Annexe 1: Description des activités de traitement des données

Cette annexe décrit les activités générales de traitement des données effectuées dans le cadre des services que propose Siemens pour le Produit ainsi que les personnes et les catégories de données personnelles concernées.

Produit	**Service**	**Explication**
Building Operator	Stockage de données	Les adresses de messagerie et de contact sont enregistrées/hébergées en sécurité (chiffrement) en tant que nom d'utilisateur pour se connecter au produit et contact pour toute question (via l'ID Siemens). Elles sont enregistrées sur Horizon.
	Assistance logicielle 3ème niveau	Des fichiers visibles dans le système du client peuvent contenir des données personnelles (par exemple des noms de personnes ou d'employés, des fichiers journaux des activités des utilisateurs).
Catégories de personnes concernées • Collaborateurs des clients et / ou de tierces parties qui exploitent ou utilisent le Produit.		
Catégorie de données • Principales données à caractère personnel (nom, nom d'utilisateur, adresse professionnelle, validité, droits d'utilisateur, matricule, droits d'accès, etc.) • Interlocuteurs (adresse e-mail, numéro de téléphone) • Activités journalisées (par exemple modification de configuration du système)		

Annexe 2: Mesures techniques et organisationnelles en application de l'article 32 de la Réglementation Générale pour la Protection des Données ("RGPD")

1. Contrôle d'accès physique

Les mesures suivantes sont mises en œuvre pour empêcher un accès physique non autorisé aux locaux, bâtiments ou pièces qui abritent des systèmes qui traitent et/ou utilisent des données personnelles :

a) Les composants physiques des datacenters, serveurs, équipements réseau et logiciels hôtes sont hébergés dans des installations banalisées.
b) Des barrières physiques tant au niveau périmétrique (par ex. clôtures, murs) qu'au niveau des points d'accès au bâtiment interdisent de pénétrer sans autorisation dans ces installations.
c) Les points d'accès physiques aux emplacements des serveurs sont gérés par des dispositifs de contrôle d'accès électroniques et sécurisés par des appareils de détection d'intrusion qui émettent des alarmes sonores si l'on force l'ouverture de la porte ou si l'on maintient celle-ci ouverte.
d) Établissement d'autorisations d'accès pour les collaborateurs et les tiers, avec la documentation correspondante.
e) Tous les visiteurs sont obligés de s'identifier et sont enregistrés.
f) Recours à des caméras (vidéosurveillance) pour surveiller l'accès physique aux installations du datacenter.
g) Les datacenters sont surveillés par un personnel de sécurité 24x7, positionné à l'intérieur et autour du bâtiment.

2. Contrôle d'accès aux systèmes

Les mesures suivantes sont mises en œuvre pour empêcher d'utiliser sans autorisation les systèmes de traitement des données qui fournissent les services numériques :

a) L'utilisateur et l'administrateur accèdent aux datacenters, serveurs, équipements réseau et logiciels hôtes selon un modèle de droits d'accès basé sur des rôles. Ils reçoivent un ID unique pour gérer convenablement leur authentification sur tous les composants du système.
b) Le principe du moindre privilège garantit que les utilisateurs n'accèdent au système que pour remplir leur mission. Lorsqu'un compte utilisateur est créé, il dispose d'un accès minimum. Pour obtenir un accès au-delà de ces moindres privilèges, il faut disposer des autorisations adéquates.
c) Les privilèges d'accès informatiques sont révisés régulièrement par le personnel compétent.
d) L'accès aux systèmes est révoqué au bout d'un délai raisonnable une fois que l'utilisateur a été supprimé (compte désactivé).
e) Des mots de passe/phrases secrètes à usage unique sont attribués, qui doivent être modifiés immédiatement après la première utilisation.
f) Les mots de passe/phrases secrètes de l'utilisateur sont changés au moins tous les 90 jours, et doivent respecter des critères de complexité.
g) Les actions relatives à la sécurité sont enregistrées avec un horodatage.
h) Expiration automatique d'une session utilisateur en cas d'inactivité, et obligation de rentrer son identifiant et son mot de passe pour rouvrir la session.
i) Les équipements (par exemple ordinateurs portables) sont configurés avec des logiciels antivirus permettant de filtrer le courrier électronique et détecter les programmes malveillants.
j) Des mécanismes de pare-feu sont configurés pour restreindre l'accès à l'environnement informatique et délimiter des grappes d'ordinateurs.
k) Les pare-feu sont actualisés régulièrement avec des stratégies (fichiers de configuration).

3. Contrôle d'accès aux données

Les mesures suivantes garantissent que les personnes habilitées à utiliser les systèmes de traitement des données accèdent aux Données personnelles uniquement lorsqu'elles en ont le droit, et que les Données personnelles ne sont ni lues, ni copiées, modifiées ou supprimées sans autorisation au cours du traitement, de l'utilisation et du stockage.

a) L'utilisateur et l'administrateur accèdent aux datacenters, serveurs, équipements réseau et logiciels hôtes selon un modèle de droits d'accès basé sur des rôles. Ils reçoivent un ID unique pour gérer convenablement leur authentification sur tous les composants du système.
b) Le principe du moindre privilège garantit que les utilisateurs n'accèdent au système que pour remplir leur mission. Lorsqu'un compte utilisateur est créé, il dispose d'un accès minimum. Pour obtenir un accès au-delà de ces moindres privilèges, il faut disposer des autorisations adéquates.
c) Les privilèges d'accès informatiques sont révisés régulièrement par le personnel habilité.
d) La lecture et la modification des Données personnelles donne lieu à un enregistrement avec horodatage.
e) Un plan d'intervention a été mis en place pour parer aux éventualités suivantes en cas d'incident :
   - Rôles, responsabilités et stratégies de communication et de contact en cas d'atteinte à l'intégrité.
   - Procédures spécifiques de réaction aux incidents.
   - Protection et réaction de tous les composants système critiques

4. Contrôle de la transmission des données

Les mesures suivantes sont mises en œuvre pour s'assurer que les Données personnelles ne sont pas lues, copiées, modifiées ou supprimées sans autorisation pendant leur transfert :

a) Prévention de copie non autorisée: Les mesures décrites précédemment prévoient d'empêcher la copie illégale de l'infrastructure de stockage physique en tant que telle (par exemple en transférant des données sur un support externe comme un disque dur).
b) Utilisation d'un modèle de droits d'accès à base de rôles : décrit précédemment.
c) Politiques de pare-feux : décrites précédemment.
d) Mise en œuvre d'un plan d'intervention : décrit précédemment.
e) Démantèlement du dispositif de stockage : quand un dispositif de stockage a atteint la fin de sa durée de vie utile, une procédure de démantèlement est prévue pour empêcher d'exposer les données du client à des tiers non autorisés. Toutes les unités de mémoire magnétique sont démagnétisées et détruites physiquement en conformité avec les pratiques courantes du métier et la loi de protection des données en vigueur.
f) Points d'accès sécurisés : seul un nombre limité de points d'accès autorisent l'accès au cloud par établissement d'une session de communication sécurisée avec vos instances de stockage ou d'ordinateur au sein des Services.
g) Connexion du personnel au réseau : le personnel se connecte au réseau par le biais d'un mécanisme d'authentification sécurisée qui limite l'accès aux appareils du réseau et à d'autres composants sur le cloud.

5. Contrôle de saisie des données

Les mesures suivantes sont mises en œuvre pour déterminer rétrospectivement si, et par quelle personne, des **Données personnelles** ont été saisies, modifiées ou supprimées des systèmes de traitement des données qui fournissent les services numériques :

Historique des activités utilisateur : les développeurs et administrateurs qui ont besoin d'accéder à nos systèmes pour de la maintenance doivent explicitement en faire la demande. Le personnel autorisé se connecte au réseau par le biais d'un mécanisme d'authentification sécurisée qui limite l'accès aux appareils du réseau et à d'autres composants sur le cloud et enregistre toutes activités pertinentes pour une évaluation de la sécurité.

6. Contrôle du respect des instructions

Les mesures suivantes sont mises en œuvre pour garantir que les Données personnelles traitées pour votre compte ne peuvent l'être que conformément à vos instructions :

a) Communication interne : différentes actions de communication interne sont menées au niveau mondial pour aider les collaborateurs à comprendre leurs rôle et responsabilités et communiquer les événements significatifs en temps utile. Parmi ces actions figurent notamment des programmes d'orientation et de formation des nouveaux embauchés et des réunions de direction régulières pour communiquer entre autres sur la performance des activités.
b) Dissociation de l'entreprise : Le réseau de production est logiquement dissocié du réseau d'entreprise par un ensemble complexe de dispositifs de sécurité et de séparation. Les développeurs et administrateurs qui ont besoin d'accéder à nos systèmes pour maintenance doivent explicitement y demander l'accès. Le personnel autorisé se connecte ensuite au réseau via des moyens sécurisés.
c) Programme de conformité rigoureux : l'infrastructure informatique est conçue et administrée selon les meilleures pratiques de sécurité et certaines normes de sécurité informatique.
d) Politiques et sensibilisation à la sécurité : nous et nos Autres sous-traitants organisons périodiquement des formations de sensibilisation à la sécurité auprès de tous les utilisateurs des systèmes d'information. Des politiques et procédures ont été élaborées à partir des besoins de sécurité et de protection des données.

7. Contrôle de disponibilité

Les mesures suivantes sont mises en œuvre pour protéger les Données à caractère personnel contre la destruction ou la perte accidentelle ou intentionnelle.

a) Détection incendie et extinction : Des équipements de détection et d'extinction incendie sont installés dans nos datacenters. Le système de protection contre l'incendie utilise des détecteurs de fumée dans tous les environnements de datacenters, espaces d'infrastructure mécanique et électrique, locaux de production de froid et de chaud.
b) Systèmes d'alimentation redondants : les systèmes d'alimentation électrique des datacenters sont conçus pour être entièrement redondants et accessibles à la maintenance, transparents pour le fonctionnement, 24 heures sur 24 et sept jours sur sept. Des onduleurs fournissent une alimentation de secours en cas de panne électrique des charges critiques et vitales de l'installation. Les datacenters utilisent des générateurs pour fournir une alimentation de secours à l'ensemble de l'installation.
c) Régulation de la température et de l'ambiance : le personnel et les systèmes surveillent et régulent les niveaux de température et d'humidité adéquats dans les datacenters.
d) Maintenance préventive : l'exécution d'une maintenance préventive assure le fonctionnement continu de l'équipement des datacenters.

8. Contrôle de séparation des données

Les mesures suivantes sont mises en œuvre pour s'assurer que les Données personnelles recueillies à différentes fins peuvent être traitées séparément :

a) Environnement de locataires multiples : la plateforme est un environnement virtuel de plusieurs tenants. Des processus de gestion de la sécurité et des contrôles de sécurité conçus pour isoler chaque client de l'autre sont mis en place. Des systèmes empêchent les clients d'accéder à des hôtes physiques ou à des instances qui ne leur sont pas attribués par filtrage via le logiciel de virtualisation.
b) Dissociation de l'entreprise : décrit précédemment.

Annexe 3: Liste des Autres sous-traitants approuvés

Cette annexe énumère tous les Autres sous-traitants engagés par Siemens pour fournir des Services au client

Nom du sous-traitant	Pays du sous-traitant	Service fourni par le sous-traitant	Garanties de transfert mises en œuvre par le sous-traitant	
Amazon Web Services Inc. (y compris autres entités, voir : https://aws.amazon.com/de/compliance/sub-processors)	USA **Remarque :** AWS est certifié Privacy Shield. Les données sont traitées exclusivement au sein de l'EEE (en l'occurrence à Dublin).	Hébergement des données	☒ ☐ ☒ ☐	Sans objet, Autre sous-traitant situé dans l'Espace Économique Européen / un pays bénéficiant d'une décision d'adéquation Contrat type UE Privacy Shield BCR-P
Atos IT Solutions and Services GmbH	Atos IT Solutions and Services GmbH	Administration et service informatiques	☒ ☐ ☒ ☐	Sans objet, Autre sous-traitant domicilié dans l'Espace Économique Européen / un pays bénéficiant d'une décision d'adéquation Contrat type UE Privacy Shield BCR-P
Sociétés affiliées Siemens	Inde (veuillez adapter au besoin pour votre pays)	Développement de logiciel sur le cloud et déploiements AWS	☒ ☒ ☐ ☐	Sans objet, Autre sous-traitant domicilié dans l'Espace Économique Européen / un pays bénéficiant d'une décision d'adéquation Contrat type UE Privacy Shield BCR-P