NAVIFY INVENTORY

ANNEXE - Accord Spécifique de Traitement des Données à Caractère Personnel

entre

CLIENT

- le Responsable de Traitement -

- ci-après dénommé le CLIENT -

et

ROCHE DIAGNOSTICS FRANCE

- le Sous-Traitant -

- ci-après ROCHE -

1. CHAMP D'APPLICATION

(1) Termes applicables. Le présent Accord Spécifique de Traitement de Données à Caractère Personnel ("**l'Accord**") est gouverné par les Conditions Générales Produits Numériques et Services associés et son annexe relative au traitement des données à Caractère Personnel (« les Conditions Générales »). Tous les termes figurant avec une majuscule ont le sens défini dans le présent Accord ou le cas échéant dans les Conditions Générales Produits Numériques et Services associés et son annexe de traitement des données à caractère personnel. Les termes et conditions du présent Accord s'appliquent uniquement à l'Offre.

(2) Conditions spécifiques à l'Accord. Les termes et conditions spécifiques applicables à l'Accord sont décrits ci-aprèS

(3) Objet. L'objet du présent Accord résulte de l'Offre ROCHE

(4) Durée. La durée de cet Accord correspond à la Durée du Contrat.

2. SPECIFICATION

(1) Nature et finalité du traitement des Données personnelles par ROCHE pour le CLIENT: fournir les Services tels que décrits dans l'Offre.

(2) Portée géographique. : Le traitement des données personnelles convenu par contrat sera effectué comme défini dans les Conditions Générales.

En outre, aux fins du présent Accord, le traitement des données personnelles peut être traité en dehors de l'Union européenne (comme décrit dans la section 4 ci-dessous). Le niveau de protection adéquat est le résultat de clauses contractuelles standard (article 46, paragraphe 2, points c et d du RGPD) (CCS). ROCHE déclare et reconnaît que l'outil

de transfert est efficace sur le lieu de destination et que les mesures techniques et organisationnelles sont définies à l'Annexe A.

(3) Categorie des personnes concernées : Les catégories de Personnes Concernées sont les employés, les prestataires et les agents du CLIENT qui utilisent la Solution Logicielle.

(4) Type de données : e-mail, nom, prénom..

3. MESURES TECHNIQUES ET ORGANISATIONNELLES

(1) Les Mesures Techniques et Organisationnelles nécessaires figurent à l'Annexe A du présent Accord et sont par les présentes approuvées par le CLIENT. À compter de la date d'entrée en vigueur du présent Accord, le CLIENT reconnaît et accepte de considérer les Mesures techniques et organisationnelles décrites dans le présent Accord comme appropriées, en tenant compte de l'état actuel du développement technologique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité du risque pour les Personnes concernées.

(2) Les mesures documentées constituent la base de cet Accord . Dans la mesure où le CLIENT exige des modifications, ces modifications seront mises en œuvre d'un commun accord.

4. SOUS-TRAITANCE

ROCHE peut faire appel à des sous-traitants (sous-traitants supplémentaires) comme décrit dans les Conditions Générales. En outre, les sous-traitants suivants sont expressément approuvés par le CLIENT aux fins du présent Accord :

Sous-traitants	Entités juridiques/pays	Service
Filiales de Roche impliquées dans le Global Customer Services	Roche Diagnostics International AG, Suisse Roche Diagnostics S.L, Espagne	Prestation de services d'assistance tels que décrits dans le formulaire de commande pour l'assistance de deuxième et troisième niveau.
Amazon Web Services, Inc.	Francfort (Allemagne) pour les clients EMEA et APAC et Ohio (États-Unis) pour les clients NA et LATAM.	Amazon Web Services (AWS) en tant que fournisseur d'hébergement et de services de sécurité pour la maintenance de la sécurité des services. Toutes les données seront hébergées exclusivement sur l'instance AWS à Francfort (Allemagne) pour les clients d'EMEA et de la région APAC et en Ohio (États-Unis) pour les clients de NA et de LATAM.

Landra Sistemas, S.L.	C/Cataluña, 47 ENT 15570 Narón, A Coruña, Spain	Équipe de développement et d'entretien des produits de navify® Inventory
Redsauce Engineering Services, S.L.	c/ Catalunya 72, 08840 Viladecans (Barcelona), Spain	Équipe de développement et d'entretien des produits de navify® Inventory

A - Mesures techniques et organisationnelles

1. Confidentialité (article 32, paragraphe 1, point b du RGPD)

- **Contrôle d'accès physique:**

  navify® Inventory est une solution basée sur le cloud, exécutée sur une infrastructure virtuelle, gérée par ROCHE et hébergée sur Amazon Web Services (AWS). Toutes les installations de traitement des données sont protégées contre les accès non autorisés par des mesures d'authentification sécurisées. L'accès physique aux installations de ROCHE est limité et contrôlé au minimum par des contrôles biométriques, des badges d'entreprise, des verrous physiques et des gardes de sécurité. Le contrôle d'accès physique aux centres de données AWS est géré par AWS.

  Les centres de données gérés par AWS qui hébergent des données sensibles sont à la pointe de la technologie et utilisent des approches architecturales et d'ingénierie innovantes. Les centres de données sont hébergés dans des installations anonymes situées dans l'UE, en particulier dans la région de Francfort, en Allemagne, et au Royaume-Uni, en particulier dans la région de Londres. L'accès physique est strictement contrôlé à la fois au niveau du périmètre et aux points d'entrée du bâtiment par le personnel de sécurité qui utilise la vidéosurveillance, les systèmes de détection d'intrusion et d'autres moyens électroniques. Le personnel AWS autorisé doit passer l'authentification à deux facteurs au moins deux fois pour accéder aux étages du centre de données. Tous les visiteurs et les sous-traitants doivent présenter une pièce d'identité, s'inscrire et être escortés en permanence par le personnel autorisé.

  L'accès physique aux centres de données n'est fourni qu'aux personnes qui ont un besoin professionnel légitime de ces privilèges. Cela est déterminé par les politiques et les procédures d'AWS, et inclut à la fois les employés autorisés et les sous-traitants approuvés qui exécutent les services convenus dans l'environnement physique. Lorsqu'un collaborateur ou un prestataire n'a plus besoin de ces privilèges pour l'entreprise, son accès est immédiatement révoqué, même s'il reste collaborateur ou prestataire. Tous les accès physiques aux centres de données sont consignés et vérifiés régulièrement par le biais de jetons physiques (c.-à-d. des badges) et d'exigences d'authentification secondaires (c.-à-d. des jetons, des données biométriques, des pin) en fonction de l'emplacement spécifique saisi dans le centre de données. Tous les emplacements de prise en charge des clients nécessitent une authentification multifacteur désignée par AWS.

  Les centres de données sont surveillés par le personnel AWS pour les systèmes et équipements électriques, mécaniques et de soutien à la vie afin que tout problème soit immédiatement identifié. Une maintenance préventive est effectuée pour maintenir la disponibilité continue de l'équipement.

- **Contrôle d'accès électronique:**

  Assurer une gestion complète de l'identité de l'utilisateur et du cycle de vie des comptes, de l'intégration à la résiliation, afin d'empêcher tout accès non autorisé aux systèmes de traitement et de stockage des données. Tout accès à navify® Inventory est sécurisé par authentification de sorte que chaque compte d'utilisateur dispose d'un mot de passe sécurisé qui est géré par une politique (complexité, heure de réinitialisation, etc.). La solution utilise également une communication sécurisée de bout en bout (cryptage en transit) et crypte les données au repos (dans les bases de données).

- **Contrôle d'accès interne (autorisations pour les droits d'accès utilisateur et de modification des données):**

  navify® Inventory fonctionne selon des politiques et des contrôles visant à empêcher la lecture, la copie, la modification ou la suppression non autorisées de données dans le système. L'accès est défini en fonction du rôle spécifique attribué à chaque utilisateur. Le personnel de Roche n'a pas de droits d'accès aux données des clients stockées dans le système. Si un accès est requis dans des cas exceptionnels (par exemple, pendant l'assistance du client), un processus strict de gestion des accès est appliqué pour s'assurer que l'accès est maintenu au minimum requis. Les journaux d'application ne contiennent aucune donnée personnelle sensible.

- **Contrôle d'isolement:**

  navify® Inventory est hébergé sur une plateforme multi-locataires avec une segmentation claire des données entre les locataires (isolement au niveau du locataire) et les applications (isolement au niveau de l'application). Le traitement isolé des données est contrôlé par la couche d'autorisation, qui met en œuvre des politiques visant à limiter l'accès des utilisateurs aux données.

- **Pseudonymisation (article 32, paragraphe 1, point a du RGPD; article 25, paragraphe 1 du RGPD):**

  Des stratégies de cryptage sont utilisées pour s'assurer que toutes les données sont cryptées à tout moment en transit et au repos. Le cryptage, associé à des systèmes et procédures de gestion des clés appropriés, garantit que les données ne peuvent pas être associées à une personne concernée spécifique sans l'aide d'informations supplémentaires. Les clés de cryptage et de décryptage sont gérées par Roche à l'aide d'un Service de Gestion des Clés (SGC), afin de s'assurer qu'aucune personne ou aucun système non autorisé ne peut décrypter les données cryptées.

2. **Intégrité (article 32, paragraphe 1, point b du RGPD)**

- **Contrôle de transfert des données:**

  Le serveur d'extraction d'inventaire navify® est utilisé pour l'analyse de modèles de données, l'exploration de données, l'extraction de données et la surveillance des ressources. Un agent navify® Inventory Data Integration Service (Athena) est installé sur le serveur d'extraction et se connecte directement à divers systèmes de base de données d'entreprise. Il accepte également les exportations de données dans des formats de fichiers courants tels que csv, xml, etc. Les extractions basées sur des fichiers sont suspendues temporairement pendant le processus ETL. Les extractions de données sont exécutées à une fréquence spécifiée qui est configurable par le client, ou en temps réel via un flux.

  L'agent navify® Inventory Data Integration Service (Athena) utilise un protocole sécurisé et propriétaire sur un cryptage SSL/TLS de pointe pour communiquer avec le serveur navify® Inventory Data Gateway. L'agent doit s'authentifier auprès du serveur de passerelle de données navify® Inventory en utilisant un compte utilisateur navify® Inventory enregistré et un identifiant d'organisation (locataire) afin d'établir une connexion valide et active avec la Data Gateway.

  Le serveur d'extraction de données navify® Inventory s'exécute dans les locaux du client et derrière son pare-feu. Il est accessible via RDP via une connexion VPN sécurisée via le protocole IPSEC. La connexion VPN peut être fournie via Axeda (si disponible) ou le service VPN du client.

  La communication entre l'agent navify® Inventory Data Integration Service et la Data Gateway pendant l'extraction des données et le transfert vers navify® Inventory Production Cloud est sécurisée par des bibliothèques de cryptage de haut niveau.

Les données prennent en charge les principaux navigateurs contemporains, y compris, mais sans s'y limiter, Google Chrome, Mozilla Firefox, Microsoft Internet Explorer (IE), Microsoft Edge, Apple Safari, Opera. La communication entre ces navigateurs et le serveur Web Pulse est sécurisée par le protocole HTTPS avec un cryptage TLS de haut niveau de pointe.

Toutes les informations sensibles sont sécurisées et cryptées en permanence.

- **Contrôle de la saisie des données:**

  navify® Inventory extrait des données du système du client avec navify® Inventory Data Integration Service Agent. Les données extraites sont stockées dans l'entrepôt de données de transit, où elles sont validées pour la qualité, transformées, puis transférées à l'entrepôt de données de production pour les rapports et les analyses.

  Les données extraites du système du client ne sont pas modifiées par ROCHE.

3. **Disponibilité et résilience (article 32, paragraphe 1, point b du RGPD)**

   - **Contrôle de la disponibilité:**

     La prévention de la destruction ou de la perte accidentelle ou intentionnelle de données est réalisée grâce à l'architecture redondante de l'analyse de données sur plusieurs couches ainsi qu'à une stratégie de récupération des données impliquant plusieurs canaux.

     L'architecture redondante consiste du côté application d'un pare-feu d'application Web (fonctionnant sur des serveurs à charge équilibrée), des serveurs d'application Web (fonctionnant sur des serveurs à charge équilibrée), un entrepôt de données sur la base de données Vertica (avec duplication de données sur les nœuds de cluster de base de données), etc.

     Des sauvegardes de la configuration du serveur sont créées régulièrement, des sauvegardes des données sont effectuées selon un calendrier quotidien automatisé. Des tests de restauration sont effectués régulièrement pour vérifier les capacités de récupération.

     Les centres de données physiques, détenus et exploités par AWS, disposent d'équipements de sauvegarde prêts à l'urgence. La climatisation, l'alimentation électrique, les télécommunications et la connectivité Internet sont conçues de manière redondante afin que les opérations continues soient maintenues en cas d'urgence. Les systèmes d'alimentation électrique sont conçus par AWS pour être entièrement redondants. Ainsi, en cas de panne, des unités d'alimentation sans interruption peuvent être engagées pour des fonctions spécifiques, tandis que des générateurs peuvent fournir une alimentation de secours pour l'ensemble de l'installation. AWS emploie et utilise des personnes et des systèmes pour surveiller et contrôler la température et l'humidité afin d'éviter toute surchauffe et de réduire ainsi les éventuelles interruptions de service.

     Les pare-feu et les logiciels antivirus sont utilisés pour empêcher l'accès, la modification, le vol ou la destruction d'informations sensibles par toute personne non autorisée. Les canaux d'accès réseau et de communication sont configurés pour n'accepter que le trafic minimal absolu requis pour que navify® Inventory fonctionne et fonctionne comme prévu.

     navify® Inventory est surveillé en permanence et le personnel d'assistance est informé de tout écart par rapport aux conditions d'exploitation attendues pour intervenir si nécessaire.

- **Reprise rapide (article 32, paragraphe 1, point c du RGPD):**

  Des stratégies de sauvegarde sont utilisées pour garantir un rétablissement rapide des services et la conservation des données.

  ROCHE a mis en place un plan de continuité des activités/plan de reprise après sinistre (à exécuter uniquement si absolument nécessaire). Dans la plupart des cas, si les données doivent être actualisées, Data Analytics peut effectuer un rechargement historique à partir du système source et reprendre le chargement incrémentiel.

4. **Procédures pour les tests, évaluations et analyses réguliers (article 32, paragraphe 1, point d du RGPD; article 25, paragraphe 1 du RGPD)**

   - **Gestion de la protection des données:**

     L'analyse des données fonctionne selon des politiques et des procédures visant à protéger les données en fonction de leur sensibilité et de leur criticité. Des examens réguliers, des audits internes et externes sont effectués pour valider l'efficacité opérationnelle de ces politiques et procédures et garantir l'alignement et la satisfaction des exigences légales et réglementaires (HIPAA, RGPD, etc.), des cadres de contrôle internationalement reconnus (SOC2) et des normes de sécurité de l'information (système de management de la sécurité de l'information certifié selon la série de normes ISO 27000).

   - **Gestion de la réponse aux incidents:**

     Les incidents sont détectés et traités conformément à des procédures clairement définies, en se concentrant sur la quarantaine et la restauration des services conformément aux SLA applicables. Les incidents affectant des données sensibles ou personnelles, ou répondant à d'autres niveaux d'impact définis, feront l'objet d'une analyse détaillée pour identifier les causes profondes afin de définir des mesures correctives et préventives pour minimiser la probabilité d'une récurrence future.

   - **Protection des données dès la conception et protection des données par défaut (article 25, paragraphe 2 du RGPD):**

     Le cadre des politiques et procédures fonctionne comme indiqué dans la section «Gestion de la protection des données» ci-dessus.

     ROCHE Engineering suit les 10 meilleures pratiques de codage sécurisé de l'OWASP.

     En outre, des évaluations de la vulnérabilité et des tests de pénétration sont effectués tous les trimestres, et des correctifs sont régulièrement appliqués.

   - **Contrôle de la commande ou du contrat:**

     Aucun traitement de données par des tiers conformément à l'article 28 du RGPD n'a lieu sans instructions correspondantes de la part des clients. Des dispositions contractuelles claires et sans ambiguïté sont établies, les contrats avec les prestataires de services sont gérés activement, tout changement concernant les prestataires de services impliqués sera communiqué en temps opportun aux clients.