VERSION AOUT 2025

NAVIFY LAB OPERATIONS

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) Application. 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

(2) Parties. Dans cet Accord, le CLIENT est le Responsable de Traitement et ROCHE (incluant ses filiales) le Sous-Traitant

(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.

(3) Catégories de Personnes Concernées. Les catégories de Personnes Concernées sont les suivantes :

a. Salariés du Client.
b. Les Professionnels de santé,
c. Les Patients.

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

- **navify Instrument Maintenance**
  - S'agissant des catégories de personnes concernées, les salariés du Client, ROCHE traite les données suivantes : Nom d'utilisateur (adresse électronique), prénom, nom de famille, localisation, langue.
- **navify Quality Control:**
  - S'agissant des catégories de personnes concernées, les salariés du Client, ROCHE traite les données suivantes : nom d'utilisateur, e-mail, nom, prénom, lieu, langue.
- **SST**
  ***REMARQUE** ! Les catégories de données téléchargées dépendent de la configuration spécifique au client, en dessous de la configuration standard pour la TSS affichée.*

  - S'agissant des catégories de personnes concernées, les salariés du Client, ROCHE traite les données suivantes :
    - Coordonnées et identifiants (p. ex. nom d'utilisateur, prénom, nom)
    - Informations déduites et dérivées (p. ex. statut activé/désactivé, horodatages des modifications, champs de commentaire, ID de langue, etc.)

  - S'agissant des catégories de personnes concernées, Professionnel de santé, ROCHE traite les données suivantes :
    - Coordonnées et identifiants (p. ex. nom d'utilisateur, prénom, nom)
    - Informations déduites et dérivées (p. ex. statut activé/désactivé, horodatages des modifications, champs de commentaire, ID de langue, etc.)

  - S'agissant des catégories de personnes concernées, les salariés du Client, ROCHE traite les données suivantes :
    - Coordonnées et identifiants (p. ex. prénom, nom)
    - Données démographiques (sexe, date de naissance, âge, origine ethnique)
    - Données de santé (ID du test, date de prélèvement de l'échantillon)
    - Informations déduites et dérivées (p. ex. statut activé/désactivé, horodatages des modifications, champs de commentaire, ID de langue, etc.)

- **navify Lab Ops, navify Instrument Maintenance, navify Quality Control - Modèle de télémaintenance avec ThingWorx**
  - Les données personnelles traitées par ROCHE sont limitées dans la mesure où elles ont été divulguées activement par le Client à ROCHE dans le cadre de l'assistance technique. Les dispositions ci-dessous peuvent s'appliquer :
    - En ce qui concerne les catégories de données concernées, les données personnelles de l'employé du Client ci-dessous peuvent être traitées par ROCHE: données de contact professionnel, données liées à l'assistance, telles que les identifiants de connexion au système (pas de mots de passe)
    - En ce qui concerne les catégories de personnes concernées Professionnels de santé: coordonnées professionnelles
    - En ce qui concerne les catégories de personnes concernées, les données patient ci-dessous peuvent être traitées : Données de santé (ID de commande, sexe, données de naissance/âge, résultats des tests, ID du patient, ID de l'échantillon).

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

(1) 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.

Sous-traitant ultérieur de ROCHE	Prestations
Responsable de traitement	
Roche Diagnostics France	Local Roche entity holding the contract with the customer and providing first level support.
Sous traitants	
Affiliées membres du Groupe Roche et autres entités ROCHE Diagnostics International AG, Suisse ROCHE Diagnostics Corporation for North America customers, Etats-Unis ROCHE Diagnostics Uruguay and ROCHE Diagnostics Brasil pour les clients LATAM ROCHE Diagnostics Limited, UK and ROCHE Diagnostics S.L., Espagne pour les clients EMEA	Prestation des services telle que décrite dans le formulaire de commande, principalement le service d'assistance pour l'outil de simulation du système infinity. Pour le modèle d'assistance pour l'outil de simulation de système infinity, les filiales de Roche aux États-Unis, en Uruguay, au Brésil, au Royaume-Uni, en Espagne et dans la région Asie-Pacifique sont les principaux contacts d'assistance dans les régions respectives et transfèrent la demande d'assistance à Roche Diagnostics International AG ou Roche Information Solutions India Pvt Ltd, si nécessaire. 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.

ROCHE Diagnostics Asia Pacific, Singapore pour les clients APAC	
AWS	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
Okta	agissant en tant que sous-traitant de Roche et en tant que fournisseur de contrôle d'accès aux services dans la région respective, où la solution est déployée.
Smarteeva Software Inc., 7W Figueroa Street, Santa Barbara, CA 93101, Etats Unis	Smarteeva agit en tant que sous-traitant de Roche Diagnostics International AG pour la fourniture de l'assistance et des demandes de réclamations via son système de tickets.

<u>Sous-traitants si utilisation associée à navify Quality Control et navify Instrument Maintenance</u> :

Sous traitant ROCHE	Prestations
Affiliées membres du Groupe Roche et autres entités Roche Diagnostics International AG, Rotkreuz, Suisse, Roche Diagnostics SL. à San Cugat, Espagne	agissant en tant que sous-traitant des données de la filiale de Roche, qui a un contrat avec le Client. Le rôle des filiales de Roche est de fournir les services d'assistance et de maintenance (assistance de 2e ou 3 e niveau). Toute activité de traitement des données repose sur l'accord de transfert de données intersociétés (RIDTA) du groupe Roche. Fourniture/prestation de services, principalement le service d'assistance pour la solution navify Instrument Maintenance, développé et maintenu par L'équipe RIS infinity de Roche. Pour le modèle d'assistance pour la maintenance des instruments navify, la filiale Roche locale est le principal contact d'assistance qui transfère la demande d'assistance à l'équipe GCS locale qui peut contacter Roche Diagnostics International AG et/ou Roche Diagnostics S.L. représentant l'équipe de développement. Toute activité de traitement des données repose sur l'accord de transfert de données intersociétés (RIDTA) du groupe Roche.
Roche Molecular Systems, Inc. 4300 Hacienda Drive, Pleasanton CA 94588 (États-Unis)	RMS, fournisseur interne de plateformes en tant que service (PaaS) au sein de Roche, fournit la plateforme navify. Celle-ci peut accéder aux données en cas de support ou d'incident. Cet accès est conforme aux obligations de Roche en matière de sécurité, de support et de gestion des réclamations. Toute activité de traitement de données s'inscrit dans le cadre de l'accord intragroupe relatif aux transferts de données du Groupe Roche (RITDA).
AWS	AWS offre en matière d'hébergement et de sécurité des prestations visant à assurer

	la sécurité des services. Toutes les Données sont exclusivement hébergées sur : - l'instance AWS de Francfort (Allemagne) pour les clients situés dans l'Union européenne, - l'instance AWS de Paris (France) pour les clients situés dans l'Union européenne, - l'instance AWS de Londres (Royaume-Uni) pour les clients situés au Royaume-Uni, - l'instance AWS de Virginie du Nord (États-Unis) pour les clients situés aux États-Unis. Les clients situés dans d'autres zones géographiques peuvent choisir entre les serveurs respectivement situés à Francfort, à Londres et en Virginie du Nord. Roche a signé avec la société AWS, Inc les Clauses contractuelles types (version du 4 juin 2021).
Cloudflare	Cloudflare, qui intervient en tant que sous-traitant ultérieur de Roche, assure la protection de l'accès au réseau dans la zone géographique où la solution est déployée

Lorsque le modèle d'assistance à distance est en place :

Roche Information Solutions India Pvt Ltd à Pune, Inde	agissant en tant que sous-traitant des données de la filiale de Roche, qui a un contrat avec le Client. Le rôle des filiales de Roche est de fournir les services d'assistance et de maintenance (assistance de 2e ou 3 e niveau). Toute activité de traitement des données repose sur l'accord de transfert de données intersociétés (RIDTA) du groupe Roche.
Okta	agissant en tant que sous-traitant de Roche et en tant que fournisseur de contrôle d'accès aux services dans la région respective, où la solution est déployée.
Salesforce	agissant en tant que sous-traitant de Roche et en tant que fournisseur des services de gestion de la relation client (CRM) dans la région respective, où la solution est déployée. Salesforce sert de solution de billetterie.
Splunk	agissant en tant que sous-traitant de Roche et en tant que fournisseur des services de journalisation dans la région respective, où la solution est déployée.
PTC Schweiz AG (applicable uniquement si l'agent logiciel - Remote Service Edge Agent - est déployé chez le client.	Fourniture des services d'hébergement de la plateforme ThingWorx, qui permet à Roche de fournir un accès d'assistance à distance (entre autres, des sessions de partage d'écran et le transport de données). Hébergement de ThingWorx - Microsoft Azure Amsterdam, Pays-Bas. Les sociétés affiliées à PTC sont impliquées dans le support technique et les services de conseil concernant la plateforme ThingWorx (selon la région).

RECTIFICATION, LIMITATION ET EFFACEMENT DES DONNÉES À CARACTÈRE PERSONNEL

(1) ROCHE ne pourra de sa propre initiative rectifier les Données traitées pour le compte du client, les effacer ni en limiter le traitement. Elle ne peut le faire que sur instructions documentées de ce dernier. Dans la mesure où une Personne Concernée prendrait directement contact avec ROCHE aux fins de la rectification ou de l'effacement de Données ou afin d'en limiter le traitement, ROCHE devrait transmettrait cette demande au CLIENT dans les meilleurs délais.

(2) Dans la mesure où ces éléments s'inscriront dans le périmètre des prestations, ROCHE sera chargée de la politique en matière d'effacement, ainsi que du respect du « droit à l'oubli », à la rectification des données, à leur portabilité et du droit d'y accéder, dans le respect des instructions documentées du CLIENT et dans les meilleurs délais.

(3) Le CLIENT est informé du fait que ROCHE ne pourra, de sa propre initiative, assurer la portabilité des données, les rectifier, les effacer ni en limiter le traitement, en raison de leur chiffrement intégral et de la maîtrise exclusive par le CLIENT des clés de chiffrement. Ce dernier devra donc aider ROCHE à satisfaire toute demande de cet ordre et soit indemniser ROCHE de ses efforts soit assumer elle-même les obligations susvisées afin de les remplir directement par le biais de l'interface locale non chiffrée du CLIENT.

5 GARANTIE QUALITÉ ET AUTRES OBLIGATIONS DE ROCHE

(1) Outre le respect des règles définies dans le cadre de l'Accord relatif au traitement des données applicable, ROCHE devra respecter les exigences définies aux Articles 28 à 33 du RGPD. Elle devra par conséquent respecter, en particulier, les exigences suivantes :

a) La confidentialité devra être assurée, conformément à l'Article 28, Section 3, deuxième phrase, point b, ainsi qu'à l'Article 29 et à l'Article 32, Section 4 du RGPD. ROCHE ne confie le traitement des données dont il est question dans chaque Accord relatif au traitement des données qu'à ses salariés soumis à une obligation de confidentialité ou ayant souscrit un engagement en la matière et ayant préalablement acquis une bonne connaissance des règles de protection des données concernant leur emploi. Sauf exigence légale contraire, ROCHE et toute personne agissant sous son autorité et ayant accès aux Données ne devront les traiter que sur instructions du CLIENT, étant entendu que les pouvoirs conférés aux termes du présent Accord satisfont cette condition.

b) L'ensemble des Mesures techniques et organisationnelles nécessaires dans le cadre de chaque Accord relatif au traitement des données, en vertu de l'Article 28, Section 3, deuxième phrase, point c et l'Article 32 du RGPD, et visées à l'Article 3 du présent Accord, devront être effectivement mises en œuvre.

c) ROCHE et le CLIENT devront coopérer, sur demande, avec l'autorité de contrôle lors de l'accomplissement de leurs tâches respectives.

d) Le CLIENT devra être informé immédiatement de toutes inspections menées par l'autorité de contrôle et de toutes mesures prises par celle-ci, dans la mesure où elles auront un lien avec un Accord relatif au traitement des données. Il en serait de même dans le cas où ROCHE serait soumise ou partie prenante à une enquête menée par une autorité compétente sur des infractions à une loi civile ou pénale, à une règle administrative ou à un règlement ayant trait au traitement des Données, commises en lien avec un Accord relatif au traitement des données.

e) Dans la mesure où le CLIENT ferait l'objet d'une inspection menée par l'autorité de contrôle, d'une procédure administrative ou pour infraction mineure ou pénale, ou verrait engager sa responsabilité par une Personne Concernée ou par un tiers, ou formuler à son encontre une autre prétention en lien avec un Accord relatif au traitement des données, ROCHE devrait faire tout son possible pour lui apporter son soutien.

f) ROCHE devra périodiquement contrôler les processus internes et les Mesures techniques et organisationnelles afin de garantir la conformité du traitement relevant de sa responsabilité aux exigences des textes de droit ayant trait à la protection des données, ainsi que la protection des droits des personnes concernées.

g) Le CLIENT devra avoir la possibilité vérifier les Mesures techniques et organisationnelles mises en œuvre, au titre de ses pouvoirs de surveillance visés à l'Article 7 du présent Accord.

6. SOUS-TRAITANCE ULTERIEURE

(1) Dans le cadre du présent Accord, l'expression « sous-traitance ultérieure » fait référence à des services ayant un lien direct avec la fourniture du service principal. Ceux-ci ne comprennent pas les services accessoires tels que les services de télécommunication, les services postaux et de transport, de maintenance et d'assistance à l'utilisateur, les services d'élimination des supports de données, ni les autres services destinés à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels dont les équipements de traitement des données sont dotés. ROCHE devra cependant conclure des accords appropriés, juridiquement contraignants, et prendre des mesures d'inspection adéquates visant à garantir la protection des données et la sécurité des données du CLIENT, même en cas d'externalisation de services accessoires.

(2) ROCHE pourra avoir recours à des sous-traitants ultérieurs (d'autres sous-traitants chargés du traitement) expressément agréés par le CLIENT. Celui-ci consent à ce qu'il soit fait appel aux sous-traitants dont la liste figure dans l'Accord relatif au traitement des données applicables, à condition qu'un contrat soit conclu dans le respect de l'Article 28, sections 2 à 4 du RGPD :

(3) Le recours à des sous-traitants ultérieurs ou un changement parmi les sous-traitants ultérieurs existants est autorisé lorsque :
- ROCHE soumet cette externalisation au CLIENT par écrit ou sous forme de texte en observant un préavis approprié ; et
- Le CLIENT ne s'oppose pas par écrit ou sous forme de texte à l'externalisation projetée, dans un délai de deux semaines suivant la communication visée au paragraphe ci-dessus ; et
- La sous-traitance ultérieure est fondée sur un contrat, dans le respect de l'Article 28, sections 2 à 4 du RGPD.

(4) Le transfert de Données du CLIENT au sous-traitant ultérieur et le début de leur traitement par ce dernier sont subordonnés au respect préalable de toutes les exigences.

(5) Si le sous-traitant ultérieur fournit le service convenu en dehors de l'Union européenne et de l'Espace économique européen, ROCHE devra garantir le respect de la Réglementation relative à la protection des données en vigueur dans l'Union européenne en prenant des mesures appropriées. Il en sera de même s'il est prévu d'avoir recours à des prestataires de services au sens de la deuxième phrase de la Section 1) ci-dessus.

(6) Toute externalisation par un sous-traitant ultérieur est subordonnée à l'accord exprès de ROCHE (qui devra le communiquer au minimum sous forme de texte).

(7) L'ensemble des stipulations arrêtées au long de la chaîne de contrats devront être communiquées à chaque sous-traitant ultérieur supplémentaire et faire l'objet d'un accord avec celui-ci.

7. POUVOIR DE SUPERVISION DU CLIENT

(1) Le CLIENT est en droit, après consultation de ROCHE, de procéder à des inspections ou de les confier à un contrôleur désigné au cas par cas. Il est en droit de s'assurer lui-même du respect par ROCHE, dans le cadre de ses opérations, d'un Accord relatif au traitement des données, aux moyens de contrôles aléatoires devant être ordinairement annoncés raisonnablement à l'avance .

(2) ROCHE s'engage à communiquer au CLIENT, sur demande, les informations nécessaires et, en particulier, à démontrer la mise en œuvre des Mesures techniques et organisationnelles.

(3) La preuve de la mise en œuvre de ces mesures pourra être apportée

- En prouvant le respect des codes de conduite visés à l'Article 40 du RGPD ; et/ou

- Par une certification conforme à une procédure approuvée s'inscrivant dans le cadre de l'Article 42 du RGPD ; et/ou

- Par des certificats de contrôleurs actuels, des rapports ou des extraits de rapports fournis par des personnes ou organismes indépendants (par exemple, un contrôleur, un délégué à la protection des données, un département en charge de la sécurité informatique, un contrôleur de la protection des données, un contrôleur qualité) ; et/ou

- Par une certification adéquate faisant suite à un contrôle portant sur la sécurité informatique ou la protection des données ;

(4) Étant précisé que ROCHE pourra demander une rémunération en contrepartie de la possibilité qu'elle donnera au CLIENT de procéder à des inspections sans motif particulier.

8. COMMUNICATION EN CAS D'INFRACTIONS COMMISES PAR ROCHE

(1) ROCHE devra aider raisonnablement le CLIENT à remplir les obligations ayant trait à la sécurité des Données, au signalement des violations de données, aux analyses d'impact relatives à la protection des données et aux consultations préalables, dont il est question aux Articles 32 à 36 du RGPD. Cette obligation comprend :

a. L'obligation de garantir un niveau approprié de protection des données grâce à des Mesures techniques et organisationnelles déterminées en fonction des circonstances, des finalités du traitement, ainsi que de la probabilité et de la gravité prévues d'une infraction à la loi susceptible de résulter de certains facteurs de vulnérabilité en matière de sécurité. Ces mesures devront permettre une détection immédiate des cas de violation et des infractions.

b. L'obligation de porter une violation de Données à la connaissance du CLIENT dans les meilleurs délais.

c. L'obligation d'aider le CLIENT à remplir celle qui lui incombe de communiquer des informations à la Personne Concernée ; et de fournir immédiatement au CLIENT toutes informations utiles à cet égard.

d. L'obligation d'aider le CLIENT à réaliser son analyse d'impact relative à la protection des données.

e. L'obligation d'aider le CLIENT à procéder à la consultation préalable de l'autorité de contrôle.

(2) ROCHE pourra réclamer une rémunération relative aux services d'assistance non compris dans le descriptif des services et qui n'auront pas à être fournis en raison de défaillance de la part de ROCHE.

9. POUVOIR DU CLIENT DANS L'ÉMISSION D'INSTRUCTIONS

(1) Le CLIENT devra immédiatement confirmer ses instructions verbales (au minimum sous forme de texte).

(2) ROCHE devra immédiatement informer le CLIENT si elle considère qu'une instruction est contraire à la réglementation relative à la protection des données. Elle sera en droit de suspendre l'exécution de l'instruction en question jusqu'à ce que le CLIENT la confirme ou la modifie.

(3) Le CLIENT devra obtenir l'ensemble des consentements et autorisations des Personnes Concernées qui pourraient être nécessaires ou obligatoires en vertu des textes de droit applicables s'agissant des Données devant être traitées par ROCHE et ses sous-traitants ultérieurs dans le cadre du Contrat et au titre de toute Commande.

10. SUPPRESSION ET RETOUR DE DONNÉES

(1) Aucune copie de Données ne saurait être produite sans que le CLIENT en ait connaissance, à l'exception des copies de sauvegarde qui seraient nécessaires pour en garantir un traitement en bon ordre, ainsi que des Données devant être conservées en vertu d'une exigence réglementaire. Le CLIENT reconnaît qu'en raison du chiffrement des Données, en raison duquel ces dernières ne sont pas divulguées à ROCHE, celle-ci ne sera pas en mesure de sauvegarder ni de restaurer des ensembles de données déterminés mais uniquement la base de données dans son intégralité (par exemple, sous forme d'instantané). C'est au CLIENT qu'il incombe de traiter les Données de manière individualisée.

(2) Après l'achèvement des prestations définies dans le cadre d'une Commande, ou plus tôt sur demande du CLIENT, et au plus tard au moment où la Commande en question aura été entièrement honorée, ROCHE devra anonymiser ou détruire tous les documents, les résultats d'un traitement et d'une utilisation, ainsi que les ensembles de données liés au contrat, dont elle aura été en possession, dans le respect des règles relatives à la protection des données. Il en sera de même de tous éléments ayant servi à des tests, tous déchets et tous éléments redondants et mis au rebut. L'enregistrement de la destruction, de l'anonymisation ou de la suppression réalisée devra être fourni sur demande.

(3) Les documents utilisés pour démontrer un traitement de données en bon ordre, conforme à l'Accord relatif au traitement des données applicable, devront être conservés par ROCHE après qu'une Commande aura été honorée, en se référant à la durée de conservation obligatoire. ROCHE pourra remettre ces documents au CLIENT au terme de la durée du contrat afin de se libérer de cette obligation contractuelle.

11. RESPONSABILITÉ

(1) Le CLIENT ne saurait formuler à l'encontre de ROCHE plus d'une demande relative au même dommage ; sans qu'il importe de savoir si une telle demande résulte d'une Commande ou du Contrat, ni si un paiement a été effectué en lien avec un dommage particulier dans le cadre d'un Accord relatif au traitement des données. Si une demande a été formulée et suivie d'un paiement, le montant de toute autre demande concernant le même dommage sera réduit de celui du paiement d'ores et déjà effectué.

A - Mesures Techniques et Organisationnelles
navify Instrument Maintenance

a) Contrôle d'accès (utilisateurs externes/clients). En termes d'authentification et d'autorisation, les utilisateurs qui interagissent avec navify Instrument Maintenance doivent s'authentifier par le biais de la Plateforme Navify (IdP). La fonctionnalité d'authentification unique (*single sign-on*) de navify Lab Ops utilisée par navify Instrument Maintenance dans le contexte de navify Lab Ops, est gérée par la Plateforme Navify (IdP).

b) Contrôle d'accès (utilisateurs Roche). Pour les opérations *backend* et les activités de maintenance, les utilisateurs de Roche utiliseront Navify Okta comme point d'entrée pour accéder aux différentes unités.

c) Contrôles et certifications. Navify Instrument Maintenance utilise l'infrastructure Navify Cloud pour déployer son application. Cette Infrastructure est certifiée ISO 27000, ISO 27017, ISO 27018 et ISO 27701.

d) Sauvegarde et récupération. La solution navify Instrument Maintenance bénéficie des fonctionnalités de sauvegarde et de récupération de la plateforme navify.

e) Gestion des changements et des versions. Pour des informations sur la gestion des changements et le versionnement, veuillez vous référer au Plan de gestion des configurations et au Manuel du projet.

f) Minimisation des données. Seules les données à caractère personnel des salariés jugées nécessaires pour faciliter l'utilisation du produit sont collectées auprès des salariés du Client qui utilisent l'application.

g) Droits des personnes concernées. La solution nIM est déployée par Roche pour le compte du responsable du traitement (le Client). Les droits des personnes concernées sont respectés, conformément à la législation ou à la réglementation locale et au contrat. Dans le respect de l'Accord relatif au traitement des données, Roche informera le responsable du traitement des demandes qu'elle recevra des personnes concernées. En outre, le responsable du traitement pourra effectuer lui-même un suivi de l'ensemble des demandes émanant de ces dernières et Roche pourra l'aider si des questions sont posées, conformément à l'Accord relatif au traitement des données. Le responsable du traitement pourra transmettre une éventuelle demande d'effacement de données à la solution nIM de Roche, qui réalisera cet effacement dans le respect de l'Accord relatif au traitement des données.

h) Chiffrement. Le chiffrement des données en transit est réalisé selon le protocole https et en utilisant la version 1.2 ou une version plus récente du protocole de sécurité TLS au sein des connecteurs concernés.

i) Correctifs, analyse et tests de l'environnement. L'analyse de la solution est effectuée à différents niveaux :

- Au cours du développement :
- Analyse de sécurité des dépendances tierces avec MEND.
- Analyse statique du code de sécurité avec SonarQube.
- Analyse des artefacts (par exemple, images Docker) avec le registre Docker Harbor.
- Au cours de l'exécution :
- Les images de machines virtuelles de l'infrastructure cloud navify et l'ensemble de l'infrastructure sont surveillés en permanence à l'aide de Tenable et Dome9.

Les correctifs et, plus généralement, le déploiement et la mise à jour de l'application nIM sont gérés à l'aide des flux de travail GitOps.

j) Renforcement. Le renforcement est réalisé au niveau des images Docker en limitant certaines capacités, conformément aux meilleures pratiques définies dans la fiche de sécurité Docker d'OWASP. En outre, les groupes de sécurité d'AWS sont utilisés pour n'ouvrir que les ports nécessaires. Cette mesure s'applique également aux composants en périphérie, pour lesquels le pare-feu Linux de Roche sert à limiter les ports autorisés. Par ailleurs, les images utilisées dans l'infrastructure Cloud navify sont des images spécialement adaptées et renforcées. Le renforcement repose également sur des services tels que :

- Hardened AMI : il s'agit d'images obligatoires utilisées pour gérer toute charge de calcul telle que les instances EC2, ECS ou EKS. Plusieurs versions de système d'exploitation sont disponibles, auxquelles sont intégrés les agents de sécurité nécessaires.
- Dome9 vous aide à évaluer votre posture de sécurité par référence à un référentiel conformité ou à certaines exigences, principalement en lien avec l'ensemble de règles spécialement définies pour l'Infrastructure Cloud de la Plateforme navify, lesquelles doivent être respectées pour demander votre compte suivant (STAGE/QA ou PROD).
- Splunk – Il s'agit de nos outils d'agrégation de journaux, accompagnés de tableaux de bord prédéfinis, qui vous aident notamment à identifier les cas dans lesquels l'utilisation de votre compte est risquée.
- SysDig Monitor and Secure – Il s'agit d'un outil utilisé pour les produits basés sur Docker.
- Cloudflare – Obligatoire pour tout point de terminaison exposé.

k) Surveillance des incidents et réponse. Voir le concept de service [7], section Modèle d'assistance pour plus de détails. Des informations détaillées sur les activités de surveillance et de journalisation du point de vue de l'infrastructure se trouvent dans le manuel GCS Cloud Support Runbook et le manuel Runbook RSE/SRO (*Site Reliability Engineer*, Ingénieur en Fiabilité de Site/*Site Reliability Operations*, Opérations de Fiabilité de Site). Un plan de maintenance logicielle sera fourni pour l'Étape DO.

l) Validation des entrées. Toutes les API utilisées dans nIM sont conçues en s'appuyant sur des *frameworks* tels que Spring, qui valident automatiquement les paramètres d'entrée afin de prévenir les attaques XSS et les injections SQL, en excluant les valeurs non conformes.

m) Système(s) de gestion des clés. Les secrets sont gérés au moyen de Hashicorp Vault. Ils sont injectés dans les pods Kubernetes correspondants, ce qui garantit qu'aucun secret n'est conservé en texte brut dans une quelconque partie du système.

n) Localisation et hébergement. Le service est déployé et hébergé chez le fournisseur de cloud AWS et sa localisation correspond à la zone géographique du client.

o) Journalisation et surveillance. La journalisation et la surveillance reposent sur des outils de la plateforme tels que Splunk et Grafana. L'application Navify Instrument Maintenance fournit des indicateurs au format standard Prometheus, qui peuvent être utilisés pour détecter des schémas d'accès et d'utilisation inhabituels.

p) Sécurité des réseaux. Les réseaux de l'environnement Cloud sont isolés. Le réseau de données et les réseaux d'applications sont clairement séparés. De plus, un WAF (pare-feu d'applications web) basé sur Cloudflare est utilisé pour prévenir les attaques par déni de service distribué (DDoS) et d'autres types d'attaques sur les API exposées.

q) Profilage, y compris la prise de décisions individuelles automatisées. navify Instrument Maintenance n'est pas concerné.

r) Périodes de conservation et suppression des données. Les données seront conservées jusqu'à la fin du contrat du client et ne seront accessibles qu'aux Affiliées de Roche et à Roche Global, conformément à ce contrat.

s) Enregistrement sécurisé des contrôles. Il s'agit de l'une des finalités de l'application. Chaque action effectuée est enregistrée et peut être exportée sous forme de rapports portant sur la maintenance des instruments.

t) Tests de sécurité et analyse. Toutes les données sensibles de l'application sont stockées dans HashiCorp Vault, qui garantit leur sécurité et leur protection contre les acteurs malveillants. Le binaire du service est conforme aux meilleures pratiques de sécurité Docker définies dans la fiche Docker Security Cheat Sheet de l'OWASP en matière d'analyse. La surface d'exposition du service aux failles et vulnérabilités est ainsi réduite.

u) Gestion des risques liés au tiers.La Plateforme Navify sert à gérer les informations d'identification des utilisateurs. Elle utilise en arrière-plan le système OKTA de gestion des identités et des accès. Pour de plus amples informations, veuillez consulter le document DPIA de ce prestataire. Cloudflare est utilisé comme pare-feu d'application web. Nous utilisons

aussi la Data Localization Suite (Suite de Localisation des Données), également fournie par Cloudflare. Celle-ci permet à l'application nIM de définir le périmètre des données afin qu'aucune d'entre elles ne franchisse des frontières imprévues et que leur protection reste cantonnée à des régions connues.

v) Transparence. Les personnes concernées doivent être informées des activités de traitement des données par le responsable du traitement.

B- Mesures techniques et organisationnelles

Navify Quality Control

(a) Contrôle d'accès (utilisateurs externes/clients).
En termes d'authentification et d'autorisation, les utilisateurs interagissant avec navify Quality Control doivent s'authentifier via la plateforme Navify (IdP). La fonction d'authentification unique de navify Lab Ops et utilisée par navify Quality Control au sein de cobas
Le contexte du laboratoire central Infinity est géré par la plateforme Navify (IdP).

(b) Contrôle d'accès (utilisateurs Roche).
Pour les activités liées à l'infrastructure dorsale des opérations et à la maintenance, les utilisateurs de Roche utiliseront Navify Okta comme point d'entrée pour accéder aux différentes unités.

(c) Audits et certifications.
Le contrôle qualité de navify utilise l'infrastructure cloud de navify pour déployer son application. Navify Cloud Infrastructure est certifiée ISO 27000, ISO 27017, ISO 27018 et ISO 27701.

(d) Sauvegarde et Récupération.
La solution navify Quality Control s'appuie sur les fonctionnalités de sauvegarde et de récupération fournies par la navify Platform.

(e) Gestion des modifications et du versionnage.
Pour plus d'informations sur la gestion des modifications et le contrôle des versions, reportez-vous au plan de gestion des configurations et le Manuel du projet

(f) Minimisation des données.
Seules les données personnelles des employés jugées nécessaires pour faciliter l'utilisation du produit sont collectées auprès des employés du clients, qui sont les utilisateurs de l'application.

(g) Droits des personnes concernées.
Le responsable du traitement des données est responsable de la gestion des droits des personnes concernées. La solution nQC de Roche est déployée par Roche pour le compte du contrôleur des données (client). Roche nQC assistera le contrôleur des données et exécutera ses demandes.

(h) Cryptage.
Le cryptage en transit est fourni par le biais de https avec une version TLS >= 1.2 dans les connecteurs applicables.

(i) Correction, analyse et tests de l'environnement.
La numérisation de la solution est effectuée à différents niveaux :
- Temps de développement :

- Analyse de sécurité des dépendances tierces avec MEND.
- Analyse statique des codes de sécurité avec SonarQube.
- Artefacts (p. ex. images de docker) scannant avec le registre Harbor docker.
- Temps d'exécution :
- L'infrastructure cloud de navify, les images des machines virtuelles et l'infrastructure globale de l'environnement sont surveillées en permanence à l'aide de Tenable et Dome9.

Les correctifs et, en général, le déploiement/la mise à jour de l'application nQC sont gérés à l'aide des flux de travail GitOps.

j) Renforcement de la sécurité.
Le renforcement se produit au niveau de l'image du Docker en limitant certaines capacités telles que définies dans les meilleures pratiques de la fiche de sécurité Docker OWASP. De même, les groupes de sécurité AWS sont utilisés pour ouvrir uniquement les ports requis. Cela s'applique également à la tranche composants exploitant le pare-feu de Roche Linux pour limiter les ports autorisés. En outre, les images utilisées dans navify Cloud Infrastructure sont des images renforcées personnalisées de navify et des services supplémentaires tels que :
● IAM renforcé : il s'agit d'images obligatoires à utiliser pour fournir une charge informatique telle que instances EC2, ECS ou EKS. Plusieurs saveurs de SG sont disponibles, ainsi que les des agents de sécurité intégrés.
● Dome9 - vous aide à évaluer votre posture de sécurité par rapport au cadre de conformité ou exigences, principalement par rapport à un ensemble de règles personnalisées navify Platform Cloud Infrastructure qui est requis pour réussir à passer afin de demander votre compte suivant (STAGE/QA ou PROD).
● Splunk - Nos outils d'agrégation de journaux fournis avec des tableaux de bord prédéfinis pour vous aider à identifier lorsque vous utilisez votre compte à risque et plus encore.
● SysDig Monitor and Secure - Au cas où vos produits seraient basés sur des dockers.
● Cloudflare – Obligatoire pour tout critère d'évaluation exposé.

k) Surveillance et gestion des incidents.
Des informations détaillées sur les activités de surveillance et de journalisation du point de vue de l'infrastructure sont disponibles dans le Runbook de l'assistance Cloud de GCS et le Runbook SRE/SRO (Site Reliability Engineer/Site Reliability Operations). Pour l'OD d'étape, un plan de maintenance du logiciel sera fourni.

(l) Validation des entrées.
Toutes les API utilisées dans le nQC sont conçues en s'appuyant sur des cadres comme Spring qui effectuent déjà la validation des entrées de paramètres pour éviter l'injection XSS et SQL en échappant aux valeurs non attendues.

(m) Systèmes de gestion des clés.
Les secrets sont gérés à partir de Hashicorp Vault. Ces secrets sont injectés dans les Kubernetes Pods correspondants, ce qui garantit qu'aucun secret n'est conservé dans le texte du plan dans aucune partie du système.

(n) Mise en place et Hébergement.
Le service est déployé et hébergé dans le fournisseur de cloud AWS et son emplacement est la région du client.

(o) Journalisation et surveillance.
La journalisation et la surveillance sont fournies en tirant parti des capacités de la plateforme comme Splunk et Grafana. L'application navify Quality Control expose les indicateurs de la norme Prometheus qui peuvent être utilisés pour détecter les modèles d'accès et d'utilisation inhabituels de la solution.

(p) Sécurité du réseau.
Les réseaux d'environnement cloud sont isolés, avec une séparation claire entre le réseau de données et les réseaux d'applications. De plus, le WAF (Web Application Firewall) basé sur Cloudflare est utilisé pour prévenir les DDoS et d'autres types d'attaques contre les API exposées.

(q) Profilage, y compris la prise de décision individuelle automatisée.
Non applicable à navify Quality Control.

(r) Périodes de conservation et destruction des données.
Les données seront conservées jusqu'à la fin du contrat du client et ne seront accessibles qu'aux filiales de Roche et à Roche Global en vertu d'un accord client.

(s) Enregistrement sécurisé des audits.
En raison de la nature de l'application, ses enregistrements d'audit sont collectés du côté Infinity. Chaque changement d'état se produit dans Infinity et le nQC n'est qu'un miroir de leur état/contraintes.

(t) Tests et analyses de sécurité.
Toutes les données sensibles de l'application sont stockées dans le coffre de Hashicorp, elles sont donc sécurisées et protégées contre les acteurs malveillants.
Le fichier binaire du service suit les meilleures pratiques de l'OWASP Docker Security Cheat Sheet pour la numérisation, réduisant ainsi la surface de faiblesse et de vulnérabilité du service.

(u) Gestion des risques liés aux tiers.
Plateforme Navify pour la gestion des identifiants des utilisateurs. En coulisses, ils utilisent OKTA comme fournisseur d'accès/d'identité pour la gestion des identités. Pour de plus amples informations, veuillez consulter leur document DPIA ici. Cloudflare en tant que pare-feu de notre application Web et l'utilisation de la suite de localisation des données, fournies par le même Cloudflare. La suite de localisation des données permet à l'application nQC de définir la portée des données, de ne pas traverser de frontière inattendue et de préserver la confidentialité des données dans les régions connues.

(v) Transparence.
Les informations aux personnes concernées concernant les activités de traitement des données doivent être fournies par l'intermédiaire du responsable du traitement des données.

C- Mesures Techniques et Organisationnelles System Simulation Tool

Les contrôles, procédures et mesures du système, opérationnels et procéduraux suivants ont été mis en œuvre au sein des composants du System Simulation Tool component (SST), dès la conception, afin de promouvoir le traitement et le stockage sécurisés des données personnelles, d'atténuer le ou les risques de cybersécurité connus et de faciliter le respect des obligations pertinentes en matière de protection des données.

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

En termes d'authentification et d'autorisation, les utilisateurs ou les systèmes interagissant avec le SST doivent s'authentifier via le navify Access Control. Tous les utilisateurs qui ont accès à l'outil ont les mêmes droits et niveaux d'accès aux données du TSS.

Toutes les API du SST sont protégées au moyen de jetons d'accès qui peuvent être obtenus auprès de navify Access Control pour les acteurs humains et/ou de service.

(b) Contrôle d'accès (utilisateurs Roche).

Les utilisateurs de Roche accéderont au SST via le navify Access Control qui offre un accès sécurisé au personnel de Roche en exploitant les identifiants des employés de Roche et le processus de connexion.

Toutes les API du SST pour edge et cloud sont protégées par des jetons d'accès qui peuvent être obtenus auprès de navify Access Control pour les acteurs humains et/ou de service.

(c) Audits et certifications.

infinity SST est déployé sur l'infrastructure de la plateforme navify et il utilise les services de la plateforme navify (navify Access Control) qui ont les certifications suivantes: certifications ISO 27000, ISO 27017, ISO 27018 et ISO 27701

(d) Sauvegarde et récupération.

La base de données du SST est déployée à l'aide d'AWS RDS qui est configuré avec une politique de sauvegarde et une haute disponibilité via le déploiement Multi-AZ.

(e) Gestion des modifications et gestion des versions.
● Les versions logicielles seront gérées conformément au MQMS-D&D-GSP-06 Gestion de la configuration [6], au plan de gestion de la configuration [7] et au MQMS-D&D-GSP-10 Développement logiciel [8]. La numérotation des versions logicielles pour SST suit le modèle V.I.S.B. où V est la version majeure, I est la version mineure, S est le correctif de service et B est le numéro de construction.
● La documentation est versionnée en utilisant les mêmes conventions que celles utilisées par le logiciel pour assurer la cohérence et la traçabilité
● Un référentiel de contrôles GitHub est utilisé pour gérer tous les éléments de configuration logicielle. Des étiquettes uniques sont utilisées pour identifier et décrire chaque élément de configuration logicielle.
● Les versions de code sont identifiées dans le référentiel de codes (GitHub) à l'aide des normes de version logicielle. La documentation est gérée dans des systèmes internes de gestion des documents.
● Les modifications sont appliquées aux fenêtres temporelles lorsqu'un accès faible à l'application est attendu.
● Les temps d'arrêt prévus pendant la fenêtre de maintenance devraient être de l'ordre de < 10 minutes. Pendant ce temps, l'application ne sera pas disponible et affichera un écran indiquant les activités de maintenance en cours.

(f) Minimisation des données.
Le SST gère uniquement les données requises pour la configuration des scénarios de simulation.
(g) Droits des Personnes concernées.
Roche agit en tant que sous-traitant pour infinity SST. Roche suivra les demandes du contrôleur des données afin d'assurer un traitement cohérent et sécurisé des données ainsi que la santé de la personne concernée. Par conséquent, Roche fournit un processus global de demande de la personne concernée qui peut être utilisé pour contacter directement Roche en tant que personne concernée. Roche s'alignera avec le responsable du traitement concerné sur les commentaires requis et les modalités de communication.
(h) Chiffrement.
Dans le transport: le cryptage est fourni par la moyenne de https avec une version TLS >= 1.2 dans les connecteurs applicables (p. ex., agent utilisateur du navigateur Web vers le back-end SST). De plus, dans les versions futures du SST, le fichier contenant la configuration est protégé par une clé symétrique générée par le SST et utilisée lors de la génération du fichier de configuration.
Au repos: dans les versions futures, la base de données (SC.9) et le stockage d'objets (SC.11) seront cryptés en exploitant les mécanismes de cryptage intégrés d'AWS.
(i) Correctifs, numérisation et tests de l'environnement.
La numérisation de la solution est effectuée à différents niveaux :

- Temps de développement :
o Analyse de sécurité des dépendances tierces avec Mend.
o Analyse statique des codes de sécurité avec SonarQube.
o Artefacts (p. ex. images de docker) numérisation avec le registre Harbor docker.
- Durée d'exécution :

o L'infrastructure cloud de Navify, les images des machines virtuelles et l'infrastructure globale de l'environnement sont surveillées en permanence à l'aide de Tenable et Dome9.
(j) Durcissement.
Le durcissement se produit au niveau de l'image du docker en limitant certaines capacités.

De même, les groupes de sécurité AWS sont utilisés pour ouvrir uniquement les ports requis. Cela s'applique également aux composants edge qui utilisent le pare-feu Roche Linux pour limiter les ports autorisés.

En outre, les images utilisées dans navify Cloud Infrastructure sont des images renforcées personnalisées de navify et des services supplémentaires tels que :

● IAM renforcé : il s'agit d'images obligatoires à utiliser pour fournir une charge de calcul telle que des instances EC2, ECS ou EKS. Plusieurs types de SE sont disponibles, associés aux agents de sécurité intégrés nécessaires.
● Dome9 - vous aide à évaluer votre posture de sécurité par rapport au cadre ou aux exigences de conformité, principalement par rapport à un ensemble de règles personnalisées navify Platform Cloud Infrastructure qui est nécessaire pour réussir à passer afin de demander votre compte suivant (STAGE/QA ou PROD).
● Splunk - Nos outils d'agrégation de journaux sont livrés avec des tableaux de bord prédéfinis pour vous aider à identifier où vous utilisez votre compte à risque et plus encore.
● SysDig Monitor and Secure - Au cas où vos produits seraient basés sur des dockers.
● Cloudflare - Obligatoire pour tout point de terminaison exposé à partir de navify Cloud.

(k) Surveillance et réponse aux incidents.
La SST en tant qu'application cloud fait partie des mesures de surveillance de navify cloud. La réponse aux incidents est assurée par le biais des processus globaux de Roche.
(l) Validation des données d'entrée.
Toutes les API utilisées dans le SST sont conçues en s'appuyant sur des cadres comme Spring qui effectuent déjà la validation des entrées de paramètres pour éviter les injections XSS et SQL en échappant aux valeurs non attendues.
(m) Système(s) de gestion des clés.
Cela se fera avec une réflexion clé, au moment de la mise en œuvre on ne sait pas encore laquelle.
(n) Emplacement et hébergement.
SST sera hébergé dans navify Cloud Infrastructure basée sur AWS dans une région basée aux États-Unis. L'accès au TSS sera limité géographiquement aux États-Unis.
(o) Enregistrement et surveillance.
SST est connecté aux outils Splunk et Grafana afin de consulter les journaux (Splunk) et de surveiller les indicateurs de traitement (Grafana). Les équipes de déploiement des services sont informées des comportements anormaux observés par le biais de la surveillance et peuvent rechercher des journaux afin d'en trouver la cause.
(p) Sécurité du réseau.
Les réseaux d'environnement cloud sont isolés, avec une séparation claire entre le réseau de données et les réseaux d'applications. De plus, le WAF (Web Application Firewall) basé sur Cloudflare est utilisé pour prévenir les DDoS et d'autres types d'attaques contre les API exposées.
(q) Le Profilage, Y Compris La Prise De Décision Individuelle Automatisée.
Sans objet, aucune personne concernée n'est affectée.
(r) Périodes de conservation et élimination des données.
Une fois la simulation terminée, la sandbox utilisée pour exécuter la simulation et les données associées sont automatiquement supprimées 1 jour après de l'environnement cloud.
(s) Enregistrement d'audit sécurisé.
Étant donné que la solution ne traite pas de données personnelles/cliniques, aucun audit n'est en place pour la première version du produit. Les versions suivantes utiliseront le service d'audit fourni par navify Platform.
(t) Tests et analyses de sécurité.
L'analyse des vulnérabilités du code est effectuée dans chaque intégration de demande d'extraction, y compris les portes qualité, ce qui empêche la fusion du code dans la succursale principale au cas où ces portes ne seraient pas remplies.

L’analyse de la solution est effectuée à différents niveaux :

- Temps de développement :
  - Analyse de sécurité des dépendances tierces avec Mend.
  - Analyse statique des codes de sécurité avec SonarQube.
  - Artefacts (p. ex. images de docker) numérisation avec le registre Harbor docker.
- Durée d’exécution :
  - L’infrastructure cloud de Navify, les images des machines virtuelles et l’infrastructure globale de l’environnement sont surveillées en permanence à l’aide de Tenable et Dome9.

Les tests de pénétration menés par une entreprise externe sont effectués régulièrement sur l’ensemble de la solution.

(u) Gestion des risques liés aux tiers.

infinity SST s’appuie sur la plateforme navify sans ajouter de tiers supplémentaires. Tous les tiers doivent faire l’objet d’une évaluation régulière basée sur leur classification des risques afin de garantir leurs capacités. De telles évaluations sont également requises pour les tiers de la plateforme navify.

(v) Transparence.

Les données personnelles traitées par SST sont téléchargées sur le cloud par l’utilisateur client lui-même. Il incombe donc à l’utilisateur client, en tant que responsable du traitement, d’informer les personnes concernées.

(w) Tests de pénétration

Infinity SST organisera des sessions de tests de pénétration, bien que l’on ne sache pas encore à quelle fréquence et à quel moment la publication aura lieu. Les résultats seront intégrés dans une conception architecturale plus approfondie et dans l’évaluation des risques de sécurité informatique des produits. Si des modifications majeures de l’architecture ou du système sont mises en œuvre, des tests de pénétration supplémentaires seront programmés dans le cadre du développement du produit Roche.

Il est exécuté dans un environnement aussi similaire que possible à celui de la production.