NAVIFY ANALYTICS

Annexe - Accord Spécifique de Traitement des Données à Caractère Personnel

entre

LE CLIENT

– le responsable du traitement –

– désigné ci-après le "CLIENT" –

et

Roche Diagnostics France

– le sous-traitant –

– désigné 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. 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) La nature et la finalité du traitement de données personnelles : fournir la solution informatique et ses services au CLIENT.

(2) Champ d'application géographique. Le traitement des Données à caractère Personnel contractuellement déterminé sera effectué selon les indications figurant dans l'Accord relatif au traitement des données

(3) En outre, aux fins du présent Accord, le traitement des données personnelles peut être mené en dehors des Etats Unis par les filiales de ROCHE (comme décrit dans la section 4 ci-dessous). Le niveau adéquat de protection résulte de clauses contractuelles standards (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 dans l'annexe A. Pour les transferts de données pour lesquels des lacunes potentielles dans le niveau de protection dans le pays de destination ont été identifiées, ces lacunes seront comblées par des mesures techniques et organisationnelles supplémentaires de ROCHE qui sont spécifiées à l'Annexe A.

Données traitées. ROCHE peut traiter des données personnelles ou y avoir accès pendant la mise en œuvre technique de navify Analytics for Core Lab et navify Integrator for Lab ou l'assistance et la maintenance fournies via une solution d'assistance à distance comme spécifié dans le Contrat de niveau de service. Cela dépend du CLIENT ainsi que du cas d'assistance, des données exactes partagées avec ROCHE.

Vous trouverez ci-dessous des informations détaillées sur le type et les catégories de données personnelles traitées pour la fourniture de navify Analytics pour Core Lab et navify Integrator pour Lab, Implementation and Support Services.

navify Analytics for Core Lab	
Catégories des Personnes concernées	Type de données
Collaborateurs, prestataires et agents du CLIENT (personnes physiques uniquement, pas d'entités)	Données utilisateur (ID utilisateur, nom, adresse e-mail, adresse IP, horodatages, commentaires et ID de session) Personne physique qui utilise l'instrument (technicien de laboratoire) (ID, nom, site)
Médecins ou toute autre Personne Concernée dans le secteur de la santé (HCP) en lien avec des commandes passées au CLIENT	Code de l'expéditeur, nom de l'expéditeur, adresse professionnelle
Clients du CLIENT (patients)	ID de la commande, ID de l'échantillon, ID du patient, âge, sexe, résultat du texte, ID de l'échantillon

navify Analytics for Pathology Lab	
Catégories des Personnes concernées	Type de données
Collaborateurs, prestataires et agents du CLIENT (personnes physiques uniquement, pas d'entités)	Données utilisateur (ID utilisateur, nom, adresse e-mail, adresse IP, horodatages, commentaires et ID de session) Personne physique qui utilise l'instrument (technicien de laboratoire) (ID, nom, site)
Médecins ou toute autre Personne Concernée dans le secteur de la santé (HCP) en lien avec des commandes passées au CLIENT	Code de l'expéditeur, nom de l'expéditeur, adresse professionnelle
Clients du CLIENT (patients)	ID de la commande, Code ID, Block ID , âge, Slide ID, horodatage

navify Analytics for Molecular Lab	
Catégories des Personnes concernées	Type de données
Collaborateurs, prestataires et agents du CLIENT (personnes physiques uniquement, pas d'entités)	Données utilisateur (ID utilisateur, nom, adresse e-mail, adresse IP, horodatages, commentaires et ID de session) Personne physique qui utilise l'instrument (ID, nom, site)

Clients du CLIENT (patients)	Numéro de test de l'échantillon, horodatages, résultats, commandes de tests

navify Analytics for POC	
Catégories des Personnes concernées	Type de données
Collaborateurs, prestataires et agents du CLIENT (personnes physiques uniquement, pas d'entités)	Données utilisateur (ID utilisateur, nom, adresse e-mail, adresse IP, horodatages, commentaires et ID de session) Personne physique qui utilise l'instrument (ID, nom, site)
Médecins ou toute autre Personne Concernée dans le secteur de la santé (HCP) en lien avec des commandes passées au CLIENT	Code de l'expéditeur, nom de l'expéditeur, adresse professionnelle
Clients du CLIENT (patients)	ID patient, âge, sexe, résultat texte, ID de commande et horodatages

ROCHE ne peut utiliser des Données Anonymisées ou d'autres données non personnelles à ses fins que conformément aux Conditions Générales Produits Numériques et Services signées entre ROCHE et le CLIENT et dans la mesure autorisée par les lois applicables, à condition qu'aucune ré-identification de ces Données Anonymisées ne soit légalement ou techniquement possible.

3. MESURES TECHNIQUES ET ORGANISATIONNELLES

(1) Les Mesures techniques et organisationnelles nécessaires sont indiquées à l'Annexe A au présent Accord et sont approuvées par le CLIENT. À la date d'effet du présent Accord, le CLIENT reconnaît qu'il considère les Mesures techniques et organisationnelles qui y sont décrites comme appropriées, compte tenu de l'état des connaissances technologiques, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les Personnes Concernées.

(2) Les mesures documentées constituent le fondement du présent Accord. Dans la mesure où le CLIENT demanderait que des modifications y soient apportées, celles-ci devraient être effectuées d'un commun accord.

4. SOUS-TRAITANCE

ROCHE peut faire appel à des sous-traitants (sous-traitants supplémentaires) tel qu'il est écrit dans l'Accord. En outre, les sous-traitants suivants sont expressément approuvés par le Client aux fins du présent Accord.

Sous-traitant ROCHE	Services
Filiales de ROCHE, notamment mais non limité à :	Fourniture des services tels que décrits dans l'Offre, principalement le service d'assistance pour la solution informatique. Le customer success manager appartenant aux entités juridiques décrites ci-dessous recevra la demande :

	● Roche Diagnostics Corporation, États-Unis pour les clients d'Amérique du Nord ● Roche Diagnostics Uruguay et Roche Diagnostics Brésil pour les clients de LATAM ● Roche Diagnostics Limited, Royaume-Uni et Roche Diagnostics S.L., Espagne pour les clients EMEA ● Roche Diagnostics Asie-Pacifique, Singapour pour les clients APAC La demande initiale sera toujours lue par la filiale. Les filiales décident si elles transmettent la demande au support de 1er niveau. Les filiales impliquées dans le support de 1er niveau sont : ● Roche Services (Europe) Ltd pour les clients EMEA-centre de Budapest ● Roche Services (Asie-Pacifique) Sdn. pour les clients APAC-centre de Kuala Lumpur ● Services Roche Amériques pour les clients NAM et LATAM - Centre du Costa Rica Lorsque les demandes ne peuvent pas être résolues, elles sont transmises à Roche Diagnostics International AG (Rotkreuz, Suisse) et Roche Information Solutions India Pvt Ltd (Puna, Inde). Pour le transfert de données vers l'Inde, le mécanisme de transfert est basé sur l'accord de transfert de données inter-sociétés de Roche contenant les clauses contractuelles types de l'UE du 4 juin 2021.
Amazon Web Services, Inc.	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 de l'UE, l'instance AWS à Londres (Royaume-Uni) pour les clients du Royaume-Uni, l'instance AWS en Virginie du Nord (États-Unis) pour les clients américains. Les clients situés dans les autres régions peuvent choisir l'emplacement du serveur entre Francfort, Londres et la Virginie du Nord. Roche a signé les clauses contractuelles types (version du 4 juin 2021) avec AWS, Inc
Parametric Technology Schweiz AG (« PTC ») (applicable uniquement si Remote Service Edge Agent est déployé chez le Client), Badenerstrasse 15 8004 Zürich.	Fourniture des services d'hébergement de ThingWorx plateforme fournissant un accès à distance (sessions de partage d'écran). Hébergement de ThingWorx - Microsoft Azure Amsterdam, Pays-Bas. Les sociétés affiliées à PTC sont impliquées dans le support technique et des services de conseil concernant la plateforme ThingWorx (selon la région). Cette activité de traitement des données est basée sur un Accord de traitement des données signé entre Roche Diagnostics International AG et Parametric Technology (Schweiz) AG et sur des clauses contractuelles standard en cas de transfert de données de l'UE vers des pays tiers.

A) Mesures Techniques et Organisationnelles

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

- **Contrôle d'accès physique :**

  navify Analytics 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.

  Centres de données: 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 professionnel 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 par 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 :**

  Compléter l'identité de l'utilisateur et le cycle de vie de la gestion des comptes en place, de l'intégration à la résiliation, afin d'empêcher l'utilisation non autorisée des systèmes de traitement et de stockage des données. Tous les accès à navify Analytics sont sécurisés par une authentification afin que chaque compte utilisateur dispose d'un mot de passe sécurisé qui est géré selon des règles (complexité, délai de réinitialisation, etc.). La solution fait également

appel à une communication entièrement sécurisée (cryptage en transit) et code toutes les données au repos (dans les bases de données).

- **Contrôle d'accès interne (permissions pour les droits d'accès et de modification des données par les utilisateurs) :**

  navify Analytics 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 déterminé spécifiquement par le rôle qu'une personne particulière joue. 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'isolation :

navify Analytics 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 par ailleurs l'impossibilité d'associer des données à une personne concernée spécifique sans l'aide d'informations supplémentaires. Les clés de chiffrement et de déchiffrement sont gérées par ROCHE au moyen d'un Service de gestion de clé, afin de veiller à ce qu'aucune personne ou système non autorisé ne puisse déchiffrer des données chiffrées.

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

   - **Contrôle du transfert de données :**

     Le serveur d'extraction navify Analytics est utilisé pour l'analyse de modèles de données, l'exploration de données, l'extraction de données ainsi que la surveillance des ressources. Un agent navify Analytics Data Integration Service (Athena) est installé sur le serveur d'extraction et se connecte directement à divers systèmes de bases 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 Analytics Data Integration Service (Athena) utilise un protocole sécurisé et propriétaire sur un cryptage SSL/TLS de pointe pour communiquer avec le serveur navify Analytics Data Gateway. L'agent doit s'authentifier auprès du serveur de passerelle de données navify Analytics en utilisant un compte utilisateur et un identifiant d'organisation (tenant) navify Analytics enregistrés afin d'établir une connexion valide et active avec la passerelle.

Le serveur d'extraction de données navify Analytics 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 de données et la passerelle pendant l'extraction des données et le transfert vers navify Analytics 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 à tout moment.

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

  navify Analytics extrait des données du système du client avec navify Analytics 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.

2. **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 pour permettre la poursuite des opérations en continu en cas d'urgence. Les systèmes d'alimentation électrique sont conçus par AWS pour être entièrement redondants de sorte qu'en cas de panne, des unités ASI peuvent être mises en service pour des fonctions spécifiques, alors que des générateurs peuvent assurer 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 en réduisant 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 Analytics fonctionne et fonctionne comme prévu.

navify Analytics fait l'objet d'une surveillance permanente et une assistance personnelle est informée de tout écart par rapport aux conditions opérationnelles attendues pour intervenir si nécessaire.

- **Récupération 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.

3. **Procédures de tests réguliers, d'évaluation et d'examen (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 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 des commandes ou des contrats :**

     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.