CONDITIONS GÉNÉRALES DE PROTECTION DES DONNÉES, TERRA CLOUD GMBH

1.
Préambule
Dans le § 11 alinéa 5 BDSG (Bundesdatenschutzgesetz, loi fédérale allemande sur la protection des données), le législateur a disposé que les mesures de sécurisation des opérations de traitement des données et notamment des données issues d'une commande devaient être maintenues, même pendant la maintenance, le nettoyage et l'entretien des installations informatiques. En cas de non-respect, le Donneur d'ordre peut attendre des sanctions allant de sanctions financières sévères jusqu'à l'interdiction du traitement des données. TERRA CLOUD GmbH (ci-après dénommé le Preneur d'ordre) aide le Donneur d'ordre à respecter ces exigences légales en donnant au Donneur d'ordre la possibilité d'appliquer les dispositions légales du § 11 BDSG via les présentes conditions générales de protection des données.

2. Relations contractuelles
Les réglementations suivantes s'appliquent entre le Preneur d'ordre et le Donneur d'ordre, en complément de tous les accords déjà conclus entre le Donneur d'ordre et le Preneur d'ordre, dans le cadre desquels le Preneur d'ordre ou le tiers mandaté par ses soins entre en contact avec des données personnelles au sens de la loi fédérale allemande sur la protection des données (Bundesdatenschutzgesetz). Les contrats concernés sont notamment les accords de maintenance à distance.

3. Définitions

3.1 Données personnelles
Les données personnelles sont des informations particulières concernant la situation personnelle ou matérielle d'une personne naturelle définie ou définissable.

3.2 Collecte
La collecte correspond à la récupération des données de la personne concernée.

3.3 Traitement
Le traitement correspond à la sauvegarde, la modification, la transmission, le blocage et la suppression de données personnelles.

3.4 Sauvegarde
La sauvegarde est l'enregistrement, la réception et la conservation de données personnelles sur un support de données dans le but de les traiter ou de les utiliser.

3.5 Suppression
La suppression consiste à la dissimulation des données personnelles sauvegardées.

3.6 Blocage
Le blocage est un marquage apposé sur les données personnelles pour limiter leur traitement ou leur utilisation.

3.7 Traitement des données sur commande Le traitement des données sur commande correspond à la collecte, au traitement, à l'utilisation ou à la suppression de données personnelles par le Preneur d'ordre, sur commande du Donneur d'ordre.

4. Objet, durée, portée, type, objectif, etc. de la commande

4.1 Objet
Conformément au paragraphe 2, l'objet du contrat est de permettre la maintenance à distance des systèmes informatiques utilisés par ou pour le Donneur d'ordre.

4.2 Durée
La durée de chaque contrat dépend des différents accords.

4.3 Portée, type et objectif de la collecte
Dans le cadre de l'exécution des contrats concernés, il n'est pas exclu que le Preneur d'ordre reçoive des données personnelles de manière totalement fortuite. Par ailleurs, le Preneur d'ordre ne collecte ou ne traite aucune donnée personnelle.

4.4 Types de données et personnes concernées
Les données produites par le Donneur d'ordre peuvent correspondre à des données personnelles "simples", mais également des données personnelles sensibles au sens du § 3 alinéa 9 BDSG. Les personnes concernées peuvent être notamment des clients et prospects du Donneur d'ordre.

4.5 Correction, blocage et suppression des données
Le Preneur d'ordre n'effectuera aucune correction, suppression ni aucun blocage des données sans instructions du Donneur d'ordre. Les parties établissent qu'une telle utilisation n'entre pas dans l'objet des contrats au sens du paragraphe 2.

5. Instructions du Donneur d'ordre
Une instruction est une demande officielle du Donneur d'ordre pour que le Preneur d'ordre traite les données personnelles d'une manière particulière. Le Donneur d'ordre est en droit de donner des instructions complètes. Les instructions orales doivent être confirmées par écrit par le Donneur d'ordre.

6. Confidentialité des données
Le Preneur d'ordre effectue des prestations pour le Donneur d'ordre, uniquement dans le cadre des accords conclus dans le présent contrat et selon les instructions du Donneur d'ordre. Il utilise les données transmises uniquement pour le traitement des données convenu, et à aucune autre fin. Aucune copie, ni aucun duplicata ne seront créés sans que le Donneur d'ordre ne le sache. Lors du traitement des données personnelles du Donneur d'ordre dans le cadre du contrat, le Preneur d'ordre s'engage à garantir la protection des données conformément à la loi fédérale allemande sur la protection des données (Bundesdatenschutzgesetz, BDSG) et conformément aux §§ 91 et suivants de la loi sur les télécommunications (Telekommunikationsgesetz, TKG) et aux lois spéciales comme la loi SGB V par exemple. Il s'engage à respecter les mêmes règles de protection de la confidentialité que celles du Donneur d'ordre. Si le Donneur d'ordre est soumis à des lois spéciales sur la protection des données dépassant la loi fédérale allemande sur la protection des données (Bundesdatenschutzgesetz), la loi sur les télémédias (Telemediengesetz) et la loi sur les télécommunications (Telekommunikationsgesetz), le Donneur d'ordre s'engage à informer expressément le Preneur d'ordre de l'application de ces lois. Le Preneur d'ordre établira et respectera alors immédiatement les obligations qui lui incombent dans le cadre de ces lois. Il engagera uniquement des collaborateurs dont il aura préalablement vérifié la fiabilité et le sérieux. Le Preneur d'ordre atteste qu'il emploie pour effectuer les travaux uniquement des collaborateurs formés aux dispositions de protection des données déterminantes et qu'il surveille le respect des dispositions en matière de protection des données. Le Preneur d'ordre atteste que les collaborateurs qu'il engage pour le traitement des données du Donneur d'ordre s'engagent toujours par écrit à respecter le § 5
BDSG sur la confidentialité des données. Par ailleurs, le Donneur d'ordre est en droit, à son entière discrétion, de conclure des accords de confidentialité séparés avec les collaborateurs concernés. Le traitement des données pour le Donneur d'ordre est uniquement autorisé dans les locaux du Donneur d'ordre prévus à cet effet. Tout traitement des données dans un espace privé est notamment expressément interdit. Le Preneur d'ordre ne pourra communiquer les informations sur les différentes données liées à l'exécution du contrat entre le Preneur d'ordre et le Donneur d'ordre à des tiers que sur accord écrit préalable. Les droits et devoirs d'information expressément régis par le contrat ou prévus par la loi restent inchangés. Le Donneur d'ordre est le seul à communiquer des informations, en toute responsabilité et selon le droit sur la protection des données. Sur demande du Donneur d'ordre, le Preneur d'ordre doit participer à la production du répertoire de procédures ou à la rédaction des descriptions du traitement de données effectué. Il doit transmettre les données nécessaires au Donneur d'ordre dès que possible. Le Preneur d'ordre s'engage à appliquer et à respecter les mesures techniques et organisationnelles conclues dans le présent contrat ou générales tombant sous sa responsabilité conformément au § 9 BDSG. En outre, il organisera son exploitation de manière à ce qu'elle soit conforme aux exigences particulières de la protection des données. Il prendra des mesures techniques et organisationnelles afin de protéger raisonnablement les données du Donneur d'ordre de toute perte ou utilisation abusive. Le Preneur d'ordre consigne par écrit et de manière compréhensible les mesures prises pour respecter ses obligations issues du paragraphe précédent.

7. Secret commercial Le Preneur d'ordre s'engage à garder confidentielles toutes les informations commerciales pertinentes, importantes et non connues de tous du Donneur d'ordre (secret commercial). Il oblige également ses collaborateurs à respecter ce secret. Indépendamment de ce qui précède, le Donneur d'ordre reste en droit de conclure directement des accords de confidentialité avec les collaborateurs du Preneur d'ordre.

8. Sécurité des données Le Preneur d'ordre garantit l'application et le respect continus des mesures organisationnelles et techniques obligatoires suivantes :

- toutes mesures permettant d'éviter que des personnes non autorisées n'aient accès aux installations de traitement des données avec lesquelles les données personnelles sont traitées (contrôle d'entrée) ;

L'accès des personnes sera strictement contrôlé par du personnel de contrôle, des services de sécurité ou via des systèmes d'alarme électroniques, optiques et mécaniques. L'accès aux bâtiments du centre de données doit se faire dans le respect des politiques de sécurité de TERRA CLOUD GmbH et d'une procédure spéciale avec inscription préalable. L'accès n'est possible qu'aux personnes autorisées et sous surveillance permanente d'un collaborateur de TERRA CLOUD GmbH, et il est en général payant. TERRA CLOUD GmbH se réserve le droit d'archiver et d'utiliser les données vidéo des accès et, si nécessaire, de refuser l'accès.

Aucun accès à la salle de serveurs elle-même n'est prévu. Des locaux adaptés et séparés sont mis à disposition si des travaux individuels sont nécessaires.

- Toutes mesures permettant d'éviter que des personnes non autorisées puissent utiliser les installations et procédures de traitement des données (contrôle d'accès) ;
- Toutes mesures permettant de limiter l'accès des personnes autorisées à utiliser les procédures de traitement des données aux données personnelles relevant de leurs compétences (contrôle d'accès aux données) ;
- Toutes mesures permettant d'éviter que les données personnelles ne soient lues, copiées, modifiées ou éliminées par des personnes non autorisées

pendant le transfert électronique, le transport ou la sauvegarde des données sur un support de données, et d'établir à quelles autorités les données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission) ;

- Toutes mesures permettant de vérifier et d'établir a posteriori si et par qui les données personnelles ont été introduites, modifiées ou éliminées des systèmes de traitement des données (contrôle de l'introduction) ;
- Toutes mesures permettant de s'assurer que les données personnelles traitées sur commande soient uniquement traitées conformément aux instructions du Donneur d'ordre (contrôle de commande) ;
- Toutes mesures permettant de protéger les données personnelles contre toute suppression ou perte accidentelle (contrôle de disponibilité) ;

- Toutes mesures permettant de s'assurer que les données collectées ou destinées au traitement à des fins différentes – notamment pour différents clients du Preneur d'ordre – soient traitées séparément (contrôle de séparation) ;

L'une de ces mesures consiste notamment à utiliser des procédures de verrouillage correspondant au niveau actuel de la technique.
Une liste de toutes les mesures prises est consultable sur https://downloads.terracloud.de, à condition que la sécurité d'exploitation du centre de données de TERRA CLOUD GmbH le permette.

9. Interlocuteur
Les Parties conviennent qu'il est nécessaire d'établir des règles de communication afin de garantir une exécution du contrat sûre, sans perturbations et conforme au droit sur la protection des données. Le Preneur d'ordre informe immédiatement le Donneur d'ordre en cas de perturbation grave du fonctionnement de l'exploitation ou des logiciels, en cas de soupçon de violation de la protection des données ou d'autre irrégularité lors du traitement des données. Avant toute manipulation importante sur le système, le Preneur d'ordre doit informer immédiatement le Donneur d'ordre des modifications prévues et peut les effectuer ou les démarrer sur autorisation correspondante du Donneur d'ordre uniquement. Les Parties nomment des interlocuteurs mutuels et informeront l'autre partenaire au contrat de toute modification immédiatement et par écrit. En l'absence de règle spéciale, les coordonnées des collaborateurs désignés comme interlocuteurs ou personnes chargées du dossier doivent toujours être indiquées dans les données de base. Le Preneur d'ordre s'engage à garantir par des mesures organisationnelles et techniques que seuls les collaborateurs nommés puissent demander l'accès aux systèmes attribués au Donneur d'ordre.

10. Droits et obligations de contrôle et d'accès Le Preneur d'ordre travaille exclusivement dans le cadre de la loi sur la protection des données, des accords correspondants et des instructions du Donneur d'ordre. Il devra corriger, effacer et bloquer les données personnelles dès lors que le Donneur d'ordre en aura fait la demande dans le cadre de l'accord convenu ou d'une instruction. Le preneur d'ordre n'utilise les données transmises pour traitement à aucune autre fin. Aucune copie ni aucun duplicata ne seront créés sans que le Donneur d'ordre ne le sache. Si une instruction émise par le Donneur d'ordre semble selon le Preneur d'ordre aller à l'encontre de dispositions légales, ce dernier en informera immédiatement le Donneur d'ordre. Le Preneur d'ordre a le droit de repousser l'exécution de ladite instruction jusqu'à confirmation ou modification de la part des responsables du côté du Donneur d'ordre. Le Preneur d'ordre met les données nécessaires au suivi conformément au § 4g alinéa 2 p. 1 BDSG à disposition du Donneur d'ordre, sur demande. Le Preneur d'ordre informe immédiatement le Donneur d'ordre en cas de perturbation grave du fonctionnement de l'exploitation ou des logiciels, en cas de soupçon de violation de la protection des données ou d'autre irrégularité lors du traitement des données. Le Preneur d'ordre sait et accepte que le Donneur d'ordre puisse à tout moment contrôler le respect des dispositions légales relatives à la protection des données et des accords contractuels dans la mesure nécessaire, notamment en demandant des informations et en consultant les données enregistrées et les programmes de traitement des données. Après la conclusion des travaux inclus dans le contrat, le Preneur d'ordre doit remettre au Preneur d'ordre tous les documents arrivés en sa possession relevant de la loi sur la protection des données et tous les résultats de traitement et d'utilisation pertinents et protégés par la protection des données et régis par les relations contractuelles au sens du paragraphe 2. Les supports de données du Preneur d'ordre doivent ensuite être supprimés physiquement. Les matériaux résiduels et de test doivent immédiatement être supprimés ou remis au Donneur d'ordre. L'effacement ou la suppression doit être confirmé au Donneur d'ordre par écrit, en précisant la date. Le Preneur d'ordre effectue la suppression conforme à la loi sur la protection des données des matériaux résiduels et de test sur commande du Donneur d'ordre. Le Donneur d'ordre peut dans certains cas choisir une conservation ou un transfert des données. Les supports de données transmis et toutes les copies et reproductions effectuées ici restent la propriété du Donneur d'ordre. Le Preneur d'ordre doit prendre toutes les précautions nécessaires pour que ces éléments ne soient pas accessibles à des tiers. Le Preneur d'ordre s'engage à transmettre les informations à tout moment au Donneur d'ordre, si ses données et documents sont concernés. Le Preneur d'ordre sait et accepte que le Donneur d'ordre puisse à tout moment contrôler le respect des dispositions légales relatives à la protection des données et des accords contractuels dans la mesure nécessaire, notamment en demandant des informations et en consultant les données enregistrées et les programmes de traitement des données, ou en se rendant et en visitant les locaux du Preneur d'ordre réservés à l'exécution de la commande du Donneur d'ordre. Dans ce but, le Preneur d'ordre s'engage à garantir l'accès aux locaux de l'entreprise au Donneur d'ordre ou au tiers mandaté (auditeurs).

11. Sous-traitants
Le recours à des sous-traitants n'est permis que sur autorisation écrite du Donneur d'ordre. Dans ce cas, le Preneur d'ordre doit s'assurer par un contrat que les règles établies s'appliquent également aux sous-traitants. Il doit vérifier régulièrement le respect de ces obligations. La transmission de données n'est autorisée que si le sous-traitent a rempli son obligation conformément au § 11 BDSG.

12. Obligations d'information, loi applicable
Si les données du Donneur d'ordre devaient être mises en danger par le Preneur d'ordre, en raison d'une saisie, d'une confiscation, d'une procédure d'insolvabilité ou d'une procédure transactionnelle ou de tout autre événement ou mesure prise par un tiers, le Preneur d'ordre doit en informer immédiatement le Donneur d'ordre. Dans ce cadre, le Preneur d'ordre informera immédiatement toutes les personnes responsables que les données sont la propriété et la responsabilité exclusive du Donneur d'ordre en tant qu'autorité responsable au sens de la loi fédérale allemande sur la protection des données (Bundesdatenschutzgesetz). Le droit allemand est en vigueur.

13. Description des mesures techniques et organisationnelles – Mesures de protection des données
Les informations indiquées ici se trouveront à l'avenir sur le site internet, dans la rubrique sur les informations sur la protection des données :

Contrôle d'entrée

Mesures permettant d'éviter que des personnes non autorisées n'aient accès aux installations de traitement des données avec lesquelles les données personnelles sont traitées :

Le terrain et le bâtiment sont sous vidéosurveillance 24h/24. Des capteurs de mouvements déclenchent la lumière à l'extérieur et une alarme à l'intérieur. En-dehors des heures de fonctionnement, le bâtiment est surveillé par un prestataire externe. Les fenêtres et les portes sont protégées par une alarme. Le système d'alarme est relié à la police.
Le terrain/bâtiment est clôturé jusqu'au dernier trimestre 2015.
Les visiteurs (y compris les techniciens et les clients) ne peuvent accéder à l'entreprise que via le siège. Les portes d'entrée pour les fournisseurs sont ouvertes depuis le siège pour les personnes autorisées et inscrites. En vertu du règlement, les visiteurs ne se déplacent jamais seuls dans le bâtiment et portent en permanence un badge visiteur.
Tout visiteur doit se signaler à l'accueil. L'accès de toute personne étrangère au service fera l'objet d'un compte-rendu à l'accueil. Tous les techniciens et clients doivent s'inscrire 24 heures avant leur visite pour que le prétexte de la visite puisse être vérifié.
L'accès sans surveillance au bâtiment (uniquement pour les collaborateurs) s'effectue par identification RFID associée à un mot de passe / PIN.

Accès aux Cubes
Par Cube, l'on désigne les zones organisationnelles au sein du centre de données dans lesquelles les serveurs sont placés.
L'accès à la cage d'escalier (vers les Cubes) est grillagé. Des capteurs de mouvements et des caméras viennent également protéger cette zone.
L'accès à l'étage des serveurs s'effectue par une identification gérée par le siège. (Les collaborateurs de Terra Cloud disposent d'un pass en cas d'urgence).
Toutes les portes du centre de données sont équipées d'une alarme qui se déclenche si elles restent ouvertes plus longtemps qu'autorisé (quelques secondes). Cet état est vérifié sur le mur vidéo.
Les salles de serveurs ne sont pas reliées à la structure externe du bâtiment.
L'accès à toute salle de serveurs fera automatiquement l'objet d'un compte-rendu.
Des visites de contrôle sont effectuées dans tout le bâtiment Terra Cloud au moins deux fois par jour (où l'on surveillera tout problème ou changement potentiel).

Accès Cube 1 (Hosting, Iaas & SaaS)
Seuls les collaborateurs de Terra Cloud ont accès au Cube 1. Accès par identification RFID et PIN. Les accès font l'objet d'un compte-rendu.

Accès Cube 2 (Housing)
Accès par identification RFID et PIN. Les accès font l'objet d'un compte-rendu. Chaque armoire de serveur est séparée des autres par une grille. Les portes des grilles correspondantes s'ouvrent sur inscription. Chaque client a uniquement accès aux zones qu'il loue.

Contrôle d'accès

Mesures permettant d'éviter que des personnes non autorisées puissent utiliser les installations et procédures de traitement des données :

Tous les systèmes internes sont reliés à un Active Directory. Il n'existe aucun accès administratif et direct aux systèmes de Hosting. L'accès d'administration est établi indirectement via jump server. Ces accès sont particulièrement sécurisés et nécessitent des mots de passe spéciaux :

- 16 caractères
- Minuscules et majuscules, chiffres et caractères spéciaux
- Changement tous les 7 jours
- Les mots de passe ne doivent pas être composés de noms, de mots ou de suites de touches de clavier

Tous les systèmes sont reliés au monde extérieur via une ligne internet redondante (alimentée depuis 2 Länder). Ces lignes sont sécurisées par plusieurs systèmes de pare-feux centralisés. Les normes de ces pare-feux seront modifiées régulièrement. Les pare-feux sont entretenus par un prestataire professionnel externe et sont surveillés en interne et en externe. Cela permet de garantir une détection automatique rapide des attaques.
Tous les réseaux du client sont séparés les uns des autres via VLAN.
Chaque réseau client (en option dans le domaine Housing) reçoit par ailleurs un pare-feu professionnel et un contrôle d'accès personnel pour l'auto-administration.

Contrôle d'accès aux données

Mesures permettant de limiter l'accès des personnes autorisées à utiliser les procédures de traitement des données aux données personnelles relevant de leurs compétences :

Un concept d'autorisation par ordinateur associé à Active Directory a été mis en place. La structure d'autorisation obtenue s'applique à l'ensemble du système de l'entreprise : les autorisations peuvent être différenciées en fonction des fichiers, des données, des programmes et du système d'exploitation, et les droits de lecture, de modification et de suppression peuvent être limités. L'on s'assurera que chaque utilisateur ait uniquement accès aux données pour lesquelles il possède une autorisation. Le concept d'autorisation, défini par le poste occupé par chaque collaborateur, est établi par écrit (documentation via l'Active Directory). Des profils utilisateurs prédéfinis réunissent différents droits d'accès. En outre, le concept d'autorisation est consigné dans le programme de l'application, dans l'Active Directory. Tous les accès de chaque utilisateur font l'objet d'un compte-rendu.
Il existe une séparation physique constante entre le système de gestion (Administrator) et le réseau productif (réseaux clients).
Sur les systèmes de gestion, l'on prendra soin de bien différencier l'accès dont à besoin chaque collaborateur. Chaque accès d'un collaborateur fera l'objet d'un compte-rendu.
Les mots de passe des clients servant à accéder à l'interface de gestion seront générés automatiquement en tant que mots de passe cryptés, et seront conservés cryptés dans une base de données propre. Les collaborateurs de Terra Cloud ne connaissent pas les mots de passe.

Contrôle de la transmission

Mesures permettant d'éviter que les données personnelles ne soient lues, copiées, modifiées ou éliminées par des personnes non autorisées pendant le transfert électronique, le transport ou la sauvegarde des données sur un support de données, et d'établir à quelles autorités les données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données.

Les réseaux clients sont séparés les uns des autres via VLAN. Le VLAN est géré automatiquement. Une double-attribution est impossible. Les VLAN sont également entretenus par des collaborateurs spécialement formés.
Les adresses IP publiques sont entretenues et attribuées par des collaborateurs spécialement formés.
Sur le **Cube 1**, chaque client à son propre VLAN. L'entretien du système est assuré par un administrateur de Terra Cloud. Chaque client des domaines Hosting, IaaS et/ou SaaS bénéficie d'un pare-feu virtuel. Le client peut également commander des sauvegardes régulières contre un supplément : ainsi, les sauvegardes physiques sont établies en flux codé et conservées dans d'autres compartiments coupe-feu ou, sur demande, sur un centre de données partenaire pour que le client y ait accès électroniquement.
Le codage des données de sauvegarde est obligatoire et est effectué par le client. Terra Cloud ne connaît pas ces mots de passe et ne peut ni les déchiffrer ni les réinitialiser.
Sur le **Cube 2**, un VLAN propre est également mis en place. L'entretien du système est cependant entièrement à la charge du client (concept de colocation/housing). Toutes les mesures de sécurité dépendent donc du client.
Sur les **Cubes 1 et 2**, il est possible de commander une protection contre les logiciels malveillants pour le pare-feu. Cependant, par défaut, aucune protection End Point n'est prévue. Le **réseau de gestion** est isolé du réseau public. Sur ce réseau, tous les appareils USB sont interdits et tous les ports USB sont désactivés. Le correctif indirect est obtenu via WSUS. Il est possible d'accéder au système via le jump server. Par ailleurs, un scanner anti-virus centralisé est installé.
Sur les **systèmes Office**, un anti-virus est installé sur tous les ordinateurs, au niveau central sur le pare-feu, sur le serveur de messagerie et sur les serveurs internes. Tous les scanners anti-virus et l'ensemble de la configuration sont entretenus au niveau central.

Contrôle de l'introduction

Mesures permettant de vérifier et d'établir a posteriori si et par qui les données personnelles ont été introduites, modifiées ou éliminées des systèmes de traitement des données.

Tous les accès au système de gestion font l'objet d'un compte-rendu. Toutes les modifications de configuration font l'objet d'un compte-rendu et sont enregistrées.
Tous les mécanismes de log et protocoles de transaction fournis par le fabricant du logiciel sont utilisés pour dresser des compte-rendus de toutes les introductions pour toutes les applications.
Par ailleurs, les modifications sont répertoriées et archivées à l'aide d'un système logiciel de gestion du changement basé sur des tickets.

Contrôle de disponibilité

Mesures permettant de protéger les données personnelles contre toute suppression ou perte accidentelle.

Les sauvegardes du système interne de gestion et du système Office interne sont effectuées selon un plan de sauvegarde. De plus, les sauvegardes sont conservées en géo-redondance. Aucune sauvegarde n'est effectuée de manière standard sur les deux Cubes.
L'alimentation électrique de Terra Cloud est intégrée via un réseau en anneau. L'alimentation est garantie à l'entreprise par contrat.
L'entreprise installe une alimentation redondante sans interruption (ASI) qui intègre des équipements de protection contre la foudre et les surtensions. Le fonctionnement de l'alimentation sans interruption est testé automatiquement une fois par trimestre. L'ASI peut alimenter l'ensemble du centre de données en électricité pendant 20 minutes. En cas de panne d'électricité, un groupe électrogène de secours alimenté par un réservoir de diesel d'un volume suffisant pour assurer l'alimentation pendant cinq jours est à disposition. Le fonctionnement du groupe électrogène de secours est testé une fois par mois.
La connexion à internet est assurée par deux lignes différentes et physiquement séparées, issues de deux Länder différents. Les deux lignes ne se croisent pas.
Le refroidissement de la salle de serveurs est effectué 90 % de l'année via un système de refroidissement à air. À cet effet, deux systèmes de climatisation ont été installés de manière redondante. Les deux installations sont connectées pour que les deux surfaces froides passives soient à la disposition du "chiller".
Des capteurs sont placés dans l'ensemble du bâtiment en protection contre les fuites d'eau et d'humidité.
L'entreprise dispose également de bacs de rétention d'eau à tous les endroits nécessaires et d'installations de déshydratation et de drainage sur le terrain. Par ailleurs, la zone des serveurs est constituée d'un double sol de 60 cm d'épaisseur.
L'installation d'extinction est constituée d'une installation d'extinction N2 avec alerte incendie et d'une détection précoce des incendies. Le système d'alerte incendie est directement relié aux pompiers. Des extincteurs spéciaux sont également disponibles sur place. Pour compléter la protection incendie, les pompiers effectuent des visites régulières. Les pompiers se chargent également de dispenser régulièrement des formations sur les opérations d'extinction au sein du centre de données.
Une gestion centralisée des correctifs avec environnement de test physiquement séparé est également disponible. Pour la gestion des correctifs, des exercices d'intervention d'urgence et des délais de maintenance réguliers sont organisés pour tous les techniciens (et répertoriés).

Contrôle de séparation

Mesures permettant de s'assurer que les données collectées ou à traiter à des fins différentes soient traitées séparément.

Le principe de séparation s'applique pour la séparation du Cube 1, du Cube 2 et du système de sauvegarde (ligne supplémentaire).
Sur le **Cube 1**, chaque client dispose de son propre VLAN et de son propre pare-feu. Sur le **Cube 2**, des armoires et des grilles individuelles sont installées. Le système de sauvegarde dispose de sa propre alimentation et est sécurisé par un chiffrement AES 256 bit. Le mot de passe utilisé ne peut être ni réinitialisé ni déchiffré par Terra Cloud.