Les génératrices des centres de données peuvent alimenter en courant l'installation entière[A]	Surveillance et maintenance régulière des systèmes et appareils électriques, mécaniques et de maintien des fonctions vitales pour détecter immédiatement les erreurs[A]
2.	Infrastructure de réseau redondante[C]	Sauvegarde séparée[C]
3.	Alarme incendie automatique avec détecteurs de fumée et équipements anti-incendie dans les	Surveillance personnelle de la température et de l'humidité dans le centre de données[A]

	environnements du centre de données, les locaux d'infrastructure mécanique et électrique, les locaux de refroidissement et les locaux d'équipement des génératrices[A], Protection grâce aux installations sous eau, de double verrouillage ou de gicleurs de gaz[A]	
4.	Climatisation des centres de données[A]	Répartition en faisceau des centres de données dans le monde entier[A] Exclusion des centres de données « froids », tous sont actifs[A]
5.	Système de surveillance de la température et de l'humidité dans les centres de données[A]	Système automatisé de déplacement du trafic des données des clients du domaine concerné en cas de perturbations[A]
6.	Configuration N+1 garantissant qu'en cas d'une panne d'un des centres de données, il reste suffisamment de capacité pour déplacer le trafic des données sur les sites restants[A]	Maintien de plusieurs zones géographiques de disponibilité pour la sauvegarde des données, l'alimentation des zones par divers réseaux des entreprises d'approvisionnement indépendantes[A]

7.	Connexion redondante des zones de disponibilité aux plusieurs opérateurs de transit Tier 1[A]	Séparation spatiale des zones de disponibilité dans les régions métropoles typiques et aménagement de zones de disponibilité dans les zones inondables à faible risque[A]
8.	Maintien de systèmes de production des sauvegardes dans les centres de données[A]	Possibilité de stockage de données dans différentes zones de disponibilité[A]
9.		Contrôles internes réguliers de la disponibilité et de la résistance des systèmes[A]
10.		Réalisation des audits de sécurité et des tests d'intrusion[A]
11.		Les modifications de routine, d'urgence et de configuration de l'infrastructure existante sont autorisées, enregistrées, testées, approuvées et documentées conformément aux normes industrielles[A]
12.		Indications concernant l'information des clients en cas d'une modification nécessaire[A]

3. Incident Response Management

N°	Mesures techniques	Mesures organisationnelles
1.	Utilisation de Firewall et sa mise à jour régulière[A]	Équipe de gestion des incidents[A]
2.	Utilisation de VPN[A]	Utilisation des procédés de diagnostic typiques de la branche[A]
3.	Mise à disposition des informations sur les connexions cryptées[A]	Disponibilité permanente des équipes de gestion des incidents[A]
4.	Utilisation du procédé de signature (en option)[A]	Processus formel pour le traitement ultérieur des incidents de sécurité[A]

5.		Documentation des incidents de sécurité dans un système de tickets[A]
6.		Directive sur la gestion des incidents[A]

4. Contrôle des saisies

N°	Mesures techniques	Mesures organisationnelles
1.		Directive sur les autorisations pour saisir, lire, modifier et effacer les données[C]
2.		Gestion des droits de saisie[C]
3.		Directive sur les mots de passe[C]
4.		Exigence d'authentification des personnes autorisées[C]
5.		Mesures de sécurité pour la saisie des données dans le mémoire ainsi que la lecture, la modification et l'effacement des données enregistrées[C]
6.		Documentation des inscriptions effectuées[C]

5. Gestion de la protection des données (article 32, point d RGPD)

N°	Mesures techniques	Mesures organisationnelles
1.	Documentation des procédures consultable électroniquement[A]	
2.	Documentation technique de la saisie, de la modification et de l'effacement des données[A]	
3.	Contrôle manuel et automatique des fichiers journaux créés à cette fin du côté du logiciel[A]	