ACTIVITY TRACKER + NAVIFY INTEGRATOR

ANNEXE - Accord Spécifique de Traitement des Données à Caractère Personnel

entre

CLIENT

- le Responsable de Traitement -

- ci-après dénommé le CLIENT -

et

ROCHE DIAGNOSTICS FRANCE

- le Sous-Traitant -

- ci-après dénommé ROCHE -

1. CHAMP D'APPLICATION

1) Introduction. Le présent Accord relatif au traitement des données (ci-après dénommé l'« Accord relatif au traitement des données » ou l'« **Accord** ») fait partie intégrante du Contrat en tant qu'annexe à celui-ci. Les termes et expressions comprenant des majuscules qui sont employés dans le présent Accord sans y être définis ont la signification qui leur est attribuée dans le Contrat.
2) Parties. Dans le cadre du présent Accord, le CLIENT est le responsable du traitement et Roche (y compris ses Affiliées) est le sous-traitant (ou le sous-traitant ultérieur) chargé du traitement des Données à caractère Personnel.
3) Objet. L'objet de chaque Accord relatif au traitement des données ressort de l'Offre.
4) Durée. La durée du présent Accord correspond à celle de l'Offre.

2. SPÉCIFICATION

1) La nature et la finalité du traitement par ROCHE pour le CLIENT des Données à caractère Personnel sont précisément déterminées à l'Annexe 1.
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) Transfert de données
   nI sert uniquement l'application achetée/évaluée par le Client. En ce sens, si l'application traite des données personnelles, nI effectuera l'échange (transition des données) entre le système d'information du laboratoire du Client et l'application de service, ce qui signifie qu'alors seulement un traitement des données personnelles par nI aura lieu.
   Traitement du cas d'utilisation d'Activity Tracker : Selon l'Offre, l'installation de navify Integrator sur l'infrastructure du client est utilisée dans le but de collecter des informations pour automatiser et simplifier le processus de facturation pour le client et Roche (via l'application de suivi d'activité).
4) Les catégories de Personnes Concernées sont listées ci-dessous :
   - Données des patients
   - Données des professionnels de santé
5) Types de données. L'objet du Traitement des Données à Caractère Personnel (les « Données ») comprend les types et catégories de Données à Caractère Personnel ci-après :
   - Informations sur la commande

- Informations sur l'échantillon
- Informations sur les résultats
- Opérateur d'instruments.

CLARIFICATION :

- Roche utilise un ID d'échantillon transformé pour différencier et compter l'utilisation des services (test cobas respiratory flex), qui comporte un risque de réidentification pour moins de 12 ID d'échantillon différents par facturation. Le risque de réidentification est négligeable pour de plus grandes quantités d'ID d'échantillon et les données sont alors considérées comme anonymes.
- Aux fins d'utilisation d'Activity Tracker, aucune donnée personnelle n'est requise, par conséquent nI applique le hachage à tous les champs de données personnelles dans le message/la charge utile.
- Tout le message/la charge utile est également crypté par nI, puis transmis au Suivi d'activité
- Le hachage et le cryptage ont lieu sur nI edge (composant sur site de la nI), sur les sites des clients
- 'ensemble du message/de la charge utile est transféré par nI de manière hachée et chiffrée, car il est nécessaire de différencier les événements pour un comptage adéquat des tests effectués.

3. MESURES TECHNIQUES ET ORGANISATIONNELLES

1) Les Mesures techniques et organisationnelles nécessaires sont indiquées à l'Annexe A au présent Accord et sont approuvées par le CLIENT. À la date d'effet du présent Accord, le CLIENT reconnaît qu'il considère les Mesures techniques et organisationnelles qui y sont décrites comme appropriées, compte tenu de l'état des connaissances technologiques, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les Personnes Concernées.
2) Les mesures documentées constituent le fondement du présent Accord. Dans la mesure où le CLIENT demanderait que des modifications y soient apportées, celles-ci devraient être effectuées d'un commun accord.

4. SOUS-TRAITANCE

ROCHE 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
Affiliées membres du Groupe Roche et autres entités ROCHE Information Solutions India Pvt Ltd, 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. Toute activité de traitement des données est basée sur l'accord de transfert de données intersociétés (RIDTA) du groupe Roche contenant les clauses contractuelles types de l'UE du 4 juin 2021.

ROCHE Diagnostics International AG, Suisse ROCHE Diagnostics Corporation pour les clients d'Amérique du Nord, Etats-Unis ROCHE Diagnostics Uruguay and ROCHE Diagnostics Brésil pour les clients LATAM ROCHE Diagnostics Limited, UK and ROCHE Diagnostics S.L., Espagne pour les clients EMEA ROCHE Diagnostics Asia Pacific, Singapore pour les clients APAC	La demande initiale sera toujours lue par la filiale. Les filiales décident si elles transmettent la demande au support de 1er niveau. Les filiales du groupe Roche impliquées en tant que 1er point de contact sont: ● Roche Diagnostics Corporation, Inc., (Indianapolis, US) pour les clients d'Amérique de Nord, ● 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, ● Roche Diagnostics Asia Pacific pour les clients APAC, Les filiales impliquées dans le support de 2e niveau sont : ● Roche Services (Europe) Ltd pour les clients EMEA (Centre Budapest) ● Roche Services (Asia Pacific) Sdn. Pour les clients APAC (Centre Kuala Lumpur) ● Roche Services Americas pour les clients NAM and LATAM (Centre Costa Rica) When the requests cannot be solved, they are forwarded to Roche Diagnostics International AG (Rotkreuz, Switzerland) and Roche Information Solutions India Pvt Ltd (Puna, India).
AWS	agissant en tant que sous-traitant de Roche et en tant que fournisseur de l'hébergement de données (services cloud) dans la région respective, où la solution est déployée. Tous les traitements seront hébergés exclusivement sur l'instance AWS dans ● Francfort (Allemagne) pour les clients de l'UE, ● Instance AWS dans l'Oregon (États-Unis) pour les clients américains. ● D'autres sites d'hébergement peuvent être convenus en fonction des besoins des clients. Roche a signé les clauses contractuelles types (version du 4 juin 2021) avec AWS, Inc
Cloudflare	agissant en tant que sous-traitant de Roche et en tant que fournisseur de la protection d'accès au réseau et dans la région respective, où la solution est déployée.

5. 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.

6. 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.

7. SOUS-TRAITANCE

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.

8. 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[1].
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

1

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 ;
- 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.

9. 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.

10. 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.

11. 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.

12. RESPONSABILITÉ

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 POUR navify Integrator

Les contrôles, procédures et mesures suivants ont été mis en œuvre lors de la conception de navify Integrator (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.

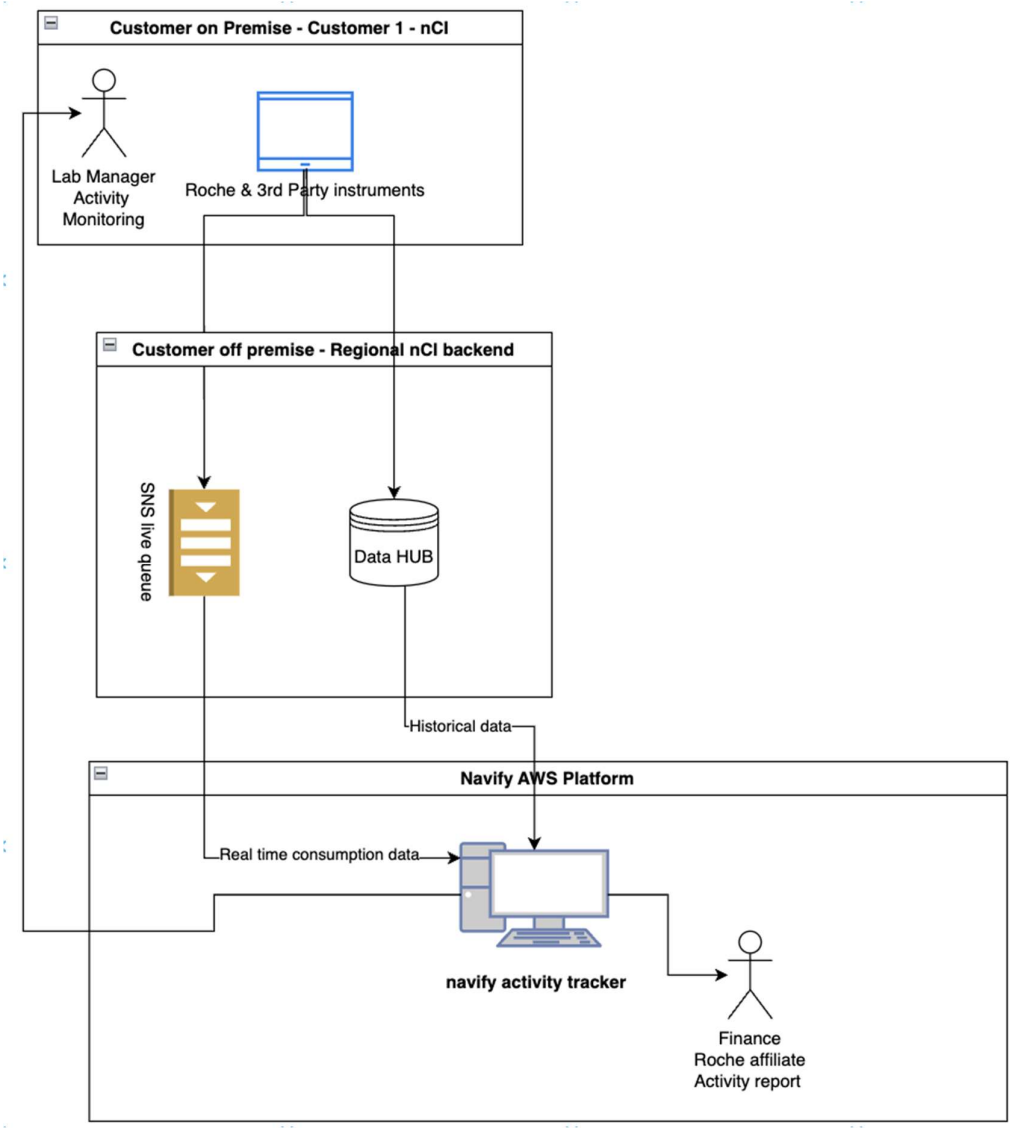
Non pertinent : nI n'interagit qu'avec les systèmes sans intervenir dans les activités des utilisateurs. Le texte relevant de la conformité à la réglementation ne concerne en l'occurrence aucun public.

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.

B) Mesures techniques et organisationnelles pour Activity Tracker

Les contrôles, procédures et mesures suivants ont été mis en œuvre dans le cadre d'Activity Tracker 1.0.0 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.



Vous trouverez ci-dessous une liste récapitulative des mesures techniques et organisationnelles :

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

En termes d'authentification et d'autorisation, les utilisateurs ou les systèmes qui interagissent avec Activity Tracker doivent s'authentifier par le biais le contrôle des accès (Access Control) navify.

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

Les utilisateurs de Roche accéderont à Activity Tracker en passant par le fournisseur d'identité de la plateforme navify qui garantit un accès sans risque au personnel de Roche en s'appuyant sur le processus de connexion et les identifiants des employés de Roche.

(c) Audits et Certifications.

Les utilisateurs de Roche accéderont à Activity Tracker en passant par le fournisseur d'identité de la plateforme navify qui garantit un accès sans risque au personnel de Roche en s'appuyant sur le processus de connexion et les identifiants des employés de Roche.

(d) Sauvegarde et Récupération.

La solution Activity Tracker bénéficie des fonctionnalités de sauvegarde et de récupération de la plateforme navify. Activity Tracker utilise la topologie des N répétitions (pour les lectures et les écritures) de ses services et utilise des zones de disponibilité (les AZ d'AWS) au sein des régions de production localisée, et, par conséquent, la solution est tolérante aux erreurs, présente un taux de disponibilité élevé et est conforme à la réglementation..

(e) Gestion des modifications et versionnage.

- Les versions des logiciels seront gérées conformément à la gestion de configuration QAP et à la gestion de configuration SOP. La numérotation des versions de logiciels utilisée pour Activity Tracker obéit au modèle V.I.S.B., où V correspond à une Version majeure, I à une Version mineure, S au chemin du service (Service Path) et B au numéro de génération.

- Dans un souci de cohérence et de traçabilité, les versions de la documentation obéissent aux mêmes conventions que celles appliquées aux logiciels

- Un référentiel de contrôle GitHub est utilisé pour conserver l'ensemble des éléments de configuration des logiciels. Des étiquettes uniques permettent d'identifier et de décrire chaque élément de configuration des logiciels.

- Les versons de code sont étiquetées dans le référentiel des codes (GitHub) selon les normes de numérotation des versions. La documentation est chargée et signée dans SAP.

(f) Minimisation des données.

Toutes les données utilisées par Activity Tracker sont traitées et chiffrées par navify integrator, de sorte que seules des données techniques sont utilisées dans l'application.

(g) Droits des personnes concernées.

N/A

(h) Cryptage.

N/A

(i) Correction, analyse et tests de l'environnement.

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 Activity Tracker sont gérés à l'aide des flux de travail GitOps.

(j) Renforcement de la sécurité.

Le renforcement est réalisé au niveau des images Docker en limitant certaines capacités. 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 et gestion des incidents.

Du point de vue du client, le processus sera le même que pour les autres produits numériques. 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).

(l) Validation des entrées.

Toutes les API utilisées dans Activity Tracker 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) Systèmes de gestion des clés.
Les secrets sont gérés au moyen de Hashicorp Vault qui est un système de gestion des secrets fourni par Roche. 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) Emplacement et Hébergement.

Le dispositif de suivi des activités sera déployé dans différentes régions pour assurer la disponibilité et la conformité réglementaire.

(o) Journalisation et Surveillance.

La journalisation et la surveillance reposent sur des outils de la plateforme tels que Splunk et Grafana. Activity Tracker fournit des indicateurs au format standard Prometheus, qui peuvent être utilisés pour détecter des schémas d'accès et d'utilisation inhabituels.

(p) Sécurité du réseau.

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 décision individuelle automatisée.

N/A

(r) Périodes de conservation et destruction des données.

Activity Tracker supprime automatiquement les données au terme d'une période configurable.

(s) Enregistrement sécurisé des audits.

N/A

(t) Tests et analyses de sécurité.
Un balayage des vulnérabilités de code est effectué à chaque demande de tirage, y compris les murs de qualité, qui empêche la fusion du code dans la branche principale dans le cas où les conditions au franchissement de ces murs ne seraient pas remplies. Les images de machine virtuelle de l'infrastructure cloud navify et l'infrastructure de l'environnement dans son ensemble sont surveillées en permanence à l'aide de Tenable et Dome9.

(u) Gestion des risques liés aux tiers.

N/A

(v) Transparence.

S/O : Le dispositif de suivi d'activité ne gère que les données techniques, de sorte que l'avertissement réglementaire ne s'applique pas.

(w) Test de pénétration

Activity Tracker organise une session de test de pénétration sur chaque version majeure de l'architecture globale par une entreprise externe. Les résultats sont 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.