navify Quality Performance

ANNEXE - Accord Spécifique de Traitement des Données à Caractère Personnel

Entre

Le CLIENT
- le Responsable de Traitement -
- ci-après dénommé le CLIENT -
Et

ROCHE DIAGNOSTICS FRANCE
- le Sous-Traitant -
- ci-après ROCHE -

1. CHAMP D'APPLICATION

(1) Application. Cet Accord Spécifique de Traitement des Données à Caractère Personnel (ci-après "l'Accord)") est une annexe faisant partie intégrale de l'Offre et du Contrat. Les termes en majuscule ont le sens défini dans le présent Accord ou le cas échéant dans les Conditions Générales Produits Numériques et Services associés et son annexe de traitement des données à caractère personnel.
(2) Parties. Dans cet Accord, le CLIENT a la qualité de Responsable de Traitement et ROCHE (incluant ses filiales), la qualité de Sous-traitant de Données à Caractère Personnel.
(3) Objet. L'objet de cet Accord résulte de l'Offre ROCHE.
(4) Durée. La durée de cet Accord correspond à la Durée de l'Offre.

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) Role de nI. nI sert uniquement l'application qui est achetée par le CLIENT. En ce sens, si l'application traite des données personnelles, nI effectuera l'échange (la transition des données) entre le système d'information du laboratoire du CLIENT et l'application de service, ce qui signifie que ce n'est qu'à ce moment-là qu'un traitement des données personnelles par nI aura lieu. Selon l'Offre, l'installation de navify Integrator sur l'infrastructure du CLIENT sert à la collecte de données pour la navify Quality Performance. Les données produites par les systèmes de laboratoire du CLIENT (contrôleur des données) sont transportées via navify Integrator vers navify Quality Performance. navify Integrator effectue l'échange des données du laboratoire vers l'application de service et crypte les données tout en conservant leur signification pour l'application de service (ici choisie navify Quality Performance). Les données restent chiffrées, préservant leur intégrité et leur signification pour l'application de service.

(4) Catégories de Personnes concernées. Les catégories de Personnes Concernées sont les suivantes :
a. Les clients des clients (patients)

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

En ce qui concerne la collecte des informations relatives à la commande auprès du client et leur mise à la disposition du tiers (p. ex., phlébotomiste, laboratoire) Catégorie a) des Personnes concernées ci-dessous:

- Données démographiques du patient (p. ex., âge, nom, prénom, sexe)
- Tests à effectuer (aucun résultat)
- Informations sur l'échantillon (ID de l'échantillon/type d'échantillon)

a) En ce qui concerne le recueil des informations d'échantillonnage auprès de tiers (p. ex. phlébotomiste, laboratoire) et leur envoi à la catégorie a) de personnes concernées ci-dessous:

- Données démographiques du patient (p. ex., âge, nom, prénom, sexe)
- Informations sur l'échantillon (ID de l'échantillon/type d'échantillon)

b) In respect to the collecting of the transport information from 3rd party (e.g. phlebotomist, laboratory) and sending it to the orderer Category a) of Data Subjects below:

- Informations sur l'échantillon (ID de l'échantillon/type d'échantillon)
- Information de commande (plusieurs tests à effectuer).

2. 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.

3. SOUS-TRAITANCE

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

Sous-traitant ultérieur de ROCHE	**Adresse / Pays**	**Service**
Roche Group affiliates, inter alia Roche Diagnostics International AG, Rotkreuz, Suisse, Roche Information Solutions India Pvt Ltd in Pune, Inde, Roche Diagnostics SL. in 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. Toute activité de traitement des données repose sur l'accord de transfert de données intersociétés (RIDTA) du groupe Roche.
AWS	Frankfurt ou autres data center situés en EEE	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. Actuellement, Francfort-sur-le-Main.

Cloudflare	EEE	agissant en tant que sous-processeur de Roche et en tant que fournisseur de la protection d'accès au réseau et dans la région respective, où la solution est déployée.
Interoperability Health (UK) Limited d.b.a (applicable si l'outil d'interoperability est installé)	EEE	Agissant en tant que sous-traitant de Roche et fournissant les services d'interopérabilité entre l'application et les systèmes SIL du client.

4. RECTIFICATION, LIMITATION ET EFFACEMENT DES DONNÉES À CARACTÈRE PERSONNEL

(1) ROCHE ne peut, de sa propre autorité, rectifier, effacer ou restreindre le traitement des Données en cours de traitement pour le compte du CLIENT, mais uniquement sur instruction documentée par le CLIENT. Dans la mesure où une Personne Concernée contacte directement ROCHE au sujet d'une rectification, d'un effacement ou d'une restriction du traitement, ROCHE transmettra la demande de la Personne Concernée au CLIENT sans retard injustifié.

(2) Dans la mesure où cela est inclus dans la portée des services, la politique d'effacement, le « droit à l'oubli », la rectification, la portabilité des données et l'accès seront assurés par ROCHE conformément aux instructions documentées par le CLIENT sans retard injustifié.

(3) Le CLIENT prend note du fait que ROCHE ne sera pas en mesure de procéder seule à la portabilité, à la rectification, à l'effacement ou à la limitation du traitement de données en raison de son cryptage complet et de son contrôle exclusif du CLIENT sur les clés de décryptage. Par conséquent, le CLIENT doit apporter à ROCHE un soutien approprié et rapide dans la mise en œuvre d'une telle demande, et doit soit rémunérer les efforts de ROCHE, soit conserver les obligations ci-dessus afin de les satisfaire directement par le biais d'une interface locale non cryptée du CLIENT.

5 GARANTIE QUALITÉ ET AUTRES OBLIGATIONS DE ROCHE

(1) Outre le respect des règles énoncées dans le présent DPA applicable, ROCHE devra se conformer aux exigences réglementaires mentionnées aux articles 28 et 33 du RGPD. Par conséquent, ROCHE assure, en particulier, sa conformité aux exigences suivantes:

a) La confidentialité conformément à l'article 28, paragraphe 3, phrase 2, point b, aux articles 29 et 32, paragraphe 4 du RGPD. ROCHE confie uniquement à ces collaborateurs le traitement des données indiqué dans chaque accord de traitement de données qui ont été tenus à la confidentialité et ont été préalablement familiarisés avec les dispositions relatives à la protection des données pertinentes pour leur travail. ROCHE et toute personne agissant sous son autorité qui a accès aux Données ne traiteront ces Données que sur instruction du CLIENT, ce qui inclut les pouvoirs accordés dans le présent Accord, à moins que la loi en vigueur ne l'exige.

b) Mise en œuvre et respect de toutes les Mesures Techniques et Organisationnelles nécessaires pour chaque DPA conformément à l'article 28, paragraphe 3, phrase 2, point c, et à l'article 32 du RGPD, et comme indiqué à la Section 3.

c) ROCHE et le CLIENT coopèrent, sur demande, avec l'autorité de surveillance dans l'exécution de ses tâches.

d) Le CLIENT sera immédiatement informé de toutes les inspections et mesures effectuées par l'autorité de contrôle, dans la mesure où elles sont liées à un accord de traitement de données. Cela s'applique également dans la mesure où ROCHE fait l'objet d'une enquête ou est partie d'une enquête menée par une autorité compétente en lien avec des infractions à une loi civile ou pénale, ou à une règle ou réglementation administrative concernant le traitement des Données en lien avec un accord de traitement de données.

e) Dans la mesure où le CLIENT fait l'objet d'une inspection par l'autorité de contrôle, d'une infraction administrative ou sommaire, d'une procédure pénale, d'une demande en responsabilité par une Personne Concernée ou par un tiers ou de toute autre demande en lien avec un DPA, ROCHE fera tout son possible pour aider le CLIENT.

f) ROCHE contrôlera périodiquement les processus internes et les Mesures Techniques et Organisationnelles afin de s'assurer que le traitement effectué dans son domaine de responsabilité est conforme aux exigences de la législation applicable en matière de protection des données et de la protection des droits de la Personne Concernée.

g) Vérifiabilité des Mesures Techniques et Organisationnelles mises en œuvre par le CLIENT dans le cadre des pouvoirs de surveillance du CLIENT visés par la section 7 du présent Accord.

6. SOUS-TRAITANCE

(1) Aux fins du présent Accord, on entend par sous-traitance les services qui sont directement liés à la fourniture du service principal. Cela ne comprend pas les services auxiliaires, tels que les services de télécommunications, les services postaux/de transport, les services de maintenance et d'assistance aux utilisateurs ou l'élimination des supports de données, ainsi que d'autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des équipements de traitement de données. Toutefois, ROCHE sera tenue de prendre des dispositions contractuelles appropriées et juridiquement contraignantes et de prendre des mesures d'inspection appropriées pour assurer la protection et la sécurité des données du CLIENT, même dans le cas de services auxiliaires externalisés.

(2) ROCHE peut faire appel à des sous-traitants (sous-traitants supplémentaires) comme expressément approuvé par le CLIENT. Le CLIENT accepte la mise en service des sous-traitants énumérés dans l'accord de traitement de données applicable à la condition qu'un contrat soit conclu conformément à l'article 28, paragraphes 2 à 4 du RGPD.

(3) L'externalisation à des sous-traitants ou le changement de sous-traitants existants sont autorisés lorsque :

- ROCHE soumet une telle externalisation à un sous-traitant au CLIENT par écrit ou sous forme de texte avec un préavis approprié ; et

- le CLIENT ne s'est pas opposé à l'externalisation prévue par écrit ou sous forme de texte dans les deux semaines suivant la soumission de ROCHE au CLIENT ; et

- La sous-traitance est basée sur un accord contractuel conformément à l'article 28, paragraphes 2 à 4 du RGPD.

(4) Le transfert des Données du CLIENT au sous-traitant et le début du traitement des données par les sous-traitants ne seront entrepris qu'après que toutes les exigences auront été respectées.

(5) Si le sous-traitant fournit le service convenu en dehors de l'UE/EEE, ROCHE veillera au respect des réglementations de l'UE en matière de protection des données par des mesures appropriées. Il en va de même si des prestataires de services doivent être utilisés au sens du paragraphe 1, phrase 2.

(6) Toute nouvelle externalisation par le sous-traitant nécessite le consentement exprès de ROCHE (au minimum sous forme de texte).

(7) Toutes les dispositions contractuelles de la chaîne contractuelle sont communiquées à chaque sous-traitant supplémentaire et convenues avec lui.

7. POUVOIR DE SUPERVISION DU CLIENT

(1) Le CLIENT a le droit, après consultation avec ROCHE, de procéder à des inspections ou de les faire effectuer par un auditeur qui sera désigné dans chaque cas individuel. Elle a le droit de se convaincre du respect d'un DPA par ROCHE dans le cadre de ses activités professionnelles au moyen de contrôles aléatoires, qui doivent normalement être annoncés en temps utile.

(2) ROCHE s'engage à fournir au CLIENT les informations nécessaires sur demande et, en particulier, à démontrer l'exécution des Mesures Techniques et Organisationnelles.

(3) La preuve de ces mesures peut être fournie par

- le respect des codes de conduite approuvés conformément à l'article 40 du RGPD ; et/ou
- la certification selon une procédure de certification approuvée conformément à l'article 42 du RGPD ; et/ou
- Les certificats, les rapports ou les extraits de rapports d'auditeurs actuels fournis par des organismes indépendants (p. ex. auditeur, Délégué à la Protection des Données, service de sécurité informatique, auditeur de confidentialité des données, auditeur qualité) ; et/ou
- Une certification appropriée attribuée par un audit de sécurité informatique ou de protection des données (par ex. conformément à BSI-Grundschutz (une certification de protection informatique initiale développée par le Bureau fédéral allemand pour la sécurité des technologies de l'information (BSI)) ou ISO/IEC 27001).

(4) ROCHE peut réclamer une rémunération pour autoriser les inspections du CLIENT qui ne sont pas justifiées.

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

(4) 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 Quality Performance

Les contrôles, procédures et mesures suivants en matière de système, d'opérations et de procédures ont été mis en œuvre dans le cadre de navify Quality Performance 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 (PHYSIQUE)

Les contrôles d'accès physique aux salles des serveurs sont assurés par l'intermédiaire de l'AABD GmbH Sicherheitsdienste.Les contrôles sont constitués de :

- Le service de sécurité local reçoit une liste des employés autorisés qui vont visiter le centre de données
- Les nouveaux employés sont inscrits en fournissant leur pièce d'identité au moins 24 heures avant la visite
- L'accès au centre de données n'est accordé que par appariement positif des ID et des employés au moment de la visite
- Une carte de code valide est nécessaire pour lever les barrières
- Les bâtiments ne sont accessibles qu'avec une clé
- Le serveur/la salle d'équipement 907 n'est accessible qu'avec un transpondeur
- Les collaborateurs doivent indiquer l'heure prévue de la visite et donner leur numéro de téléphone portable pour les contacter
    - Si l'employé n'a plus l'heure prévue de la visite, le service de sécurité l'appelle et lui demande des raisons
    - Lorsqu'un appel n'est pas possible, le service de sécurité s'occupe physiquement du collaborateur qui se rend dans le centre de données
- - Une fois la visite terminée, la carte de code, la clé d'accès et le transpondeur doivent être restitués au service de sécurité.
    - Le service de sécurité signe une preuve de retour de l'équipement
    - Si l'équipement (carte code, clé d'accès, transpondeur) n'est pas retourné, la carte code et le transpondeur sont bloqués.

Les contrôles d'accès physique aux salles des serveurs sont assurés par l'intermédiaire de l'AABD GmbH Sicherheitsdienste. Les contrôles sont constitués de :

- Le service de sécurité local reçoit une liste des employés autorisés qui vont visiter le centre de données
- Les nouveaux employés sont inscrits en fournissant leur pièce d'identité au moins 24 heures avant la visite
- L'accès au centre de données n'est accordé que par appariement positif des ID et des employés au moment de la visite
- Une carte de code valide est nécessaire pour lever les barrières
- Les bâtiments ne sont accessibles qu'avec une clé
- Le serveur/la salle d'équipement 907 n'est accessible qu'avec un transpondeur
- Les collaborateurs doivent indiquer l'heure prévue de la visite et donner leur numéro de téléphone portable pour les contacter
    - Si l'employé n'a plus l'heure prévue de la visite, le service de sécurité l'appelle et lui demande des raisons
    - Lorsqu'un appel n'est pas possible, le service de sécurité s'occupe physiquement du collaborateur qui se rend dans le centre de données

- Une fois la visite terminée, la carte de code, la clé d'accès et le transpondeur doivent être restitués au service de sécurité.
    - Le service de sécurité signe une preuve de retour de l'équipement
    - Si l'équipement (carte code, clé d'accès, transpondeur) n'est pas retourné, la carte code et le transpondeur sont bloqués.

(B) CONTRÔLE D'ACCÈS (ÉLECTRONIQUE)

L'authentification à l'infrastructure dorsale du serveur est possible via l'interface administrateur sur des canaux cryptés SSL. Chaque
l'employé disposant d'un compte d'utilisateur bénéficie de privilèges basés sur la nécessité d'une description de poste et d'une formation.
Zaske applique des règles de mot de passe aux employés :

- Les mots de passe ne doivent pas être faciles à deviner. Les noms, plaques d'immatriculation, date de naissance, etc. ne sont pas autorisés comme mot de passe.
- Les mots de passe doivent contenir des majuscules et des minuscules, des caractères spéciaux et des chiffres.
- Au moins le mot de passe doit être composé de deux des quatre types de caractères.
- Si un mot de passe se compose uniquement de caractères alphanumériques, il doit contenir au minimum 8 caractères
- Si un mot de passe se compose uniquement de chiffres, il doit contenir au minimum 6 caractères et le système d'autorisation bloquera le système pour cet utilisateur après quelques tentatives pendant un certain temps.
- Les mots de passe prédéfinis doivent être remplacés par un mot de passe individuel conformément aux règles décrites après la première connexion
- Le mot de passe ne doit pas être enregistré sur des touches fonctionnelles programmables
- Le mot de passe doit être gardé secret avec le propriétaire et ne doit pas être partagé

L'accès client est accordé sur la base de deux rôles. Tout d'abord, les rôles d'administrateur ont des privilèges supplémentaires pour inviter des utilisateurs, représentant le second type d'utilisateurs. Les deux rôles sont équipés d'un mot de passe, d'un nom d'utilisateur, qui est recommandé comme pseudonyme, adresse e-mail et préférence de langue.

(C) AUDITS ET CERTIFICATIONS.

NA

(D) SAUVEGARDE ET RÉCUPÉRATION.

Dispositif à blocs répliqués distribués – Synchronisation des données du serveur actif au serveur de secours pour des raisons de redondance.

PostgreSQL – La base de données PostgreSQL est mise en miroir en temps réel sur le serveur de secours pour une sauvegarde quotidienne.

Connexion aux réseaux de base – Le centre de données principal est connecté à deux centres de données de base.

(E) GESTION DES CHANGEMENTS ET GESTION DES VERSIONS.

Zaske s'aligne sur tout changement avec Roche et communiquera toutes les mises à jour et les temps d'arrêt à Roche. Roche doit informer ses clients des impacts commerciaux potentiels.

Les changements d'urgence seront mis en œuvre sans information afin de sécuriser les données et le traitement. Les informations à Roche seront accompagnées d'explications après la mise en œuvre des changements d'urgence.

(F) MINIMISATION DES DONNÉES.

Zaske n'utilise que des données minimales nécessaires pour informer et autoriser les utilisateurs de la plate-forme.

(G) DROITS DES PERSONNES CONCERNÉES.

Les demandes des personnes concernées sont transmises par Roche à Zaske, qui agit en tant que sous-traitant pour Roche.

(H) CHIFFREMENT.

Chiffrement par mot de passe – par SHA256 à 512 et SHA3 plus, PBKDF2, bcrypt ou scrypt, Poly1305

(I) MISE À JOUR DE L'ENVIRONNEMENT, ANALYSE ET TESTS.

Zaske a plusieurs clients qui sont obligés d'auditer Zaske régulièrement. Sur la base des audits réguliers, aucun manuel supplémentaire n'a été mis en place.

(J) RENFORCEMENT DE SÉCURITÉ.

- Détection d'intrusion du serveur – toute manipulation au niveau du serveur physique sera signalée par e-mail,
- Pare-feu Windows,
- Pare-feu matériel – pour le centre de données.

(K) SURVEILLANCE ET GESTION DES INCIDENTS.

Des processus sont en place pour accepter les demandes d'assistance et de service par e-mail, téléphone ou fax. Zaske s'aligne en interne avec l'équipe pour travailler sur le cas. Le demandeur recevra une réponse de la part de Zaske pour toute mise à jour du statut.

Zaske a mis en place des processus pour surveiller activement les incidents et apporter des solutions.

(L) VALIDATION DES ENTRÉES.

- Format de données restreint – seules les données au format .XML ou .dat sont acceptées,
- Prévention des injections – interprétation schématique des données ingérées.

(M) SYSTÈME(S) DE GESTION DES CLÉS.

Les clés sont gérées à l'aide des informations de l'outil IISCrypto dans le centre de données.

(N) EMPLACEMENT ET HÉBERGEMENT.

Les bureaux de Zaske sont situés à Bad Camberg, en Allemagne

Le centre de données est basé à Wiesbaden, en Allemagne et fourni par VISTEC Internet Service GmbH Hagenauer Str. 42 65203 Wiesbaden

(O) JOURNALISATION ET SURVEILLANCE.

- Surveillance de la manipulation du serveur – toute manipulation du serveur sera signalée par e-mail,
- Surveillance des accès – Hyperviseur (Promox) pour surveiller les accès, les mises à jour et les temps d'arrêt,
- Surveillance de la prise de données - les événements d'ingestion sont consignés,
- Rapports sur les pare-feu – collecte et surveillance des rapports sur les pare-feu,

(P) SÉCURITÉ DU RÉSEAU.

Réseau privé virtuel (VPN) – un point d'accès VPN est requis pour les besoins administratifs et productifs. Les tunnels VPN sont construits uniquement via une connexion IPsec. VPN de site à site – intégré pour assurer la sécurité des environnements entre Roche et Zaske. Tunneling SSH - connexions cryptées et autorisées avec blocage des commandes et des enregistrements de données non autorisés.

(Q) PROFILAGE, Y COMPRIS LA PRISE DE DÉCISION AUTOMATISÉE INDIVIDUELLE.

La performance qualité de navify ne permet pas le profilage. De plus, le service ne comporte aucune partie de prise de décision automatisée.

(R) PÉRIODES DE CONSERVATION ET ÉLIMINATION DES DONNÉES.

Les comptes d'utilisateurs administrateurs sont conservés pendant la durée du contrat. Les comptes d'utilisateur sont gérés par l'administrateur du client et peuvent être ajoutés et supprimés à tout moment.

(S) REGISTRE D'AUDIT SÉCURISÉ.

Le service n'a pas d'intention médicale et n'offre donc pas de dossier d'audit sécurisé. Cependant, les changements sont gérés par le biais de la gestion des changements et sont donc surveillés et signalés.

(T) TESTS DE SÉCURITÉ ET ANALYSE.

- IISCrypto pour vérifier et tester les mesures de sécurité,
- Détection des intrusions – vérification quotidienne de tous les packages exécutés par RKHunter et chkrootkit avec journalisation jointe,
- Détection de la force brutale – les connexions sont surveillées par SSHGuard. En cas de tentatives de connexion suspectes, l'adresse IP de l'ordinateur qui tente de se connecter sera bloquée,
- Déni de service de protection – Des scanners sont en place pour détecter les attaques DDoS et bloquer le transfert de données à partir de sources identifiées,

SSL-test – SSL ordinaire.

(U) GESTION DES RISQUES LIÉS AUX TIERS.

Zaske a mis en place son propre processus de gestion des risques de tiers pour évaluer les risques potentiels posés par des tiers. Les changements apportés à des tiers ayant un impact sur les services proposés à Roche seront communiqués et alignés avant la mise en œuvre.

(V) TRANSPARENCE.

Les personnes concernées en tant qu'utilisateurs sont informées du traitement par la déclaration de confidentialité sur le service web de navify Quality Performance. Les utilisateurs administrateurs sont informés par l'intermédiaire du responsable du traitement des données, comme l'exige l'offre de service, afin d'activer le service.

(w) [INSÉRER DES MESURES TECHNIQUES ET ORGANISATIONNELLES SUPPLÉMENTAIRES, LE CAS ÉCHÉANT]

NA