Accord de sous-traitance de données personnelles (DPA)

Conclu en application de l'article 28 du Règlement (UE) 2016/679 (« RGPD »), complété d'une annexe relative à l'article 30 du Règlement (UE) 2022/2554 (« DORA »)

Version 1.1 — **[À COMPLÉTER : date d'entrée en vigueur]**

Entre les parties

Le Client

- Dénomination : **[À COMPLÉTER : dénomination sociale du Client]**
- Forme juridique et registre : **[À COMPLÉTER]**
- Siège social : **[À COMPLÉTER]**
- Représenté par : **[À COMPLÉTER : nom, fonction]**
- Contact conformité / protection des données (notifications des articles 5.4.2 et 5.6) : **[À COMPLÉTER : adresse email]**

ci-après « **le Client** », agissant en qualité de **responsable du traitement** ou, le cas échéant, de sous-traitant de premier rang agissant pour le compte de ses propres clients responsables du traitement (article 6.2),

et

Cryptaguard BV, société à responsabilité limitée (BV) de droit belge

- Numéro d'entreprise (BCE) : 1007.610.660
- Siège social : Fazantenlaan 9, 1600 Sint-Pieters-Leeuw, Belgique
- Représentée par : Matthieu Roland, administrateur

exploitant la plateforme logicielle **ResiPlan** (le « **Service** »), ci-après « **le Sous-traitant** »,

ensemble « les **Parties** ».

---

1. Définitions

Les termes « données à caractère personnel », « traitement », « responsable du traitement », « sous-traitant », « personne concernée », « violation de données à caractère personnel » ont le sens que leur donne l'article 4 du RGPD. Les termes « entité financière », « prestataire tiers de services TIC », « fonction critique ou importante » ont le sens que leur donne l'article 3 du règlement DORA. « Contrat principal » désigne les conditions d'utilisation du Service acceptées par le Client **[À COMPLÉTER : référence et version des CGU/du contrat de services]**, que le présent accord complète.

2. Objet et hiérarchie contractuelle

2.1. Le présent accord (le « **DPA** ») encadre les traitements de données à caractère personnel que le Sous-traitant réalise **pour le compte du Client** dans le cadre de la fourniture du Service, conformément à l'article 28 du RGPD.

2.2. Le DPA fait partie intégrante du Contrat principal. En cas de contradiction entre le DPA et le Contrat principal concernant le traitement de données à caractère personnel, le DPA prévaut.

2.3. Lorsque le Client est une entité financière au sens de DORA, ou agit pour le compte d'une entité financière, l'**Annexe 5** énonce les stipulations contractuelles requises par l'article 30 de DORA et prévaut, pour ces sujets, sur toute stipulation moins protectrice.

2.4. Les obligations et les droits du Client, en sa qualité de responsable du traitement, sont définis par le présent DPA — notamment les articles 5.1 (instructions), 5.4.2 (objection aux sous-traitants ultérieurs), 5.8 (choix du sort des données), 5.9 (audits) et 6 — ainsi que par le Contrat principal.

3. Description du traitement

La description détaillée du traitement — objet, durée, nature et finalités, catégories de données à caractère personnel et catégories de personnes concernées — figure en **Annexe 1**, conformément à l'article 28, paragraphe 3, du RGPD.

4. Durée

Le DPA s'applique aussi longtemps que le Sous-traitant traite des données à caractère personnel pour le compte du Client, et au plus tard jusqu'à l'expiration du délai de suppression prévu à l'article 5.8.

5. Obligations du Sous-traitant

5.1. Instructions documentées

Le Sous-traitant traite les données à caractère personnel **uniquement sur instruction documentée du Client**, y compris en ce qui concerne les transferts vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit d'un État membre ; dans ce cas, il informe le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public. Le Contrat principal, le paramétrage du Service par le Client et le présent DPA constituent les instructions documentées initiales. Le Sous-traitant informe immédiatement le Client si, selon lui, une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

5.2. Confidentialité

Le Sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité, et ne traitent les données que sur instruction et pour les besoins de leurs fonctions.

5.3. Sécurité du traitement

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles décrites en **Annexe 2**, conformément à l'article 32 du RGPD, en tenant compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques. Le Sous-traitant peut faire évoluer ces mesures, à condition de ne pas en réduire le niveau de protection global.

5.4. Sous-traitance ultérieure

5.4.1. Le Client accorde au Sous-traitant une **autorisation écrite générale** de recourir aux sous-traitants ultérieurs listés en **Annexe 3**.

5.4.2. Le Sous-traitant informe le Client de tout projet (i) d'ajout ou de remplacement de sous-traitant ultérieur, ou (ii) de **modification des localisations** (régions ou pays) de fourniture du Service ou de traitement/stockage des données listées aux Annexes 3 et 4 — y compris lorsqu'un sous-traitant ultérieur existant change de localisation — **au moins 30 jours** avant sa prise d'effet. La notification est adressée par email au contact conformité désigné en tête du présent DPA, doublée d'une notification aux administrateurs de l'organisation du Client et de la mise à jour de la page publique de transparence ; le délai d'objection court à compter de l'email. Lorsque le Client a déclaré agir pour le compte d'un responsable du traitement ou d'une entité financière tiers, le préavis est porté à **60 jours** afin de préserver une fenêtre d'objection utilisable en cascade. Le Client peut émettre des objections légitimes et documentées dans ce délai ; à défaut d'accord sur une solution alternative raisonnable, le Client peut résilier le Contrat principal pour la partie du Service concernée, sans pénalité et avec remboursement au prorata des sommes prépayées correspondant à la période non courue.

5.4.3. Le Sous-traitant impose par contrat à chaque sous-traitant ultérieur des obligations de protection des données **au moins équivalentes** à celles du présent DPA, notamment des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Le Sous-traitant demeure **pleinement responsable** envers le Client de l'exécution de leurs obligations par les sous-traitants ultérieurs.

5.5. Assistance — droits des personnes concernées

Compte tenu de la nature du traitement, le Sous-traitant aide le Client, par des mesures techniques et organisationnelles appropriées, à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (articles 12 à 23 du RGPD : accès, rectification, effacement, limitation, portabilité, opposition). Le Service permet au Client de consulter, rectifier, exporter et supprimer lui-même les données ; pour toute demande nécessitant l'intervention du Sous-traitant, celui-ci répond dans un délai maximal de **10 jours ouvrés**. Si une personne concernée s'adresse directement au Sous-traitant, celui-ci transmet la demande au Client sans délai injustifié et ne lui répond pas lui-même, sauf instruction contraire du Client.

5.6. Notification des violations de données et des incidents TIC

5.6.1. **Violations de données.** Le Sous-traitant notifie au Client toute violation de données à caractère personnel **sans délai injustifié et au plus tard [À VALIDER : 24] heures** après en avoir pris connaissance, à l'adresse du contact conformité désigné en tête du présent DPA. La notification contient, dans la mesure des informations disponibles, les éléments prévus à l'article 33, paragraphe 3, du RGPD : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées, point de contact. Le Sous-traitant documente la violation et coopère avec le Client pour toute notification à l'autorité de contrôle ou communication aux personnes concernées.

5.6.2. **Incidents TIC.** Indépendamment de toute violation de données, le Sous-traitant notifie au Client, sans délai injustifié et au plus tard **[À VALIDER : 24] heures** après en avoir pris connaissance, tout incident lié aux TIC affectant le Service, avec les informations nécessaires à sa classification par le Client au titre de DORA : périmètre affecté, impact constaté ou estimé, chronologie, mesures de remédiation engagées, point de contact. Le Sous-traitant tient le Client informé de l'évolution jusqu'à résolution.

5.6.3. La notification d'une violation ou d'un incident ne vaut reconnaissance ni d'une faute ni d'une responsabilité.

Contact de notification du Sous-traitant : security@resiplan.eu

5.7. Assistance — sécurité, AIPD et consultation préalable

Le Sous-traitant aide le Client à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, compte tenu de la nature du traitement et des informations à sa disposition, notamment pour la réalisation d'analyses d'impact relatives à la protection des données (AIPD) et la consultation préalable de l'autorité de contrôle. La documentation de sécurité du Service (Annexe 2, politique de confidentialité, centre de confiance) est fournie à cette fin sans coût additionnel.

5.8. Sort des données en fin de contrat

5.8.1. Pendant toute la durée du Contrat principal, ainsi que pendant la période de transition prévue à l'Annexe 5 (30(3)(f)) et en cas d'insolvabilité, de résolution ou de cessation d'activité du Sous-traitant, le Client peut **exporter à tout moment** l'ensemble de ses données — **à caractère personnel et non personnel** (analyses d'impact, plans, registres, cartographies, documents) — via les fonctions d'export du Service (PDF, Excel/CSV, DOCX) et via l'API (JSON).

5.8.2. Au terme du Contrat principal, le Sous-traitant, **selon le choix du Client**, supprime toutes les données ou les restitue au Client dans un format structuré, couramment utilisé et aisément accessible, puis détruit les copies existantes, à moins que le droit de l'Union ou le droit d'un État membre n'exige leur conservation. À défaut d'instruction du Client dans les **[À VALIDER : 30] jours** suivant le terme, le Sous-traitant procède à la suppression ; lorsque le Client est une entité financière ayant notifié un statut FCI (Annexe 5), aucune suppression par défaut n'intervient avant la fin de la période de transition **et** une confirmation écrite. La suppression des sauvegardes intervient au plus tard **[À VALIDER : 35] jours** après la suppression des données de production. Sur demande, le Sous-traitant atteste par écrit de la suppression.

5.9. Audits et démonstration de conformité

5.9.1. Le Sous-traitant met à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD. Les questionnaires de due diligence et revues documentaires ne s'imputent pas sur la limite de fréquence ci-dessous.

5.9.2. Le Sous-traitant permet la réalisation d'**audits, y compris des inspections**, par le Client ou un auditeur tiers mandaté par lui (non concurrent du Sous-traitant, tenu à la confidentialité), et y contribue. Sauf violation avérée, incident de sécurité affectant le Client ou suspicion raisonnable et documentée de manquement, ou exigence d'une autorité de contrôle, ces audits sont limités à **un par période de douze mois**, moyennant un préavis écrit de **30 jours**, pendant les heures ouvrées, sans perturber de manière disproportionnée l'exploitation du Service, chaque Partie supportant ses propres coûts.

5.9.3. Lorsque le Client est une entité financière (ou agit pour son compte), les **droits étendus d'accès, d'inspection et d'audit prévus par l'Annexe 5 (DORA)** s'appliquent en complément et prévalent en cas de conflit.

5.10. Enregistrements de séances de crise

Lorsque le Client active la captation des séances de crise : (i) la transcription est réalisée **par défaut localement**, sur l'infrastructure du Sous-traitant en Union européenne ; le recours au prestataire cloud listé en Annexe 3 requiert une activation explicite par l'organisation du Client ; (ii) les fichiers audio et transcriptions sont soumis à une durée de conservation paramétrable par le Client ; (iii) leur accès est restreint aux rôles habilités de l'organisation du Client ; (iv) le Client fait son affaire de l'information préalable des participants à l'enregistrement, conformément aux articles 13 et 14 du RGPD.

6. Obligations du Client

6.1. Le Client garantit que le traitement confié repose sur une base juridique valable, que les données ont été collectées licitement, que les personnes concernées ont été informées conformément aux articles 13 et 14 du RGPD, et que ses instructions sont conformes au droit applicable. Le Client est responsable du paramétrage du Service (notamment gestion des comptes, rôles et permissions, activation des fonctions optionnelles) et de l'exactitude des données qu'il y introduit.

6.2. **Chaîne de sous-traitance.** Lorsque le Client agit en qualité de sous-traitant pour le compte d'un responsable du traitement, il garantit : (i) avoir obtenu l'autorisation écrite, préalable, spécifique ou générale, de ce responsable pour engager le Sous-traitant, conformément à l'article 28, paragraphe 2, du RGPD ; (ii) que les obligations imposées au Sous-traitant par le présent DPA sont au moins équivalentes à celles de son propre contrat de sous-traitance, conformément à l'article 28, paragraphe 4 ; (iii) répercuter sans délai au responsable du traitement les notifications reçues au titre des articles 5.4.2 et 5.6.

6.3. **Catégories particulières de données (art. 9 RGPD).** Le Service n'est pas destiné au traitement **systématique ou structuré** de catégories particulières de données, qui demeure interdit sans accord écrit préalable du Sous-traitant. Les mentions incidentes de telles données dans des contenus libres (déclarations d'incidents, comptes rendus d'exercices, enregistrements de séances de crise) sont couvertes par le présent DPA et bénéficient des mesures de l'Annexe 2 ; le Client veille à leur minimisation et détermine, en sa qualité de responsable, leur base juridique.

7. Transferts internationaux

Les transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales sont encadrés conformément au chapitre V du RGPD, dans les conditions décrites en **Annexe 4**. Le Sous-traitant n'opère aucun transfert non listé sans respecter la procédure de l'article 5.4.

8. Responsabilité et assurance

8.1. La responsabilité de chaque Partie au titre du présent DPA est régie par le régime de responsabilité du Contrat principal, sous réserve de ce qui suit : pour les manquements au présent DPA et les incidents affectant la sécurité ou la confidentialité des données du Client, la responsabilité du Sous-traitant est plafonnée à **[À COMPLÉTER : plafond dédié — ex. deux fois les redevances annuelles]**, par dérogation au plafond général du Contrat principal ; les exclusions de dommages indirects ne s'appliquent pas aux amendes administratives et coûts de notification directement causés par un manquement du Sous-traitant. Aucune stipulation du présent DPA ne limite la responsabilité d'une Partie envers les personnes concernées ni ne fait obstacle à l'article 82 du RGPD.

8.2. Le Sous-traitant maintient pendant toute la durée du DPA une assurance responsabilité civile professionnelle couvrant les risques cyber, auprès de **[À COMPLÉTER : assureur]**, pour un montant minimal de **[À COMPLÉTER : montant]** par sinistre ; une attestation est communiquée au Client à la signature et à chaque renouvellement sur demande.

9. Droit applicable et juridiction

Le présent DPA est régi par le droit **[À VALIDER : français]**, en cohérence avec le Contrat principal (CGU, art. 14). Tout litige relatif à sa validité, son interprétation ou son exécution relève de la compétence exclusive des tribunaux de **[À VALIDER : Paris, France, comme le Contrat principal]**,

sous réserve des compétences impératives des autorités de contrôle et des juridictions désignées par le RGPD.

10. Options souscrites et signatures

Options souscrites par le Client (cocher à la signature) :

- ☐ **Mode « IA en Union européenne seulement »** (Annexe 4) — prend effet à la signature ; inclut la transcription locale/UE des séances de crise ; pour l'organisation du Client, les fournisseurs d'IA établis hors UE sont réputés **retirés de la liste des sous-traitants autorisés** de l'Annexe 3 et toute violation de cette configuration constitue un manquement essentiel ouvrant droit à résiliation sans pénalité.
- ☐ **Statut « fonction critique ou importante » (FCI)** notifié dès la signature (Annexe 5, partie B applicable immédiatement). Entité financière bénéficiaire si distincte du Client : **[À COMPLÉTER : dénomination, LEI]**

	Pour le Client	**Pour le Sous-traitant (Cryptaguard BV)**
Nom	**[À COMPLÉTER]**	Matthieu Roland
Fonction	**[À COMPLÉTER]**	Administrateur
Date		
Signature		

Annexe 1 — Description du traitement (art. 28(3) RGPD)

Objet du traitement. Fourniture, en mode SaaS, de la plateforme ResiPlan de gestion de la continuité d'activité et de la résilience opérationnelle : analyse d'impact métier (BIA), plans de continuité et de reprise, gestion des risques, inventaire des actifs et contrats (CMDB), conformité réglementaire (ISO 22301, DORA, NIS2), exercices et gestion de crise, avec fonctions optionnelles d'assistance par intelligence artificielle.

Durée du traitement. Durée du Contrat principal, augmentée du délai de restitution/suppression prévu à l'article 5.8.

Nature du traitement. Hébergement, stockage, structuration, consultation, modification, export, transmission (notifications), suppression ; transcription audio le cas échéant ; génération de contenus assistée par IA le cas échéant.

Finalités. Permettre au Client de constituer, exploiter et démontrer son dispositif de continuité d'activité et de conformité.

Catégories de personnes concernées.

- utilisateurs du Service désignés par le Client (employés, dirigeants, prestataires) ;
- membres des cellules et équipes de crise du Client, y compris leurs suppléants ;
- contacts professionnels de tiers renseignés par le Client (fournisseurs, clients, parties prenantes, contacts d'escalade) ;
- toute personne mentionnée par le Client dans des contenus libres (déclarations d'incidents, comptes rendus d'exercices, plans, documents importés) ;
- participants aux séances de crise enregistrées, lorsque le Client active la captation (article 5.10).

Catégories de données à caractère personnel.

- identification et coordonnées professionnelles : nom, prénom, adresse email, numéros de téléphone (notamment pour les annuaires de crise), fonction, rôle, organisation ;
- données de compte et d'usage : identifiants, journaux de connexion et d'audit (horodatage, adresse IP, actions) ;
- contenus métier libres susceptibles de mentionner des personnes : incidents, risques, plans, exercices, commentaires, documents importés ;
- enregistrements audio et transcriptions des séances de crise, **uniquement si le Client active cette fonction** (article 5.10).

Catégories particulières de données (art. 9 RGPD). Régime de l'article 6.3 : pas de traitement systématique ou structuré ; mentions incidentes couvertes.

Traitements propres du Sous-traitant. Les traitements que le Sous-traitant réalise en qualité de responsable du traitement — facturation et gestion du contrat (via son prestataire de paiement), gestion de la relation commerciale, mesure d'audience de son site — sont décrits dans sa politique de confidentialité et ne relèvent pas du présent DPA.

Annexe 2 — Mesures techniques et organisationnelles (art. 32 RGPD)

Les mesures ci-dessous sont en vigueur à la date de signature ; elles peuvent évoluer sans réduction du niveau de protection global (article 5.3).

Chiffrement et réseau

- chiffrement en transit : TLS 1.2 minimum, TLS 1.3 pris en charge, sur l'ensemble des accès au Service ; HSTS activé ;
- chiffrement au repos (AES-256) sur la base de données et le stockage de fichiers ; les serveurs applicatifs ne conservent pas de données client de manière persistante — les fichiers temporaires de transcription locale sont supprimés à l'issue du traitement ;
- en-têtes de sécurité HTTP (CSP, X-Frame-Options, X-Content-Type-Options) vérifiés en production par des tests automatisés.

Contrôle d'accès et authentification

- authentification par mot de passe avec politique de robustesse, connexion fédérée (OAuth) et lien magique ;
- authentification à deux facteurs TOTP (RFC 6238) avec codes de récupération : enrôlement imposé aux comptes d'administration de la plateforme, activation disponible pour tout compte ;
- sessions en cookies sécurisés (`__Host-`, HttpOnly, SameSite), rotation de jetons, révocation à distance ;
- contrôle d'accès par rôles à deux niveaux (plateforme / organisation : administrateur, gestionnaire, utilisateur, lecteur), vérifié côté serveur sur chaque fonction.

Cloisonnement multi-locataire

- chaque requête serveur est filtrée par l'identifiant d'organisation via des index dédiés et des contrôles d'appartenance systématiques ;
- tout accès inter-locataires par un administrateur de plateforme est journalisé et signalé par une bannière d'avertissement persistante.

Journalisation et détection

- journal d'audit **chaîné cryptographiquement (SHA-256)** couvrant les créations, modifications, suppressions, événements d'authentification et de sécurité, avec états avant/après : toute altération est détectable ;
- conservation par défaut du journal d'audit applicatif : 7 ans (réduite sur demande, minimum 1 an) ; les événements de sécurité à fort volume sont archivés à froid après 90 jours, avec préservation de la chaîne d'intégrité ; les journaux techniques d'accès serveur sont conservés 12 mois ;
- détection automatique d'anomalies : force brute, bourrage d'identifiants, connexion depuis un pays inhabituel ;
- surveillance des erreurs et performances réalisée **en interne** (aucun prestataire tiers de suivi d'erreurs applicatives).

Sécurité applicative et des API

- limitation de débit sur les points d'accès, protection CSRF, assainissement des entrées (neutralisation HTML/scripts) ;

- clés d'API émises pour le Client hachées au repos (SHA-256), portées par périmètre ;
- vérification de signature HMAC et protection anti-rejeu (fenêtre temporelle) sur les webhooks ;
- secrets de production stockés hors du code, générés par générateur cryptographique.

Fonctions d'IA

- limites d'entrée strictes et cloisonnement par organisation des contextes transmis ;
- aucune utilisation des données du Client pour l'entraînement de modèles, interdiction imposée contractuellement aux fournisseurs d'IA en qualité de sous-traitants ultérieurs (article 5.4.3) ;
- journalisation des consommations IA par organisation.

Organisation et continuité

- développement soumis à revue de code, tests automatisés (unitaires, bout-en-bout, tests de sécurité OWASP) et analyse statique ;
- sauvegardes gérées par l'infrastructure de la base de données et déploiements par instantanés permettant le retour arrière ; procédure de restauration testée au moins **[À VALIDER : une fois par an]** ;
- procédure publique de signalement des vulnérabilités conforme à la RFC 9116 (`/.well-known/security.txt`) ;
- politique de moindre privilège pour le personnel du Sous-traitant ; accès de production restreint.

Annexe 3 — Sous-traitants ultérieurs autorisés

Liste en vigueur à la date de signature (article 5.4 ; notification préalable de 30 jours — 60 jours en chaîne de sous-traitance — pour tout changement). La liste à jour est publiée en permanence sur la page de transparence du Service (`/trust`).

Sous-traitant ultérieur	Finalité	Données concernées	Localisation des données	Garanties de transfert
Convex (Convex, Inc., États-Unis)	Base de données, fonctions serverless, synchronisation temps réel et stockage de fichiers	Toutes les données métier et de compte du Service	Union européenne — AWS eu-west-1 (Irlande), déploiement dédié UE	Données hébergées en UE ; accès de support depuis les États-Unis encadré par CCT (2021/914)
OVHcloud (OVH SAS, France)	Hébergement applicatif (serveur web du Service)	Données en transit et journaux techniques du serveur	Union européenne — France	Aucun transfert hors UE
Resend (Resend, Inc., États-Unis)	Envoi d'emails transactionnels (invitations, notifications, alertes)	Adresses email, contenu des emails envoyés	États-Unis	CCT (2021/914)
Anthropic (Anthropic, PBC, États-Unis)	Fournisseur IA par défaut (assistant, génération de plans, analyses) — sans entraînement sur les données client	Contenu contextuel des requêtes IA (extraits des données de l'organisation nécessaires à la requête)	États-Unis	CCT (2021/914) et, le cas échéant, certification DPF active ; option « IA UE seulement » disponible par organisation
OpenAI (OpenAI, L.L.C., États-Unis)	Fonctions IA sélectionnées et transcription cloud optionnelle des séances de crise (alternative locale disponible)	Contenu contextuel des requêtes IA ; enregistrements audio des séances de crise uniquement si la transcription cloud est activée	États-Unis	CCT (2021/914) et, le cas échéant, certification DPF active ; option « IA UE seulement » disponible par organisation
Mistral AI (Mistral AI, France)	Option « IA UE seulement » : fournisseur IA de substitution configurable par organisation	Contenu contextuel des requêtes IA lorsque l'organisation choisit cette option	Union européenne — France	Aucun transfert hors UE
Plausible Analytics (Plausible Insights OÜ, Estonie)	Mesure d'audience agrégée et sans cookie (site et application)	Statistiques de fréquentation agrégées (pages vues, référent) ; adresse IP traitée en transit pour le comptage, non conservée	Union européenne	Aucun transfert hors UE

Chaîne de sous-traitance TIC (au sens du registre d'information DORA) : rang 1 — les prestataires du tableau ci-dessus ; rang 2 — Amazon Web Services EMEA SARL (infrastructure d'hébergement du prestataire de base de données Convex, région eu-west-1, Irlande).

Les intégrations que le Client choisit de connecter à ses propres outils (Slack, Microsoft Teams, Discord, SharePoint, webhooks sortants) transmettent des données aux services **du Client** : ces éditeurs agissent alors comme destinataires ou sous-traitants du Client, non du Sous-traitant.

Annexe 4 — Transferts hors Union européenne

Localisation par défaut. Les données du Service sont hébergées en Union européenne : base de données et stockage de fichiers sur le déploiement européen dédié du Sous-traitant (AWS eu-west-1, Irlande) ; serveurs applicatifs en France.

Transferts encadrés. Certains sous-traitants ultérieurs listés en Annexe 3 sont établis aux États-Unis ou peuvent y accéder aux données. Pour chacun de ces transferts, le Sous-traitant met en œuvre :

- les **Clauses Contractuelles Types** de la Commission européenne (décision d'exécution (UE) 2021/914, modules applicables), en tant que garantie principale ;
- le cas échéant, la **certification active au cadre de protection des données UE–États-Unis (DPF)** du destinataire, vérifiée à la date de signature ;
- pour les données stockées : chiffrement en transit et au repos ;
- pour les requêtes adressées aux fournisseurs d'IA (traitées en clair par nature) : **minimisation stricte** (seul le contexte nécessaire à la requête est transmis), interdiction contractuelle d'entraînement, et rétention nulle ou strictement limitée chez le fournisseur **[À VALIDER : option « zéro rétention » souscrite auprès des fournisseurs d'IA]** ;
- une évaluation des risques de transfert documentée, communiquée au Client sur demande.

Option « IA en Union européenne seulement ». Élection formelle à l'article 10. Lorsqu'elle est souscrite, les fonctions d'IA de l'organisation du Client sont configurées sur le fournisseur européen listé en Annexe 3 (Mistral AI, France) et la transcription des séances de crise est exécutée localement ou en UE. Quatre fonctions reposant sur des capacités propres au fournisseur par défaut (analyse de conformité documentaire, veille réglementaire, import d'organigramme, cartographie assistée) sont alors indisponibles et exclues du périmètre d'utilisation ; le Sous-traitant confirme par écrit la configuration appliquée. Dans cette configuration, les fournisseurs d'IA établis hors UE sont réputés retirés de l'Annexe 3 pour l'organisation du Client.

Divulgation aux autorités de pays tiers. Le Sous-traitant notifie le Client, sauf interdiction légale, de toute demande d'accès contraignante émanant d'une autorité d'un pays tiers, la conteste dans la mesure raisonnable et ne communique que le minimum requis.

Annexe 5 — Stipulations DORA (art. 30 du Règlement (UE) 2022/2554)

Champ d'application. La présente annexe s'applique lorsque le Client est une entité financière au sens de DORA ou souscrit le Service pour le compte d'une telle entité. Le Service constitue alors un service TIC fourni par un prestataire tiers de services TIC ; le Client détermine, sous sa responsabilité, si le Service **soutient une fonction critique ou importante** (« FCI ») au sens de l'article 3, point 22, de DORA, et le notifie par écrit au Sous-traitant (ou coche l'élection de l'article 10). À compter de la réception de la notification, les stipulations du point B s'appliquent immédiatement ; les Parties formalisent les paramètres ouverts (SLA du 30(3)(a), modalités du 30(3)(f)) dans un délai de 30 jours. Le Client peut notifier à tout moment un changement de statut FCI, avec les mêmes effets. La sous-traitance de services TIC soutenant une FCI est autorisée aux conditions de l'article 5.4 et de l'Annexe 3, complétées par la présente annexe.

Tiers bénéficiaire. Lorsque le Client agit pour le compte d'une entité financière désignée à l'article 10, cette entité — ainsi que ses autorités compétentes et de résolution — bénéficie directement et peut exercer directement à l'encontre du Sous-traitant l'ensemble des droits de la présente annexe (accès, inspection, audit sur place, participation aux TLPT, informations pour le registre d'information, droits de sortie), sans qu'aucune modification du présent DPA ne puisse réduire ces droits sans son accord.

Informations pour le registre d'information du Client (art. 28(3) DORA).

- Prestataire : Cryptaguard BV — BCE 1007.610.660 — identifiant : **[À VALIDER : LEI si attribué ; à défaut, EUID BEKBOBCE1007610660 (format BRIS)]** ;
- Type de service TIC (taxonomie de l'annexe III du règlement d'exécution (UE) 2024/2956) : **S19 — Cloud services: SaaS** (gestion de la continuité d'activité et de la résilience opérationnelle) ;
- Localisation de fourniture du service et des données : Union européenne (Irlande, France) pour l'hébergement applicatif et la base de données ; États-Unis pour l'envoi d'emails transactionnels et, par défaut, pour les fonctions d'IA (option « IA UE seulement » disponible) — détail en Annexes 3 et 4 ;
- Chaîne de sous-traitance avec rangs : Annexe 3 ; le Sous-traitant fournit sur demande les données au format des modèles du registre d'information (ITS (UE) 2024/2956).

A. Stipulations applicables à tout accord (art. 30(2))

Réf.	Exigence DORA	Mise en œuvre contractuelle
30(2)(a)	Description claire et exhaustive des fonctions et services TIC, y compris conditions de sous-traitance	Annexe 1 du présent DPA ; Contrat principal ; régime de sous-traitance ultérieure : article 5.4 et Annexe 3 ; autorisation conditionnée de la sous-traitance FCI : champ d'application ci-dessus
30(2)(b)	Localisations (régions ou pays) de fourniture du service et de traitement/stockage des données, avec notification préalable de tout changement	Annexes 3 et 4 ; notification préalable de 30 jours de tout changement de sous-traitant **ou de localisation**, y compris à prestataire constant (article 5.4.2)

Réf.	Exigence DORA	Mise en œuvre contractuelle
30(2)(c)	Dispositions sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données	Annexe 2 (chiffrement, contrôle d'accès, journal d'audit chaîné garantissant l'authenticité et l'intégrité, cloisonnement)
30(2)(d)	Accès, récupération et restitution des données à caractère personnel et non personnel en cas d'insolvabilité, de résolution, de cessation d'activité ou de résiliation	Article 5.8 : export en libre-service de l'ensemble des données, personnelles et non personnelles (PDF, Excel/CSV, DOCX, API/JSON), y compris pendant la période de transition et en cas d'insolvabilité ; restitution dans un format structuré, couramment utilisé et aisément accessible ; ces engagements survivent à l'ouverture de toute procédure d'insolvabilité du Sous-traitant
30(2)(e)	Description des niveaux de service, y compris leurs mises à jour et révisions	**[À COMPLÉTER : référence au SLA du Contrat principal ou à l'annexe SLA dédiée — disponibilité cible, fenêtres de maintenance, canaux et délais de support]**
30(2)(f)	Assistance en cas d'incident TIC lié au service, sans coût additionnel ou à coût déterminé ex ante	Le Sous-traitant fournit l'assistance liée à tout incident TIC affectant le Service **sans coût additionnel** (articles 5.6 et 5.7)
30(2)(g)	Coopération avec les autorités compétentes et les autorités de résolution du Client, y compris les personnes désignées par elles	Le Sous-traitant coopère pleinement avec les autorités compétentes et de résolution du Client, ainsi qu'avec les personnes qu'elles désignent, notamment en répondant à leurs demandes d'information relatives au Service
30(2)(h)	Droits de résiliation et préavis minimaux, conformément aux attentes des autorités compétentes et des autorités de résolution	Contrat principal **[À COMPLÉTER : référence]** et article 5.4.2 (résiliation sans pénalité avec remboursement prorata) ; le Client peut en outre résilier conformément à l'article 28 de DORA, notamment en cas de manquement grave, de circonstances révélant une déficience dans la gestion des risques TIC, ou de demande de son autorité compétente
30(2)(i)	Conditions de participation aux programmes de sensibilisation à la sécurité des TIC et aux formations à la résilience opérationnelle numérique du Client	Sur demande raisonnable du Client, le personnel concerné du Sous-traitant participe, à distance, aux actions de sensibilisation du Client relatives à l'usage du Service ; le Sous-traitant met à disposition sa documentation de formation

B. Stipulations additionnelles lorsque le Service soutient une fonction critique ou importante (art. 30(3))

Réf.	Exigence DORA	Mise en œuvre contractuelle
30(3)(a)	Niveaux de service complets, avec objectifs de performance quantitatifs et qualitatifs précis, actualisés	**[À COMPLÉTER : SLA chiffré — disponibilité mensuelle cible, RTO/RPO du Service, objectifs de temps de réponse du support, indicateurs de suivi et modalités de révision]**

Réf.	Exigence DORA	Mise en œuvre contractuelle
30(3)(b)	Préavis et obligations de notification du prestataire, y compris tout développement susceptible d'avoir une incidence significative sur sa capacité à fournir le service	Le Sous-traitant notifie au Client, sans délai injustifié, tout développement susceptible d'avoir une incidence significative sur le Service ou sur sa capacité à le fournir aux niveaux convenus — y compris incident majeur, changement de contrôle, difficulté financière majeure, perte d'un sous-traitant ou d'une certification clés, changement de sous-traitant ultérieur ou de localisation (préavis de 30 jours) — via les canaux de notification des articles 5.4.2 et 5.6
30(3)(c)	Mise en œuvre et test de plans d'urgence, et mesures de sécurité TIC appropriées au cadre réglementaire de l'entité financière	Le Sous-traitant maintient un plan de continuité et de reprise de sa propre exploitation (sauvegardes, instantanés de déploiement avec retour arrière, procédures de restauration) et le teste au moins **[À VALIDER : une fois par an]** ; mesures de sécurité : Annexe 2, maintenues à un niveau approprié au regard du cadre réglementaire applicable au Client tel que notifié au Sous-traitant
30(3)(d)	Participation aux tests de pénétration fondés sur la menace (TLPT) du Client (art. 26-27 DORA)	Le Sous-traitant participe et coopère pleinement aux TLPT du Client dans la mesure où le Service entre dans le périmètre du test, sans que l'absence d'accord préalable sur les modalités puisse retarder ou conditionner cette participation ; les coûts raisonnables et documentés sont refacturés **[À COMPLÉTER : conditions tarifaires déterminées ex ante]**
30(3)(e)	Droits de suivi continu : accès, inspection et audit illimités par l'entité financière, tout tiers désigné et l'autorité compétente, coopération pleine lors des inspections sur place (y compris du superviseur principal), précisions sur portée, procédures et fréquence	Par dérogation aux limites de l'article 5.9.2 — y compris la restriction sur le choix de l'auditeur —, l'entité financière (Client ou tiers bénéficiaire), tout tiers qu'elle désigne et ses autorités compétentes disposent de **droits illimités (sans restriction) d'accès, d'inspection et d'audit**, y compris sur place, avec droit de copie de la documentation pertinente ; le Sous-traitant coopère pleinement lors des inspections menées par l'entité, ses mandataires, ses autorités compétentes ou le superviseur principal, s'engage à fournir les précisions demandées sur la portée, les procédures et la fréquence de ces contrôles, et aucune limitation contractuelle de fréquence n'est opposable
30(3)(f)	Stratégies de sortie : période de transition adéquate avec maintien du service et assistance de migration, aux coûts déterminés ex ante	En cas de résiliation, le Sous-traitant maintient le Service pendant une période de transition de **[À VALIDER : 90]** jours à compter de la date d'effet, prolongeable jusqu'à **[À VALIDER : 12]** mois sur demande de l'entité financière, aux conditions tarifaires déterminées ex ante **[À COMPLÉTER : tarif de la période de transition et de l'assistance de migration]** ; il assure l'export intégral des données dans des formats ouverts et fournit une assistance de migration raisonnable ; aucune suppression par défaut n'intervient avant la fin de la période de transition (article 5.8.2) ; le Client peut tester sa stratégie de sortie sans que le Sous-traitant puisse s'y opposer

---

Document généré depuis le référentiel de conformité du Service. Les champs marqués « À COMPLÉTER » ou « À VALIDER » doivent être renseignés ou confirmés avant signature. Ce document constitue un projet de contrat et ne constitue pas un avis juridique.