Annexe - Accord Spécifique de Traitement des Données à Caractère Personnel

entre

LE CLIENT

– le Responsable de Traitement –

– désigné ci-après le "CLIENT" –

et

Roche Diagnostics France

– le Sous-Traitant–

– désigné ci-après "ROCHE" –

1) CHAMP D'APPLICATION

(1) Conditions 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 par ROCHE pour le CLIENT des Données à caractère Personnel sont précisément déterminées dans l'Offre.

(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 aux 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). 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.

(4) Traitement pour la fourniture de la Solution Logicielle. Afin de fournir au CLIENT la navify Algorithm Suite, Roche traite des données de patients anonymisées (du point de vue de Roche, les données de patients anonymisées).

(5) Catégories de personnes concernées. Les catégories de Personnes Concernées pour ColonFlan & GAAD & KFRE sont les suivantes :

a. les patients du Client.

(6) Type de données. Le traitement des Données à caractère Personnel (les « Données ») concerne les types et catégories de Données suivants :

a. pour GAAD: âge du patient en années, sexe masculin/féminin, Elecsys AFP (résultat de laboratoire), Elecsys PIVKA-II (résultat de laboratoire),

b. pour ColonFlag: année de naissance du patient, sexe et une ou plusieurs numérations formule sanguine complète,

c. pour KFRE: âge du patient en années, sexe masculin/féminin et une ou plusieurs numérations sanguines complètes.

(7) Traitement pour l'assistance (à distance). ROCHE peut traiter des données personnelles ou y avoir accès pendant la mise en œuvre technique de la solution informatique ou l'assistance et la maintenance fournies via une solution d'assistance à distance comme spécifié dans le Contrat de niveau de service et sur autorisation du CLIENT pour chaque cas d'assistance individuel. Cela dépend du CLIENT ainsi que du cas d'assistance, des données exactes partagées avec ROCHE. Les catégories et types de données personnelles ci-dessous peuvent être traités pendant les services d'assistance :

(8) Catégories de personnes concernées. Les categories de Personnes Concernées sont les suivantes :
a. Salariés, prestataires et agents du Client,
b. Les patients du Client.

(9) Type de données. L'objet du traitement des données personnelles (« Données ») comprend les types et catégories de Données suivants :

a. En ce qui concerne la catégorie a) des sujets de données ci-dessus :
   i. Noms et coordonnées professionnelles
   ii. Données liées à l'assistance, telles que les identifiants de connexion au système (pas de mots de passe)

b. En ce qui concerne la catégorie b) des sujets de données ci-dessus :
   i. Données susceptibles d'identifier des personnes, telles que les noms ou les coordonnées (pendant le partage d'écran ou en cas de visites sur site)
   ii. Données de santé (pendant le partage d'écran ou en cas de visites sur site)

(10) Lorsque cela est techniquement possible, ROCHE limitera l'utilisation des données personnelles du CLIENT dans la mesure du possible, ce qui inclut l'anonymisation des données personnelles du CLIENT lors de la fourniture de la solution informatique ou du service respectif. ROCHE ne peut utiliser des Données Anonymisées ou d'autres données non personnelles que conformément aux Conditions Générales relatives aux Produits et aux Services Numériques 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) TRAITEMENT DES DONNÉES PERSONNELLES PAR LA SOLUTION INFORMATIQUE ET NAVIFY INTEGRATOR FOR LAB

(1) Rôle de nI. nI sert uniquement l'application qui est achetée par le CLIENT. En ce sens, si l'application traite des données personnelles, nI effectuera l'échange (la transition des données) entre le système d'information du laboratoire du CLIENT et l'application de service, ce qui signifie que ce n'est qu'à ce moment-là qu'un traitement des données personnelles par nI aura lieu.

(2) nI installé avec une solution informatique. Selon l'Offre, l'installation de navify Integrator for Lab sur l'infrastructure du CLIENT sert à la collecte de données pour la navify Algorithm Suite. Les données produites par les systèmes de laboratoire du CLIENT (contrôleur des données) sont transportées via navify Integrator for Lab vers navify Algorithm Suite. navify Integrator for Lab effectue l'échange des données du laboratoire vers l'application de service et crypte les données tout en conservant leur signification pour l'application de service (ici choisie navify Algorithm Suite). Les données restent chiffrées, préservant leur intégrité et leur signification pour l'application de service.

(3) Le transfert sécurisé de données par nI. nI ne possède pas de compréhension des données qu'il traite. Sa fonction principale est de catégoriser et de standardiser les données sans accéder à leur contenu. Ce processus garantit l'intégrité et la qualité des données lorsqu'elles servent l'application de manière sécurisée. En mettant en œuvre ces mesures, nI assure la sécurité des données et maintient un strict respect des réglementations en matière de confidentialité.

4) 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.

5) SOUS-TRAITANCE

(4) ROCHE pourra faire appel à des sous-traitants ultérieurs (d'autres sous-traitants chargés du traitement) selon les conditions de l'Accord. En outre, les sous-traitants ultérieurs suivants sont expressément agréés par le Client aux fins du présent Accord et fournir des services d'assistance comme stipulé au point 4) de cet Accord.

Sous-traitant ultérieur de ROCHE	Adresse / Pays	Service
Roche Diagnostics International AG	Forrenstrasse 2, 6343 Rotkreuz Switzerland	Fourniture de services d'assistance technique en tant qu'assistance (3e niveau) pour navify Algorithm Suite et les algorithmes.
Roche Information Solutions India Pvt Ltd à Pune, Inde	671, 75, Ganeshkhind Rd, Narveer Tanaji Wadi, Shivajinagar, Pune, Maharashtra 411005, India	Pour le transfert de données vers l'Inde: le mécanisme de transfert repose sur l'accord de transfert de données inter-sociétés de Roche fondé sur les clauses contractuelles types de l'UE du 4 juin 2021. Catégories de données personnelles mentionnées à la section 2, sous-sections (8) a et b.
Roche Diagnostics SL. à San Cugat, Spain	Avinguda de la Generalitat, 171, 173, 08174 Sant Cugat del Vallès, Barcelona, Spain	Roche Molecular Systems prendra principalement en charge l'instance américaine de navify Algorithm Suite et les algorithmes.

Roche Molecular Systems, Inc.	4300 Hacienda Drive, Pleasanton, CA 94588, USA	
Amazon Web Services	Frankfurt, Germany	Hébergement de services cloud et de stockage dans la région AWS Europe (Francfort, Allemagne) en ce qui concerne la navify Algorithm Suite et les algorithmes.
Splunk Inc.	San Francisco, Etats Unis	Fourniture de pistes d'audit et de surveillance pour la sécurité, ainsi que des indicateurs de performance concernant la navify Algorithm Suite et les algorithmes. Les services sont fournis par Splunk via AWS Region US West (Oregon, États-Unis) et AWS Region Europe (Francfort, Allemagne). Les données personnelles ne sont pas identifiables de nouveau par Splunk. L'exemple américain des services Splunk est destiné à la prise en charge aux États-Unis de la navify Algorithm Suite et des algorithmes.
PTC Schweiz AG (applicable uniquement si l'agent périphérique de service à distance 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).
Interoperability Health (UK) Limited d.b.a (applicable if the Interoperability	EEE	Agissant en tant que sous-traitant de Roche et fournissant les services d'interopérabilité entre l'application et les systèmes SIL du client.

A - Mesures Techniques et Organisationnelles
Algo Suite

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

Contrôle d'accès physique

Installations de traitement: Toutes les installations de traitement des données sont protégées contre les accès non autorisés grâce à des mesures d'authentification sécurisées.

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 datacenters sont hébergés dans des installations anonymes situées au sein de l'UE, en particulier dans la région de Francfort, en Allemagne. 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 surveillance vidéo, les systèmes de détection d'intrusion, et autres moyens électroniques. Le personnel AWS autorisé doit réussir l'authentification à deux facteurs au moins deux fois pour accéder aux étages du datacenter. Tous les visiteurs et les sous-traitants doivent présenter une pièce d'identité, s'enregistrer et être en permanence accompagnés par le personnel autorisé.

L'accès physique aux centres de données n'est autorisé qu'aux individus qui présentent un besoin légitime vis-à-vis des privilèges concernés relatifs à l'entreprise. Cela est déterminé par les politiques et les procédures d'AWS, et comprend 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, son accès est immédiatement révoqué, même s'il garde son statut au sein de l'entreprise. Tous les accès physiques aux centres de données sont systématiquement consignés et vérifiés 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 multifactorielle comme indiqué par AWS.

Les datacenters sont surveillés par le personnel AWS afin de détecter les systèmes et équipements électriques, mécaniques et de maintien des fonctions vitales, de sorte que tout problème éventuel soit immédiatement identifié. L'entretien préventif est effectué pour assurer le fonctionnement opérationnel continu de l'équipement.

Contrôle d'accès électronique

La suite NAVIFY Algorithm ne fournit pas d'accès utilisateur au système. L'accès client est limité aux messages HL7 établis - il n'y a pas d'interface utilisateur.

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

La suite NAVIFY Algorithm fonctionne selon des règles et des contrôles garantissant l'absence de lecture, de copie, de modification ou de suppression non autorisées des données du système. L'accès est spécifiquement déterminé en fonction du rôle que la personne exerce. Le personnel de ROCHE qui accède à l'infrastructure de la suite NAVIFY Algorithm ne dispose d'aucun droit d'accès aux données du client stockées sur disque ou dans les journaux d'application contenant des données personnelles.

Contrôle d'isolation

La suite NAVIFY Algorithm repose sur une architecture multi-tenant, qui stocke toutes les données d'un service particulier dans une seule base de données. L'accès aux données est strictement géré et le produit limite l'accès aux données d'un locataire aux utilisateurs appartenant uniquement à ce locataire. Ce traitement isolé de données est commandé grâce à la combinaison d'une autorisation de couche logique et d'un schéma de données visant à séparer les données de chaque installation. Le schéma de données relie toutes les données de santé d'un même établissement. L'autorisation de couche applique des stratégies de contrôle d'accès fondées sur les rôles afin de restreindre davantage les données et les ressources auxquelles chaque utilisateur est autorisé à accéder.

Pseudonymisation (Article 32, paragraphe 1, point a du RGPD ; Article 25, paragraphe 1 du RGPD)

Des stratégies de cryptage sont utilisées afin de protéger la confidentialité des données sensibles pendant la transmission sur un réseau (données en transit). Les seules données persistantes se trouvent dans les pistes d'audit, qui ne sont pas cryptées lorsqu'elles sont stockées (données au repos). Ces pistes d'audit ne contiennent aucune information personnelle. Le cryptage rend les données inintelligibles pour les entités qui n'ont pas accès à la clé cryptographique associée à l'opération de cryptage correspondante. Le cryptage des données personnelles garantit qu'il ne peut pas être associé à un sujet de données spécifique, même dans les situations où les données cryptées ont été exposées par une violation. Roche utilise de facto des algorithmes de cryptage standard, des systèmes de gestion des clés et des procédures associées pour s'assurer que les données cryptées ne sont accessibles qu'aux personnes autorisées.

Gestion des clés

La navify Algorithm Suite utilise le service de gestion des clés AWS (KMS) pour gérer de manière sécurisée les clés cryptographiques tout au long de leur cycle de vie. AWS KMS fournit une solution hautement disponible de génération de clés, de stockage, de gestion et d'audit pour le cryptage des données à travers les services AWS. AWS KMS stocke les clés principales dans des modules matériels de sécurité (HSM) approuvés FIPS 140-2. KMS est conçu de sorte que personne, y compris les employés d'AWS, ne puisse récupérer les clés principales en texte clair à partir des HSM. Les clés principales en texte clair ne sont jamais écrites sur le disque et ne sont utilisées dans la mémoire volatile des modules HSM que le temps nécessaire pour effectuer une opération cryptographique spécifique. Les mises à jour logicielles du micrologiciel du module HSM sont contrôlées par un contrôle d'accès multipartite qui est audité et examiné par un groupe indépendant au sein d'AWS ainsi que par un laboratoire certifié NIST, conformément à la norme FIPS 140-2. L'accès aux ressources KMS, telles que les demandes des services AWS pour la génération, le cryptage ou le décryptage de clés de données, est contrôlé par une politique stricte de gestion des identités et des accès, afin de s'assurer que les entités non autorisées ne peuvent pas décrypter les données cryptées. KMS exploite le service d'audit opérationnel AWS CloudTrail qui enregistre les actions effectuées par chaque utilisateur, rôle ou fonction. CloudTrail capture tous les appels de l'interface du programme d'application (API) pour KMS en tant qu'événements, y compris les appels de la console KMS et les appels de code vers les API KMS. L'activité CloudTrail est surveillée quotidiennement.

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

Contrôle du transfert de données

La navify Algorithm Suite utilise une approche de sécurité à plusieurs niveaux pour empêcher la lecture, la copie, la modification ou la suppression non autorisées de données par transfert ou transport électronique. Les ressources de la navify Algorithm Suite sont déployées dans des clouds privés virtuels (VPC). Un VPC est un espace isolé du Cloud AWS dédié à Roche en tant que client AWS. Les VPC sont segmentés en sous-réseaux IP publics et privés. Les pare-feu et les groupes de sécurité restreignent la communication vers et depuis Internet mais aussi entre les services sur le réseau interne. La connectivité réseau est refusée par défaut et nécessite une configuration par Roche pour permettre l'accès à et à partir de services spécifiques figurant sur la liste blanche. La communication entre les services au sein d'un VPC s'effectue via des canaux cryptés et mutuellement authentifiés, établis selon le protocole TLS 1.2. TLS 1.2 assure les contrôles d'intégrité des messages dans le cadre du protocole TLS handshake et permet à Roche d'exercer un contrôle sur les algorithmes utilisés pour le cryptage symétrique, l'échange de clés, l'authentification d'entité et l'intégrité des messages.

Cryptage

Toutes les données des clients sont chiffrées lors de leur transfert au sein du Virtual Private Cloud (VPC) de Roche et entre chaque instance. Pour ce faire, les données HTTPS et TLS 1.2 sont chiffrées pour le tunnel.

Réseaux privés virtuels (VPN): l'accès de Roche à tous les VPC et instances AWS est accordé via un VPN SSL (Secure Sockets Layer) basé sur le client. Toutes les authentifications SSL nécessitent une authentification multifactorielle(MFA).

Signature numérique: Roche utilise des algorithmes de signature asymétrique TLS 1.2 à chaque niveau de l'environnement Roche (par ex. Kubernetes, Amazon DocumentDB) afin de s'assurer que la personne titulaire de la demande d'accès est un utilisateur autorisé. TLS 1.2 permet aux clients de signaler les algorithmes de signature et les fonctions de hachage pris en charge et préférés. Cela permet à Roche de contrôler la prise en charge et les préférences spécifiques des algorithmes de signature.

Contrôle de la saisie des données

Les transactions effectuées dans la suite NAVIFY Algorithm sont enregistrées à l'aide d'un service de pistes d'audit qui consigne les informations échangées et le système avec lequel elles ont été effectuées. Ces données de piste d'audit ne contiennent pas de données personnelles, ne sont pas chiffrées au repos et ne sont disponibles que pour les utilisateurs Roche autorisés.

Perte des données

Des mécanismes de prévention des fuites de données (DLP) sont en place pour les environnements Roche. Les administrateurs de la plate-forme Roche NAVIFY accèdent aux systèmes Roche à l'aide de l'AWS Management Console qui est protégée par l'authentification unique Roche pour administrer et gérer le système.Les agents Dome9 suivent les changements et les activités dans l'environnement AWS, y compris l'identification de la personne, les données et l'horodatage de l'activité.

3. Disponibilité et Résilience (Article 32, paragraphe 1, point b du RGPD)

Disponibilité

Les services cloud de Navify Algorithm suite sont déployés à l'aide d'un système distribué, de tolérance aux pannes, à auto-réparation et à mise à l'échelle automatique, prenant en charge plusieurs instances de chaque service pour assurer une disponibilité maximale.

Le risque de corruption accidentelle ou intentionnelle, de destruction ou de perte d'accès aux données est atténué grâce à une stratégie de sauvegarde Cloud automatisée qui implique la duplication, la distribution et le stockage de données sur un système composé de plusieurs serveurs situés dans des emplacements physiquement séparés. Les données sont sauvegardées via la création de copies ou «sauvegardes» de la configuration et des données, qui sont ensuite transférées régulièrement vers un emplacement physique distinct. Lorsque la récupération des données est nécessaire, les fichiers de base de données copiés sont mis en ligne dans l'un des emplacements physiques disponibles.

La suite NAVIFY Algorithm est hébergée dans la région AWS de Francfort, Allemagne. Une région AWS est un groupe indépendant de centres de données AWS construits dans un lieu géographique spécifique (pays). Chaque région AWS se compose de 2 à 6 zones de disponibilité AWS, qui sont des centres de données discrets avec une alimentation, un réseau et une connectivité redondants, logés dans des environnements contrôlés (température, humidité, incendie, eau, électricité statique et sécurité physique) dans des installations séparées. Les zones de disponibilité offrent à Roche la possibilité d'exploiter des applications et des bases de données de production plus haute disponibilité, plus tolérantes aux pannes et plus évolutives que ce qu'un seul datacenter pourrait supporter.

Des plans d'urgence ont été élaborés pour tenir compte des perturbations des services. Ces plans sont testés régulièrement par le biais de simulations et de tests. Les conclusions de ces exercices sont documentés et les domaines d'amélioration sont intégrés à l'environnement technique et au processus d'urgence.

Les pare-feu, les systèmes de détection et de prévention des intrusions (IDS/IPS) ainsi que les logiciels antivirus sont utilisés afin d'empêcher l'accès, la modification, le vol ou la destruction d'informations sensibles par toute personne non autorisée. Le résultat de ces outils de sécurité est contrôlé 24 heures par jour. Si une activité anormale est détectée, des mesures proactives sont prises afin de prévenir tout dommage au système. Si nécessaire, le problème est examiné et documenté.

Évaluations des risques et tests

Les évaluations des risques comprennent l'évaluation de plusieurs facteurs qui peuvent avoir un impact sur la sécurité, ainsi que la probabilité et l'impact d'une perte de confidentialité, d'intégrité et de disponibilité des informations et des systèmes. Les activités de gestion des risques pour navify Algorithm Suite ont été initiées pendant la planification du produit et se poursuivent tout au long des activités de conception et de développement, de test, de production et après le lancement. Roche évalue et améliore continuellement les processus d'évaluation et de gestion des risques afin d'inclure les menaces nouvelles et en évolution. Les efforts d'évaluation et de test des risques comprennent les éléments suivants :

Tests de pénétration des applications: des tests de pénétration sont effectués chaque année pour identifier les vulnérabilités potentielles des applications. Les équipes chargées des applications et de l'infrastructure utilisent une approche fondée sur les risques pour hiérarchiser et atténuer ces vulnérabilités et minimiser les risques potentiels.

Plan et rapports de cybersécurité: le plan et les rapports de cybersécurité sont créés et examinés par une équipe interfonctionnelle pour mieux comprendre la position en matière de risque de sécurité logicielle. Les efforts comprennent l'identification et l'évaluation de la criticité des données traitées et stockées par le système, une évaluation de l'exposition du système aux cyberattaques et aux risques commerciaux associés, une évaluation des risques du schéma de réseau de la solution, des interfaces API et du flux de données.

Évaluations des risques par des tiers : les tiers qui ont accès aux données personnelles sont évalués pour détecter un risque potentiel en matière de sécurité, de confidentialité et de conformité réglementaire. Les risques sont évalués dans plusieurs domaines pour s'assurer que la position et les contrôles de sécurité et de conformité du tiers sont en place.

Conception de systèmes redondants

La conception du système inclut l'utilisation d'Amazon DocumentDB pour l'approvisionnement d'une infrastructure de stockage durable pour les charges de travail critiques. Amazon DocumentDB utilise un système de stockage unique, distribué, à tolérance de pannes et autoréparateur, qui réplique plusieurs copies des données dans plusieurs zones de disponibilité afin d'offrir une disponibilité et une durabilité élevées. Lors de l'enregistrement de données, Amazon DocumentDB s'assure que toutes les écritures sont enregistrées durablement sur une majorité de noeuds avant de confirmer que les données ont été stockées avec succès. De plus, Amazon DocumentDB détecte et répare automatiquement les défaillances du système de stockage afin d'éviter la perte de données et de réduire la nécessité d'effectuer une restauration ponctuelle. Amazon DocumentDB bénéficie du contrat de niveau de service Amazon DocumentDB, conçu pour offrir une durabilité de 99,9999999999% et une disponibilité d'au moins 99,9%.

Sauvegardes

Roche a développé une stratégie de sauvegarde et de restauration de base pour l'environnement NAVIFY Algorithm Suite qui garantit que les composants système et les données associées peuvent être rapidement restaurés et que les données sont conservées. Chacun des composants AWS utilise une stratégie de sauvegarde et de restauration légèrement différente qui inclut l'utilisation de zones à disponibilité multiple et de groupes à mise à l'échelle automatique à réparation automatique.

Récupération rapide (Article 32, paragraphe 1, point c du RGPD)

Des stratégies de récupération sont utilisées pour s'assurer que les services peuvent être rapidement récupérés et que les données sont conservées. La récupération rapide de l'infrastructure Cloud et des services d'application est gérée à l' aide de pipelines automatisés de livraison continue pouvant déclencher de nouveaux déploiements de l'infrastructure et des services de la suite Algorithm de NAVIFY à la demande.

Les données sont stockées dans des bases de données Amazon DocumentDB qui utilisent des fonctionnalités de sauvegarde automatisées permettant une récupération instantanée. Amazon DocumentDB effectue automatiquement un instantané quotidien complet des données (pendant les sauvegarde préférées) et capture les journaux de transactions. Les sauvegardes sont stockées dans des compartiments Amazon S3 gérés par les services pour garantir la disponibilité et la durabilité avec des périodes de conservation configurables. Les opérations de restauration point in time peuvent être effectuées jusqu'à la seconde spécifique de la période de rétention en appliquant les journaux de transactions à la sauvegarde quotidienne la plus appropriée.

4. Procédures de tests réguliers, d'évaluation et d'examen (Article 32, paragraphe 1, point d du RGPD ; Article 25, paragraphe 1 du RGPD)

Roche a mis en œuvre une série de mesures pour tester, évaluer et tester son cadre de contrôle de sécurité, notamment la mise en œuvre d'outils de surveillance et d'alerte de la conformité en matière de sécurité et de gestion des vulnérabilités, les tests de pénétration dans le réseau, les évaluations des risques et les audits tiers.

Contrôle des commandes ou des contrats

Aucun traitement de données par des tiers conformément à l'article 28 du RGPD sans instructions correspondantes de la part du CLIENT, par exemple des dispositions contractuelles claires et sans ambiguïté, une gestion formalisée des commandes, des contrôles stricts sur la sélection du Prestataire de services, une obligation de pré-évaluation, des contrôles de surveillance et de suivi.

5. Politique de sécurité

ROCHE ou ses sous-traitants pour les services commandés ne cesseront d'appliquer, à l'échelle mondiale des politiques, des normes et des procédures visant à protéger les données personnelles. Ces politiques comprennent, sans s'y limiter:

- Sécurité du système
- Sécurité de l'information et utilisation acceptable des systèmes
- Confidentialité
- Confidentialité des données
- Gestion des données

ROCHE fournira des résumés de ces politiques à la demande du Client.

B - Mesures techniques et organisationnelles
navify Integrator

Les contrôles, procédures et mesures suivants ont été mis en œuvre lors de la conception du module navify Integrator Lab [nI], tant au niveau du système, des opérations que des processus, afin de favoriser le traitement et le stockage sécurisés des données à caractère personnel, de réduire les risques connus en matière de cybersécurité et de faciliter le respect de obligations en matière de protection des données :

a) Contrôle d'accès (utilisateurs externes/clients).

Installations dédiées au traitement : toutes les installations dédiées au traitement des données sont protégées de tout accès non autorisé par des mesures d'authentification sécurisées.

Centres de données : les centres de données tiers sont physiquement sécurisés et surveillés de différentes façons, conformément au contrat conclu entre Roche et le tiers concerné. L'accès peut être accordé en fonction des besoins mais sera révoqué dès que ceux-ci disparaîtront.

navify Integrator ne fournit pas d'accès utilisateur au système lui-même.

b) Contrôle d'accès (utilisateurs Roche).

La solution navify Integrator applique des politiques et des contrôles garantissant l'absence de traitement non autorisé des données au sein du système. L'accès est déterminé spécifiquement en fonction du rôle de la personne concernée. Les collaboratrices et collaborateurs de Roche qui ont accès à l'infrastructure nI n'ont aucun droit d'accès aux informations chiffrées ni aux identifiants ni aux KEK et DEK permettant de déchiffrer les données. Dans les cas de support où des informations spécifiques sont nécessaires, les collaboratrices et collaborateurs formés sur les applications considérées peuvent obtenir un accès limité aux données des clients afin de répondre aux demandes de support. Cela n'arrivera que sur demande du client.

c) Contrôles et certifications.

Le module navify Integrator utilise l'Infrastructure Cloud pour déployer ces différentes composantes. Celle-ci est certifiée ISO27001 (097-ISMS-20), ISO27017 (097-ISMS-20-ST), ISO27018 (097-ISMS-20-CP) et ISO27701 (272-PMS-21).

d) Sauvegarde et récupération.

Compte tenu du caractère transitoire des données, celles-ci ne sont pas sauvegardées avant l'instance AWS S3. La récupération s'effectue en redéployant le cluster périphérique une fois l'infrastructure rétablie et en utilisant les données stockées dans les files d'attente pour permettre la récupération.

Les instances AWS S3 dédiées à la récupération des données ont été mises en place. L'option de versionnement est activée pour ces instances, ce qui permet de préserver, de récupérer et de restaurer chaque version de chaque objet.

e) Gestion des changements et des versions.

nI est conforme au système de gestion de la qualité de Roche Diagnostics, ce qui lui permet de contrôler tous les logiciels implémentés ainsi que la documentation relative à son système.

De plus, des alarmes spécifiques sont activées afin de surveiller toute modification indésirable de la configuration des

composantes AWS (alertes de changement de configuration AWS Config).

Les clients utilisateurs du module navify Integrator Lab sont informés de tous les changements ainsi que des interruptions de service qu'ils peuvent occasionner.

f) Minimisation des données.

nI n'applique pas le principe de minimisation des données mais celles-ci sont acheminées de manière sécurisée grâce au chiffrement de bout en bout et aux autres mesures de protection décrites dans les paragraphes qui précèdent.Le nI Data Hub est une composante utilisée dans le traitement des données. Les produits et services qui l'utilisent reçoivent une notification et doivent obligatoirement minimiser les données traitées, au niveau de la source. Le nI Datahub n'applique pas le principe de minimisation des données mais les conserve et les utilise de manière sécurisée grâce aux mesures de protection décrites dans les paragraphes précédents.

g) Droits des personnes concernées.

Compte tenu du caractère transitoire des données, nI les traite pour le compte des utilisateurs de données connectés (applications et services), qui doivent garantir le respect des droits des personnes concernées. En situation de déploiement normal, nI n'est pas à même d'identifier les personnes concernées par le traitement des données et ne peut donc répondre directement à leurs demandes.

Dans le cas du nI Datahub, les personnes concernées comprennent les patients, les prestataires de soins de santé et les techniciens de laboratoire. Ces personnes pourront exercer leurs droits légaux en s'adressant au responsable du traitement (le client) qui informera Roche de toute demande formulée en ce sens, en lui indiquant les dispositions à prendre.

h) Chiffrement.

nI gère le chiffrement à deux niveaux : d'abord au niveau de la charge utile (*payload*) puis au niveau des champs de données. Le chiffrement au niveau des champs dépend des capacités du service connecté en arrière-plan de nI, ainsi que du contrat conclu avec le client. Les deux types de chiffrement nécessitent des clés spécifiques. Les secrets permettant d'accéder à ces clés sont gérés dans un système de coffre-fort auquel le client bénéficie d'un accès spécifique. Seul ce dernier a accès à son espace dédié au sein du coffre-fort.

i) Correctifs, analyse et tests de l'environnement.

Le manuel Runbook nI a été créé pour documenter les outils disponibles, ainsi que les rôles et responsabilités liés à la journalisation et à la surveillance du produit, à la réponse aux incidents de cybersécurité et à la gestion des vulnérabilités.

j) Renforcement.

nI est renforcé en fonction des informations issues du modèle de menaces, comprenant les thalois et règlements, les risques techniques, les politiques de Roche et les politiques applicables au niveau mondial. Ce renforcement vise à assurer une protection contre :

- L'utilisation non autorisée d'informations personnelles
- Le défaut d'intégrité des données
- L'utilisation non autorisée de données
- La fourniture de données incorrectes

Ces risques sont traités par une conception appropriée du modèle d'intégration, le contrôle des politiques d'authentification et d'autorisation, l'acheminement sécurisé et les mesures de protection des données au repos.

nI est constamment surveillé pour détecter tout comportement anormal grâce aux instances Cloudwatch, Dome9 et Splunk.

k) Surveillance et réponse aux incidents.

Le manuel Runbook nI a été créé pour documenter les outils disponibles ainsi que les rôles et responsabilités liés à la journalisation et à la surveillance du produit, ainsi qu'à la réponse aux incidents de cybersécurité et à la gestion des vulnérabilités.

l) Validation des entrées.

nI n'a pas d'entrée manuelle à valider. La communication est basée sur la norme Roche Standard event 2.0 [...].

m) Système(s) de gestion des clés.

nI utilise un service de gestion des clés (*Key Management Service*) proposé par AWS, ainsi qu'un service de gestion des secrets (*Secret Management Service*) fourni par Roche DIA IT afin de gérer et déployer les identifiants permettant d'accéder au KMS.

La conception assure une gestion en couches de l'accès et du stockage des clés :

- Roche DIA IT (centre de données situé en Suisse) gère le contrôle d'accès aux clés ;
- AWS KMS (situé dans la zone géographique d'hébergement AWS) gère le cycle de vie des clés.

n) Localisation et hébergement.

Les composantes de nI sont hébergées dans différentes zones géographiques d'AWS afin de réduire la complexité liée aux transferts de données transfrontaliers. Actuellement nI est hébergé dans

- AWS eu-central-1 (Allemagne)
- AWS us-west-2 (Oregon)

La composante gestion des identifiants, HashiCorp Vault, est uniquement hébergée en Suisse.

o) Journalisation et surveillance.

Tous les événements nI sont journalisés dans navify Splunk Cloud, hébergés dans une zone géographique proche du client. De plus, dans certains cas, les services de surveillance suivants sont utilisés pour chaque composante AWS déployée :

- CloudTrail
- CloudWatch

- Alerte de changement de configuration AWS Config

La surveillance sécuritaire et les alertes nI sont gérées grâce à Cloudwatch, navify Dome9, Splunk.

La journalisation repose sur la plateforme Splunk hébergée dans le cloud AWS-Roche. Elle permet de conserver les données dans la zone géographique d'hébergement proche du client.

p) Sécurité réseau.

La sécurité réseau est assurée en associant :

- l'utilisation de CloudFlare et de BYOIP (voir navify Anywhere ci-dessus)
- le respect des meilleures pratiques de mise en réseau d'AWS (groupes de sécurité, points de terminaison VPC, NACL configuré selon le principe Zero Trust)
- l'utilisation du pare-feu du système informatique de laboratoire
- l'utilisation d'une liste blanche d'adresses IP (*IP Whitelisting*)

Pour DataHub, la sécurité réseau est assurée par le respect des meilleures pratiques de mise en réseau d'AWS. Celles-ci comprennent

- La séparation des sous-réseaux client,
- L'application des points de terminaison VPC,
- La surveillance et le contrôle des identités et des accès,
- La gestion des clés en conformité avec le service principal nI.

q) Profilage, y compris la prise de décisions individuelles automatisées.

nI n'effectue aucun type de profilage.

r) Périodes de conservation et suppression des données.

Les Données à caractère personnel Chiffrées sont stockées dans les files d'attente pendant sept jours au maximum, pour le débogage et la récupération.Dans le cas de Datahub, pour le déploiement initial, les données sont stockées pendant 13 mois au maximum. Pour les futurs déploiements, la période de conservation des données sera configurable et régie par les contrats client.

s) Enregistrement sécurisé des contrôles.

La configuration de la journalisation de nI et de CloudTrail peut fournir des enregistrements pour les contrôles mais un point de terminaison de système de contrôle ne sera pas configuré dans nI car le système n'est pas lui-même un dispositif médical.

t) Tests de sécurité et analyse.

La chaîne d'outils de développement de l'application est protégée par des tests de sécurité d'application statique (SAST)

exécutés à chaque *build* (SonarQube), qui analysent le code source à la recherche de vulnérabilités courantes, ainsi que par une analyse de la composition logicielle (SCA) réalisée sur les bibliothèques tierces à la recherche de vulnérabilités courantes, également exécutée à chaque *build* (OWASP Dependency Track), ainsi que par une SCA portant sur les images de conteneurs afin de détecter les vulnérabilités dans les images fournies.
Des tests de pénétration sont régulièrement réalisés sur différents périmètres, notamment en fonction des scénarios d'utilisation de nI, des composants de nI et du nI Datahub.

u) Gestion des risques liés au tiers.

nI peut s'appuyer sur des tiers pour des composantes spécifiques ou pour le traitement des données. Tous ces tiers doivent se soumettre à des évaluations de sécurité des fournisseurs. Roche peut avoir conclu des contrats spécifiques ayant trait au traitement des données avec des prestataires susceptibles d'être en contact avec des données sensibles des clients.

v) Transparence.

Non pertinent : nI n'interagit qu'avec les systèmes sans intervenir dans les activités des utilisateurs. Le texte relevant de la conformité à la réglementation ne concerne en l'occurrence aucun public.

z) Intégrité.

Les charges utiles des événements sont signées afin qu'il puisse être prouvé que les événements reçus par les applications sont identiques à ceux générés par les sources de données.

<Fin du Document>