ARTICLE 28 DU RGPD

Accord de traitement des données

Conditions dans lesquelles REVIEWIT SAS traite des données à caractère personnel pour le compte de ses clients dans le cadre de la solution REVIEWIT. Le présent accord est annexé au contrat principal et prévaut sur lui en matière de protection des données.

VERSION	PÉRIMÈTRE	REVUE
1.2 · Novembre 2026	**REVIEWIT SAS · solution SaaS REVIEWIT, toutes régions**	**Annuelle, et après tout changement majeur**

SOMMAIRE

– Parties
01 Objet
02 Description des traitements
03 Instructions documentées
04 Confidentialité
05 Sécurité
06 Sous-traitants ultérieurs
07 Assistance au Client
08 Violations de données
09 Conservation, restitution et effacement
10 Audits
11 Transferts hors de l'Union européenne
12 Intelligence artificielle (assistant RITA)
13 Durée et hiérarchie
A1–6 Annexes · Signatures

PARTIES

RESPONSABLE DU TRAITEMENT

Le Client

Dénomination

Siège

Immatriculation

Représenté par

SOUS-TRAITANT

REVIEWIT SAS

Siège

RCS · SIREN

Représentée par

Délégué à la protection des données : Marc Marie Aroquiassamy · dpo@we-reviewit.com

I Dispositions

ARTICLE 1 Objet

Le présent accord fixe les conditions dans lesquelles REVIEWIT traite des données à caractère personnel pour le compte du Client dans le cadre de la solution REVIEWIT, conformément à l'article 28 du règlement (UE) 2016/679 (RGPD). Il prévaut sur toute stipulation contraire du contrat principal en matière de protection des données.

ARTICLE 2 Description des traitements

Objet et durée	Fourniture de la solution REVIEWIT pendant la durée du contrat principal, puis restitution et effacement (annexe 3).
Nature et finalités	Collecte des identités, appartenances, ressources et droits d'accès ; organisation des revues d'accès ; production des preuves ; notifications ; piste d'audit et diffusion vers le SIEM du Client ; assistance par l'assistant RITA si le Client l'active ; support.
Catégories de personnes	Collaborateurs, prestataires, invités et administrateurs du Client ; réviseurs.
Catégories de données	Identité professionnelle, adresse e-mail professionnelle, statut du compte, appartenances, rôles, métadonnées de ressources, décisions et motifs, journaux d'audit (dont adresse IP). Aucune donnée sensible au sens de l'article 9 n'est attendue.
Localisation	Région d'hébergement choisie par le Client et inscrite aux conditions particulières (par défaut : Paris, Union européenne).

ARTICLE 3 Instructions documentées

REVIEWIT traite les données sur instruction documentée du Client. Constituent des instructions : le présent accord, le contrat principal et la configuration de la souscription par le Client (connecteurs et périmètres collectés, campagnes, profil de rétention, activation et réglage de l'assistant RITA, destinations SIEM). REVIEWIT informe immédiatement le Client si une instruction lui paraît constituer une violation du RGPD, et peut en suspendre l'exécution dans l'attente de sa confirmation.

ARTICLE 4 Confidentialité

Les personnes autorisées à traiter les données s'engagent à la confidentialité ou sont soumises à une obligation légale de confidentialité, et sont formées à la protection des données. L'accès du personnel de REVIEWIT aux données d'une souscription est limité au besoin, tracé dans la piste d'audit et, hors urgence, réalisé à la demande du Client.

ARTICLE 5 Sécurité

REVIEWIT met en œuvre les mesures techniques et organisationnelles décrites à l'annexe 1, qu'il maintient à jour. Il ne diminue pas le niveau de sécurité pendant la durée du contrat.

ARTICLE 6 Sous-traitants ultérieurs

Le Client donne une autorisation générale de recours aux sous-traitants ultérieurs listés à l'annexe 2. REVIEWIT informe le Client de tout ajout ou remplacement au moins trente jours à l'avance ; lorsque le changement est décidé par un sous-traitant ultérieur avec un préavis plus court, REVIEWIT en informe le Client dès qu'il en a connaissance. Le Client peut s'y opposer pour un motif légitime lié à la protection des données et, à défaut d'accord, résilier le service concerné sans pénalité.

REVIEWIT impose à chaque sous-traitant ultérieur des obligations de protection des données au moins équivalentes à celles du présent accord, compte tenu de la nature du service, et reste responsable devant le Client de leur exécution.

ARTICLE 7 Assistance au Client

- **Droits des personnes.** Toute demande reçue par REVIEWIT est transmise au Client dans les deux jours ouvrés ; REVIEWIT fournit l'assistance technique nécessaire dans un délai de cinq (5) jours ouvrés.
- **Analyses d'impact.** REVIEWIT fournit un dossier AIPD (flux, mesures, sous-traitants, durées, transferts) et répond aux questions du Client.
- **Sécurité, violations et consultation préalable de l'autorité.** Selon les articles 5 et 8.

ARTICLE 8 Violations de données

REVIEWIT notifie au Client toute violation de données à caractère personnel le concernant au plus tard **vingt-quatre heures** après en avoir pris connaissance, par courriel au contact désigné aux conditions particulières et par l'espace de support. Ce délai s'applique aussi lorsque la violation survient chez un sous-traitant ultérieur : il court à compter de la connaissance qu'en a REVIEWIT, qui n'attend pas la notification du sous-traitant ultérieur pour informer le Client.

La notification comporte, dans la mesure où elles sont connues, les informations de l'article 33.3 du RGPD ; elle est complétée au fil de l'enquête sans attendre sa clôture. REVIEWIT prend sans délai les mesures de confinement et coopère avec le Client pour ses propres notifications.

ARTICLE 9 Conservation, restitution et effacement

Les durées de conservation, la suspension de la purge, la fin de contrat, la réversibilité, l'attestation de suppression et les droits des personnes sur les données conservées sont régis par la clause « Rétention et réversibilité » version 1.2 (annexe 3), qui fait partie intégrante du présent accord, y compris ses dispositions transitoires.

ARTICLE 10 Audits

REVIEWIT met à la disposition du Client les informations nécessaires pour démontrer le respect du présent accord : dossier d'assurance (mesures, sous-traitants, rapports disponibles). Le Client peut, une fois par an et avec un préavis de trente jours, réaliser ou faire réaliser par un auditeur tenu au secret un audit documentaire ou sur place de REVIEWIT, dans des conditions qui préservent la sécurité et la confidentialité des autres clients. Chaque partie supporte ses propres frais d'audit. Le temps que REVIEWIT consacre aux audits au-delà de deux jours par an est facturé au Client au tarif du bon de commande, sauf lorsque l'audit fait suite à un incident ou à un manquement de REVIEWIT.

Pour les sous-traitants ultérieurs, la vérification s'exerce au moyen des rapports et certifications de tiers indépendants qu'ils publient (notamment ISO/IEC 27001 et SOC 2), que REVIEWIT communique au Client sur demande dans la limite de leurs conditions de confidentialité ; les sous-traitants ultérieurs d'infrastructure n'admettent pas d'inspection sur place par leurs clients.

ARTICLE 11 Transferts hors de l'Union européenne

Les données sont hébergées dans la région choisie par le Client. Aucun transfert hors de l'Union européenne n'est réalisé en dehors de ceux mentionnés à l'annexe 2, chacun avec son mécanisme : décision d'adéquation (Data Privacy Framework, pour les entités certifiées) et clauses contractuelles types de la Commission (décision 2021/914), complétées par les mesures issues de l'analyse d'impact des transferts. REVIEWIT informe le Client sans délai si un mécanisme cesse de s'appliquer, notamment en cas d'invalidation de la décision d'adéquation.

ARTICLE 12 Intelligence artificielle (assistant RITA)

- RITA est désactivable ; le mode « IA générative » n'est actif que si le Client l'active, dans la limite fixée par l'avenant de traitement IA (annexe 4).

- En mode IA, les données ne sont transmises qu'à une route autorisée : AWS Bedrock dans la région de la souscription, avec un profil d'inférence limité à sa géographie ; ou, si le Client le choisit expressément, un fournisseur en appel direct, seulement après signature par REVIEWIT d'un accord de traitement, d'un engagement de non-entraînement et, hors Union européenne, d'une analyse d'impact des transferts.
- Ni REVIEWIT ni ses fournisseurs n'utilisent les données du Client pour entraîner des modèles.
- REVIEWIT ne conserve pas les conversations ; la piste d'audit garde une empreinte de chaque question (douze mois) ; le journal de diagnostic des questions de données est purgé à trente jours.
- RITA ne prend, ne recommande ni ne rédige aucune décision de revue.

ARTICLE 13 Durée et hiérarchie

Le présent accord produit ses effets pendant la durée du contrat principal et tant que REVIEWIT détient des données du Client. En cas de contradiction, le présent accord prévaut sur le contrat principal pour ce qui concerne la protection des données ; l'annexe 3 prévaut sur l'article 9.

Les annexes 5 et 6 prévalent sur le contrat principal pour leur objet. Elles complètent les articles 1 à 13 et les annexes 1 à 4 sans les modifier ; en cas de contradiction, ceux-ci prévalent pour la protection des données à caractère personnel, sous deux réserves : l'article 25 de l'annexe 5 aménage l'article 10 pour le Client relevant de sa section B2, et l'annexe 6 précise, pour la sortie du Client, les articles 6 et 7 de l'annexe 3 et prévaut sur eux.

II Annexes

ANNEXE 1 Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles sont décrites dans le document « Annexe des mesures de sécurité » (RGPD-T04), dans sa version en vigueur à la date de signature, joint au présent accord.

ANNEXE 2 Sous-traitants ultérieurs

SOUS-TRAITANT	SERVICE	LOCALISATION	MÉCANISME DE TRANSFERT
Amazon Web Services EMEA SARL Luxembourg	Hébergement, bases de données, stockage ; envoi des notifications (Amazon SES) ; modèles d'IA (Amazon Bedrock, seulement si le Client active le mode IA de RITA)	Région choisie par le Client (Union européenne ; Paris par défaut)	Aucun transfert : données stockées et traitées dans la région. Accès ponctuel possible depuis un pays tiers pour le support : Data Privacy Framework (Amazon Web Services, Inc.) et clauses contractuelles types 2021/914
Scaleway SAS Paris	Envoi des notifications par courriel	France	Aucun transfert
Microsoft Ireland Operations Ltd	Messagerie du support (échanges avec le Client)	France (région du tenant), frontière des données de l'UE	Data Privacy Framework et clauses contractuelles types 2021/914, module 3

Les fournisseurs d'IA en appel direct (Anthropic, OpenAI, Mistral AI) ne deviennent sous-traitants ultérieurs que si le Client choisit expressément une telle route dans l'avenant de traitement IA (annexe 4), après la signature par REVIEWIT d'un accord de traitement, d'un engagement de non-entraînement et, hors de l'Union européenne, d'une analyse d'impact des transferts. À la date de publication, aucune de ces routes directes n'est ouverte. Les prestataires de REVIEWIT qui ne traitent pas les données du Client ne figurent pas dans cette annexe.

ANNEXE 3 Clause « Rétention et réversibilité »

Version 1.2 du 5 septembre 2026, jointe en intégralité au présent accord, y compris son annexe A (durées de conservation par catégorie, profil Standard).

La suspension prévue à l'article 11 de la clause est levée avant la signature du présent accord, par l'information écrite prévue à son article 11.5.

ANNEXE 4

Avenant de traitement IA

À compléter uniquement si le Client active le mode IA de l'assistant RITA.

Mode autorisé	_____
Famille de modèles et route	_____ Amazon Bedrock, région et profil de sa géographie (« eu. » en Europe) ; ou appel direct
Conservation des conversations	Aucune : les conversations ne sont jamais conservées
Date d'activation	_____
Signataire du Client	_____

ANNEXE 5

Sécurité des services et résilience opérationnelle numérique (NIS 2, DORA)

Engagements de REVIEWIT SAS envers les clients soumis à la directive (UE) 2022/2555 (NIS 2) et au règlement (UE) 2022/2554 (DORA). La présente annexe complète l'accord de traitement des données et ne le remplace pas.

Fondements : Directive (UE) 2022/2555 (NIS 2), articles 21 et 23 ; règlement (UE) 2022/2554 (DORA), articles 28 à 30.

Dispositions générales

Article 1 — Objet et champ d'application

1.1 La présente annexe complète l'accord de traitement des données (le « DPA ») conclu entre le Client et REVIEWIT. Elle fixe les engagements de REVIEWIT relatifs à la sécurité du Service et à la résilience opérationnelle numérique, que le Client doit obtenir de ses fournisseurs en application de la directive (UE) 2022/2555 (« NIS 2 »), telle que transposée dans l'État membre dont il relève, et du règlement (UE) 2022/2554 (« DORA »).

1.2 Le volet A s'applique lorsque le Client déclare, aux conditions particulières, être une entité essentielle ou importante au sens de NIS 2, ou une entité financière au sens de l'article 2 de DORA.

1.3 Le volet B s'applique en outre lorsque le Client déclare être une entité financière au sens de DORA. Sa section B2 s'applique lorsque le Client désigne par écrit le Service comme soutenant une fonction critique ou importante au sens de l'article 3, point 22, de DORA. Cette désignation relève du seul Client : REVIEWIT ne peut pas la refuser, mais peut demander les éléments qui la fondent. Lorsqu'elle intervient en cours de contrat, elle fait l'objet d'un avenant, qui peut réviser le prix ; REVIEWIT dispose alors d'un délai de trois mois à compter de la désignation pour se mettre en conformité avec la section B2.

1.4 Les engagements de la présente annexe portent sur toutes les données traitées par le Service pour le compte du Client, qu'elles soient ou non à caractère personnel.

1.5 La présente annexe est une obligation contractuelle de REVIEWIT envers des clients soumis à NIS 2 ou à DORA. Elle n'emporte aucune reconnaissance que REVIEWIT serait lui-même une entité essentielle ou importante au sens de NIS 2.

Article 2 — Définitions

Les termes définis au DPA conservent leur sens. Pour la présente annexe :

- **Service** : la solution SaaS REVIEWIT fournie au Client au titre du contrat principal, dans la région d'hébergement inscrite aux conditions particulières.
- **Incident de sécurité** : tout événement qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité du Service ou des données stockées, transmises ou traitées par lui.
- **Incident notifiable** : l'incident de sécurité défini à l'article 5.1.

- **Prise de connaissance** : le moment où REVIEWIT dispose d'un degré raisonnable de certitude qu'un incident de sécurité s'est produit ou se produit.
- **Fournisseur TIC** : tout prestataire de REVIEWIT dont le service concourt à la fourniture du Service, qu'il traite ou non des données du Client.
- **Jour ouvré** : au sens du contrat principal ; à défaut, du lundi au vendredi, hors jours fériés en France.
- **Entité financière**, **fonction critique ou importante**, **autorité compétente**, **test de pénétration fondé sur la menace (TLPT)** : au sens de DORA.

Article 3 — Articulation avec le DPA

3.1 La présente annexe complète le DPA sans le modifier et ne réduit aucun de ses engagements ni de ceux de ses annexes. En cas de contradiction avec le contrat principal, elle prévaut pour son objet ; pour la protection des données à caractère personnel, le DPA prévaut (DPA, art. 13).

3.2 Les violations de données à caractère personnel restent régies par l'article 8 du DPA : notification au plus tard vingt-quatre heures après la prise de connaissance, contenu de l'article 33.3 du RGPD, compléments au fil de l'enquête. Lorsqu'un même événement constitue à la fois une violation de données à caractère personnel et un incident notifiable, l'article 8 du DPA régit la notification de la violation et l'article 5 de la présente annexe s'applique en outre à l'incident ; la même échéance de vingt-quatre heures vaut pour les deux. Une même communication peut satisfaire aux deux si elle en réunit les contenus.

3.3 L'article 10 du DPA (audits) reste applicable dans tous les cas. Seul l'article 25 l'aménage, pour le Client relevant de la section B2 et pour le Service qui soutient la fonction critique ou importante.

3.4 Les mesures que l'annexe 1 du DPA qualifie de « Prévu » ne deviennent pas des engagements du fait de la présente annexe, sauf lorsqu'un de ses articles les stipule expressément.

Volet A — Sécurité de la chaîne d'approvisionnement (NIS 2)

Article 4 — Mesures de sécurité

4.1 REVIEWIT met en œuvre, pour le Service, les mesures techniques et organisationnelles décrites à l'annexe 1 du DPA et ne diminue pas le niveau de sécurité pendant la durée du contrat (DPA, art. 5). L'annexe 1 indique, mesure par mesure, si elle est en service, partielle ou prévue, afin que le Client apprécie la qualité des produits et des pratiques de cybersécurité de REVIEWIT, y compris de ses procédures de développement sécurisé (NIS 2, art. 21.3).

4.2 REVIEWIT maintient les pratiques de développement et de publication décrites à l'annexe 1 : analyse statique à chaque compilation, tests automatisés, images de conteneurs à étiquettes immuables analysées à la poussée et déployées par empreinte, manifeste de version scellé exigé pour le canal stable.

4.3 REVIEWIT communique au Client, à sa demande et au moins après chaque revue annuelle de l'annexe 1 : l'annexe 1 en vigueur et les changements d'état de ses mesures ; l'état de sa démarche de certification ; la synthèse du dernier test d'intrusion (art. 6.4). Il répond, une fois par période de douze mois et dans un délai raisonnable convenu avec le Client, au questionnaire de sécurité de celui-ci.

Article 5 — Notification des incidents de sécurité

5.1 **Incident notifiable.** Est notifiable tout incident de sécurité qui affecte le Service fourni au Client ou ses données et qui :

(a) rend le Service indisponible ou gravement dégradé pour le Client pendant plus de soixante minutes consécutives, hors maintenance programmée annoncée ;

(b) porte atteinte, de manière avérée ou probable, à l'intégrité, à l'authenticité ou à la confidentialité des données du Client, de sa piste d'audit ou des preuves produites par le Service ;

(c) résulte d'un accès non autorisé, avéré ou probable, aux systèmes de production de REVIEWIT ou d'un fournisseur TIC ; ou

(d) constitue une menace dont REVIEWIT estime de bonne foi qu'elle peut conduire à brève échéance à l'un des cas précédents.

En cas de doute sur le caractère notifiable d'un incident, REVIEWIT le notifie.

5.2 **Alerte sous vingt-quatre heures.** REVIEWIT adresse au Client une alerte au plus tard vingt-quatre heures après la prise de connaissance. Elle indique, dans la mesure où ils sont connus : la nature de l'incident ; ses dates de début et de détection ; les fonctions du Service et les catégories de données affectées ; si l'incident paraît causé par un acte illicite ou malveillant ; s'il est susceptible d'affecter d'autres clients ou d'avoir un impact transfrontière ; les premières mesures prises ; le contact chargé du suivi. L'alerte n'attend ni la confirmation de la cause, ni la notification d'un fournisseur TIC.

5.3 **Mise à jour sous soixante-douze heures.** Au plus tard soixante-douze heures après la prise de connaissance, REVIEWIT adresse une mise à jour qui donne l'évaluation initiale de l'incident, sa gravité, son impact et, lorsqu'ils sont disponibles, les indicateurs de compromission.

5.4 **Points d'étape.** À la demande du Client, notamment lorsqu'une autorité compétente le lui demande, REVIEWIT fournit un point d'étape sur l'état de l'incident et de son traitement.

5.5 **Rapport final sous un mois.** Au plus tard un mois après l'alerte, REVIEWIT remet un rapport final : description détaillée de l'incident, de sa gravité et de son impact ; type de menace ou cause première probable ; mesures d'atténuation appliquées et en cours ; impact transfrontière, le cas échéant. Si l'incident est encore en cours à cette date, REVIEWIT remet un rapport d'avancement, puis le rapport final au plus tard un mois après la fin du traitement de l'incident.

5.6 **Canal.** Les communications partent de l'adresse security@we-reviewit.com vers le contact de sécurité désigné par le Client (art. 9.2) et sont doublées dans l'espace de support.

5.7 **Limites.** REVIEWIT peut ne pas communiquer une information qui révélerait les données d'un autre client ou compromettrait l'enquête ou la sécurité du Service. Il le signale au Client et, lorsque l'information est requise par une autorité compétente, la lui communique directement.

5.8 **Conduite de l'incident.** REVIEWIT prend sans délai les mesures de confinement, conserve les éléments de preuve utiles et coopère avec le Client pour ses propres notifications aux autorités (NIS 2, art. 23 ; DORA, art. 19). Les délais du présent article sont des délais maximaux : REVIEWIT informe plus tôt lorsqu'il le peut.

5.9 **Réciprocité.** Le Client informe REVIEWIT sans retard injustifié de tout incident survenu chez lui qui peut affecter le Service, notamment la compromission d'un compte d'administration de la souscription ou d'un fournisseur d'identité raccordé.

Article 6 — Gestion des vulnérabilités

6.1 REVIEWIT surveille les vulnérabilités des composants du Service (code, dépendances, images de conteneurs, configuration de l'infrastructure), les qualifie selon leur gravité et leur exploitabilité, et les corrige ou les atténue, à compter de leur qualification, dans les délais suivants : vulnérabilité critique, quatorze jours ; vulnérabilité élevée, trente jours ; autres vulnérabilités, dans le cycle normal de publication.

6.2 Lorsqu'une vulnérabilité exploitée ou exploitable affecte le Service et ne peut être corrigée dans ces délais, REVIEWIT en informe le Client, avec les mesures d'atténuation appliquées et, le cas échéant, celles que le Client peut prendre de son côté. Une vulnérabilité exploitée qui produit un incident notifiable relève de l'article 5.

6.3 REVIEWIT reçoit les signalements de vulnérabilités à l'adresse security@we-reviewit.com, en accuse réception et les traite selon une politique de divulgation coordonnée qu'il publie.

6.4 REVIEWIT fait réaliser chaque année un test d'intrusion du Service par un tiers indépendant, le premier au plus tard le 30 juin 2027. Il communique au Client, sur demande et sous confidentialité, une synthèse des résultats et l'état de correction des vulnérabilités relevées.

Article 7 — Sous-traitants et fournisseurs TIC

7.1 Les sous-traitants ultérieurs qui traitent des données à caractère personnel du Client sont listés à l'annexe 2 du DPA ; leur ajout ou leur remplacement suit l'article 6 du DPA.

7.2 REVIEWIT met en outre à la disposition du Client la liste de ses prestataires informatiques, y compris ceux qui ne traitent aucune donnée du Client, avec leur identification, la nature du service rendu, le lieu des données, les transferts et leur criticité pour le Service (« Prestataires informatiques de REVIEWIT », publiée dans l'espace client du Trust Center et tenue à jour à chaque changement).

7.3 REVIEWIT évalue la sécurité de ses fournisseurs TIC avant de les retenir, puis au moins une fois par an, notamment au moyen de leurs certifications et rapports d'audit indépendants (DPA, art. 10, second alinéa), et tient compte, dans ce choix, de la qualité de leurs produits et de leurs pratiques de cybersécurité.

Article 8 — Coopération avec les autorités

8.1 REVIEWIT coopère avec les autorités compétentes et les centres de réponse aux incidents de sécurité informatique (CSIRT) dont relève le Client, lorsque le Client le lui demande pour satisfaire à ses obligations ou lorsque ces autorités le lui demandent, notamment en fournissant les informations relatives au Service nécessaires à leurs missions.

8.2 Sauf interdiction légale, REVIEWIT informe le Client de toute demande d'une autorité qui le concerne. Les demandes d'accès aux données à caractère personnel par une autorité d'un pays tiers relèvent de l'article 11 du DPA.

Article 9 — Points de contact

9.1 Pour REVIEWIT : incidents de sécurité et vulnérabilités, security@we-reviewit.com ; protection des données et violations de données à caractère personnel, dpo@we-reviewit.com (DPA, art. 8) ; et l'espace de support.

9.2 Le Client désigne aux conditions particulières un contact de sécurité et le tient à jour. Une communication adressée à ce contact vaut communication au Client.

9.3 REVIEWIT relève l'adresse de sécurité chaque jour ouvré, puis chaque jour dès la mise en place d'une astreinte.

Volet B — Résilience opérationnelle numérique (DORA)

Section B1 — Dispositions applicables à toute entité financière (DORA, art. 30.2)

Article 10 — Description du Service et sous-traitance (art. 30.2.a)

10.1 Le Service, ses fonctions et les prestations associées sont décrits au contrat principal et à l'article 2 du DPA. Le contrat principal, le DPA, ses annexes et les conditions particulières forment l'écrit unique prévu à l'article 30.1 de DORA ; REVIEWIT le remet au Client sous une forme durable et téléchargeable.

10.2 La sous-traitance est admise dans les conditions de l'article 6 du DPA et de l'article 7 de la présente annexe. Pour une fonction critique ou importante, l'article 24 fixe des conditions supplémentaires.

Article 11 — Localisations (art. 30.2.b)

11.1 Le Service est fourni, et les données sont traitées et stockées, dans la région d'hébergement choisie par le Client et inscrite aux conditions particulières, par défaut Paris, Union européenne (DPA, art. 2 et 11). Les pays depuis lesquels les sous-traitants ultérieurs interviennent figurent à l'annexe 2 du DPA.

11.2 REVIEWIT ne change pas la région d'hébergement sans instruction du Client. Il informe le Client de tout changement de pays d'un sous-traitant ultérieur ou d'un fournisseur TIC au moins trente jours à l'avance, ou, lorsque le changement est décidé par ce prestataire avec un préavis plus court, dès qu'il en a connaissance (DPA, art. 6).

Article 12 — Protection des données (art. 30.2.c)

La disponibilité, l'authenticité, l'intégrité et la confidentialité des données, y compris à caractère personnel, sont assurées dans les conditions des articles 4, 5 et 8 du DPA, de son annexe 1 et des articles 4 à 6 de la présente annexe.

Article 13 — Accès, récupération et restitution (art. 30.2.d)

13.1 En cas de fin du contrat, quelle qu'en soit la cause, l'accès aux données, leur restitution dans un format facilement accessible et leur effacement suivent l'annexe 6.

13.2 En cas d'insolvabilité, de résolution ou de cessation d'activité de REVIEWIT, REVIEWIT, ou toute personne qui le représente, met à la disposition du Client, sans frais, le paquet de restitution défini à l'annexe 6 et en maintient l'accès pendant la période d'extraction qu'elle prévoit. REVIEWIT remet en outre chaque trimestre au Client relevant de la section B2 un paquet de restitution établi à partir d'une copie de ses données à cette date, dans les formats de l'article 6 de l'annexe 6.

Article 14 — Niveaux de service (art. 30.2.e)

14.1 Les niveaux de service sont décrits aux conditions particulières et, pour une fonction critique ou importante, à l'article 20. Ils couvrent au moins la disponibilité du Service, la maintenance programmée, la prise en compte des demandes de support et les délais de notification de l'article 5.

14.2 Toute révision des niveaux de service est faite par écrit. REVIEWIT ne les réduit pas pendant la durée du contrat sans l'accord du Client.

Article 15 — Assistance en cas d'incident lié aux TIC (art. 30.2.f)

Lorsqu'un incident lié au Service survient, REVIEWIT assiste le Client, notamment pour l'analyse, le confinement, le rétablissement et la préparation de ses notifications à l'autorité compétente, sans frais supplémentaires lorsque l'incident trouve son origine dans le Service et, sinon, au tarif fixé à l'avance aux conditions particulières.

Article 16 — Coopération avec les autorités (art. 30.2.g)

REVIEWIT coopère pleinement avec les autorités compétentes et les autorités de résolution dont relève le Client, ainsi qu'avec les personnes qu'elles désignent, notamment en répondant à leurs demandes d'information et, pour la section B2, en leur ouvrant les droits de l'article 25.

Article 17 — Résiliation (art. 30.2.h et 28.7)

17.1 Le Client peut résilier le contrat principal, par notification écrite et sans pénalité, dans chacun des cas suivants :

(a) violation significative, par REVIEWIT, des lois, règlements ou stipulations contractuelles applicables ;

(b) circonstances relevées lors du suivi du risque lié aux prestataires tiers de services TIC, jugées de nature à modifier l'exécution des fonctions fournies au titre du contrat, y compris des changements importants affectant le contrat ou la situation de REVIEWIT ;

(c) faiblesses avérées de REVIEWIT dans sa gestion globale du risque lié aux TIC, en particulier dans la manière dont il garantit la disponibilité, l'authenticité, l'intégrité et la confidentialité des données ;

(d) impossibilité pour l'autorité compétente de superviser effectivement le Client du fait des conditions ou des circonstances du contrat.

17.2 La résiliation prend effet à la date indiquée par le Client dans sa notification et ouvre la sortie prévue à l'annexe 6 ; pour une fonction critique ou importante, l'article 26 s'applique. Elle n'emporte aucune pénalité. La période d'abonnement prépayée non consommée à la date d'effet est remboursée au Client au prorata, que la résiliation résulte d'un manquement de REVIEWIT (cas a et c) ou d'un motif réglementaire sans faute de sa part (cas b et d). Les crédits prépayés restent acquis à REVIEWIT et ne sont pas remboursés.

17.3 Lorsque REVIEWIT met fin au contrat ou ne le renouvelle pas, hors manquement du Client, il respecte un préavis minimal de trois mois, porté à six mois lorsque le Service soutient une fonction critique ou importante.

17.4 Les autres cas de résiliation prévus au contrat principal demeurent.

Article 18 — Sensibilisation et formation (art. 30.2.i)

REVIEWIT participe, à la demande du Client, à ses programmes de sensibilisation à la sécurité des TIC et à ses formations à la résilience opérationnelle numérique (DORA, art. 13.6), à raison d'une session à distance par an sans frais, les sessions supplémentaires faisant l'objet d'un devis.

Article 19 — Registre d'information

REVIEWIT communique au Client les informations nécessaires à la tenue de son registre d'information (DORA, art. 28.3) : dénomination, identifiants, pays d'établissement, services fournis, localisations, chaîne de sous-traitance. Identifiant national : numéro d'immatriculation de REVIEWIT indiqué à la rubrique « Parties » du DPA. Identifiant

d'entité juridique : LEI, demandé dès l'immatriculation de REVIEWIT et communiqué au Client dès son obtention.

Section B2 — Fonctions critiques ou importantes (DORA, art. 30.3)

La présente section s'applique, en plus de la section B1, au Service désigné par le Client comme soutenant une fonction critique ou importante (art. 1.3).

Article 20 — Niveaux de service chiffrés (art. 30.3.a)

20.1 REVIEWIT s'engage sur les niveaux suivants, qui permettent au Client un suivi effectif et des mesures correctrices sans retard injustifié :

INDICATEUR	ENGAGEMENT	MESURE
Disponibilité mensuelle	99,5 %	Part des minutes du mois civil pendant lesquelles les consoles et l'API du Service répondent, mesurée par la page de statut publique de REVIEWIT (sondes externes sur chaque région provisionnée, agrégats journaliers publiés) ; hors maintenance programmée annoncée
Maintenance programmée	Préavis de cinq jours ouvrés ; quatre heures par mois au plus ; hors 8 h à 20 h, heure de la région	Annonce par courriel et dans l'espace de support
Prise en compte du support	Sévérité 1 : quatre heures ouvrées ; sévérité 2 : un jour ouvré ; sévérité 3 : trois jours ouvrés	Horodatage de l'espace de support
Perte de données maximale (RPO)	Vingt-quatre heures	Test de restauration (art. 22)
Délai maximal de rétablissement (RTO)	Quarante-huit heures	Test de restauration (art. 22)
Notification des incidents	24 h, 72 h, un mois (art. 5)	Horodatage des envois

20.2 Sévérité 1 : le Service ou une fonction essentielle est inutilisable, sans contournement. Sévérité 2 : le Service est dégradé ou une fonction est inutilisable avec contournement. Sévérité 3 : toute autre demande. Les heures ouvrées sont précisées aux conditions particulières.

20.3 Lorsqu'un niveau n'est pas atteint, REVIEWIT en analyse la cause et remet au Client, sans retard injustifié, un plan d'actions correctives. Un manquement répété constitue une circonstance au sens de l'article 17.1 (b).

20.4 La perte durable de la région d'hébergement est exclue des engagements chiffrés de perte de données maximale (RPO) et de délai maximal de rétablissement (RTO) ; elle est traitée dans le plan de continuité d'activité et de reprise de l'article 22. En option « Standard + DR », et sur instruction écrite du Client, REVIEWIT conserve une copie des sauvegardes dans une seconde région de la même géographie.

Article 21 — Préavis et rapports (art. 30.3.b)

21.1 REVIEWIT remet au Client un rapport de service trimestriel : niveaux mesurés, incidents, changements notables, état des actions correctives.

21.2 REVIEWIT notifie au Client, sans retard injustifié, tout développement susceptible d'avoir une incidence significative sur sa capacité à fournir le Service conformément aux niveaux convenus, notamment : changement de contrôle, ouverture d'une procédure collective, perte ou changement d'un fournisseur TIC critique, sanction ou injonction d'une autorité, incident majeur affectant ses moyens.

Article 22 — Continuité d'activité et sécurité (art. 30.3.c)

22.1 REVIEWIT établit, met en œuvre et teste au moins une fois par an un plan de continuité d'activité et de reprise couvrant le Service, qui comprend un test de restauration chronométré vérifiant le RPO et le RTO de l'article 20. Le premier test est réalisé avant la signature du premier contrat relevant de la présente section, et au plus tard le 30 juin 2027.

22.2 REVIEWIT communique au Client, sur demande, la synthèse du plan, les résultats du dernier test et les actions correctives décidées. À la demande du Client, il participe, dans des conditions convenues, aux tests de continuité du Client qui impliquent le Service.

22.3 REVIEWIT maintient les mesures, outils et politiques de sécurité de l'annexe 1 du DPA et des articles 4 à 6 de la présente annexe.

Article 23 — Tests de pénétration fondés sur la menace (art. 30.3.d)

23.1 Lorsque le Client est tenu de réaliser des TLPT au titre des articles 26 et 27 de DORA, REVIEWIT y participe et y coopère pleinement, à sa demande.

23.2 Le périmètre, les règles d'engagement, le calendrier et les mesures de protection des autres clients sont convenus par écrit avant le test. Lorsque le test pourrait affecter la qualité ou la sécurité des services fournis aux autres clients, ou la confidentialité de leurs données, REVIEWIT peut proposer un test groupé au sens de l'article 26.4 de DORA, mené par un testeur qu'il mandate.

23.3 Les tests respectent les conditions d'utilisation des fournisseurs d'infrastructure de REVIEWIT. REVIEWIT obtient auprès de l'hébergeur les autorisations nécessaires aux tests.

23.4 Les frais de la participation de REVIEWIT sont fixés par un devis accepté préalablement par le Client.

Article 24 — Sous-traitance d'une fonction critique ou importante

24.1 REVIEWIT tient à jour la liste des sous-traitants qui concourent au Service soutenant la fonction critique ou importante et la communique au Client.

24.2 REVIEWIT informe le Client au moins trente jours à l'avance de toute modification importante de cette chaîne de sous-traitance. Le Client peut s'y opposer et, à défaut d'accord, résilier sans pénalité (DPA, art. 6).

24.3 REVIEWIT surveille ses sous-traitants et répond de leur exécution devant le Client (DPA, art. 6).

24.4 Les sous-traitants d'infrastructure contractent à leurs conditions standard, qui ne sont pas négociables. REVIEWIT communique au Client leurs engagements, notamment leurs rapports d'audit indépendants et leurs accords de traitement des données.

Article 25 — Accès, inspection et audit (art. 30.3.e)

25.1 Par dérogation à la limite annuelle et au préavis de trente jours de l'article 10 du DPA, le Client, un tiers qu'il désigne et l'autorité compétente disposent sur REVIEWIT, pour le Service, d'un droit d'accès, d'inspection et d'audit sans restriction, y compris celui de prendre copie sur place de la documentation pertinente. REVIEWIT ne limite pas l'exercice effectif de ce droit par d'autres stipulations ni par ses politiques internes.

25.2 L'exercice de ce droit préserve la sécurité du Service et la confidentialité des données et informations des autres clients. Lorsqu'un audit porterait atteinte aux droits d'autres clients, les parties conviennent d'autres niveaux d'assurance, tels qu'un rapport de tiers indépendant ou un audit groupé, sans retarder l'audit au-delà du nécessaire.

25.3 Hors urgence et hors demande d'une autorité compétente, le Client annonce l'audit avec un préavis raisonnable de dix jours ouvrés. En cas d'urgence ou à la demande d'une autorité, l'audit peut avoir lieu avec un préavis court ou sans préavis.

25.4 REVIEWIT coopère pleinement aux inspections et audits, y compris sur place, conduits par l'autorité compétente, le superviseur principal, le Client ou le tiers désigné. Il précise à l'avance le périmètre, les modalités et la fréquence envisageables, sans que cette information restreigne le droit de l'article 25.1.

25.5 Pour les sous-traitants ultérieurs d'infrastructure, qui n'admettent pas d'inspection sur place par leurs clients, la vérification s'exerce au moyen de leurs rapports et certifications indépendants (DPA, art. 10).

25.6 La personne qui audite est tenue au secret. Chaque partie supporte ses propres frais d'audit. Le temps que REVIEWIT consacre aux audits au-delà de deux jours par an est facturé au Client au tarif du bon de commande, sauf lorsque l'audit fait suite à un incident ou à un manquement de REVIEWIT.

Article 26 — Stratégie de sortie (art. 30.3.f)

26.1 La sortie suit l'annexe 6. Pour une fonction critique ou importante, la période de transition est adéquate au sens de l'article 30.3.f de DORA : REVIEWIT continue d'y fournir le Service, afin de réduire le risque de perturbation chez le Client ou d'assurer sa résolution et sa restructuration, et le Client peut migrer vers un autre prestataire ou vers une solution interne, selon la complexité du Service.

26.2 Le Client peut, par notification, porter la période de transition jusqu'à six mois, le Service étant facturé au prorata aux conditions du contrat principal.

26.3 REVIEWIT apporte au plan de sortie du Client toute information utile (DORA, art. 28.8) et, à sa demande, le teste avec lui dans des conditions convenues.

Dispositions communes

Article 27 — Confidentialité

Les rapports d'incident, résultats de tests, rapports d'audit et rapports de service échangés au titre de la présente annexe sont confidentiels. Le Client peut les communiquer à ses autorités compétentes, à ses auditeurs et au tiers qu'il désigne, tenus au secret.

Article 28 — Durée et révision

28.1 La présente annexe produit ses effets pendant la durée du DPA (DPA, art. 13).

28.2 Elle est revue chaque année avec l'annexe 1, et après toute évolution de la transposition de NIS 2 dont relève le Client ou des normes techniques prises en application de DORA. Toute modification fait l'objet d'un écrit signé des deux parties.

ANNEXE 6

Changement de fournisseur, portabilité et sortie (Data Act)

Conditions dans lesquelles le Client quitte la solution REVIEWIT, emporte ses données et obtient leur effacement complet, conformément au chapitre VI du règlement (UE) 2023/2854. La présente annexe complète l'accord de traitement des données et ne le remplace pas.

Fondements : Règlement (UE) 2023/2854 (Data Act), chapitre VI, articles 23 à 31, et article 32 ; règlement (UE) 2016/679 (RGPD), article 28.3.g.

Dispositions générales

Article 1 — Objet et champ d'application

1.1 La présente annexe complète l'accord de traitement des données (le « DPA ») conclu entre le Client et REVIEWIT. Elle met en œuvre, pour le Service, le chapitre VI du règlement (UE) 2023/2854 (le « Data Act ») : changement de fournisseur de services de traitement de données, portabilité des données et des actifs numériques, et effacement à la sortie.

1.2 Elle s'applique à tout Client, quel que soit son lieu d'établissement, et quelle que soit la cause de la fin du contrat : changement de fournisseur, passage à une infrastructure sur site, résiliation, non-renouvellement ou effacement demandé par le Client.

Article 2 — Articulation avec le DPA et l'annexe 3

2.1 La clause « Rétention et réversibilité » version 1.2 (annexe 3 du DPA, la « clause ») régit la conservation des données pendant le contrat. La présente annexe précise ses articles 6 (fin de contrat et réversibilité) et 7 (attestation de suppression) pour la sortie du Client ; elle ne modifie pas ses autres articles.

2.2 Le DPA prévaut pour la protection des données à caractère personnel. La présente annexe ne réduit aucun de ses engagements ; elle prévaut sur le contrat principal pour son objet.

2.3 La suspension des articles 4, 6.2 et 7 de la clause, prévue à son article 11, est levée avant la signature du DPA, par l'information écrite prévue à son article 11.5 (DPA, annexe 3). Ces articles recouvrent ainsi leur plein effet.

Article 3 — Définitions

Les termes définis au DPA et dans la clause conservent leur sens. Pour la présente annexe :

- **Service** : la solution SaaS REVIEWIT fournie au Client au titre du contrat principal.
- **Changement de fournisseur** : le passage du Client du Service à un autre fournisseur de services de traitement de données, ou à une infrastructure TIC sur site, au sens du Data Act ; par extension, la sortie du Client assortie de l'effacement de ses données.
- **Données exportables** : les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement, ou cogénérées, par l'utilisation du Service par le Client, à l'exclusion des actifs ou données protégés par des droits de propriété intellectuelle ou constituant un secret des affaires de REVIEWIT ou de tiers.

- **Actifs numériques** : les éléments sous forme numérique, y compris les applications, dont le Client a le droit d'usage indépendamment du contrat.
- **Notification de sortie** : la demande écrite par laquelle le Client engage le changement de fournisseur.
- **Période de préavis** : la période qui sépare la réception de la notification de sortie du début de la période de transition.
- **Période de transition** : la période pendant laquelle le contrat reste applicable et le Service continue d'être fourni, afin que le Client effectue le changement.
- **J** : la date de fin de la période de transition, qui est la date de fin du contrat principal.
- **Paquet de restitution** : l'archive remise au Client, qui contient ses données exportables dans les formats de l'article 6, leur documentation et leur manifeste d'intégrité.
- **Archive d'export** : la copie technique des bases de la souscription, vérifiée par une restauration réelle, que REVIEWIT produit à J pour établir le paquet de restitution et prouver l'effacement ; elle n'est pas remise au Client.
- **Période d'extraction** : la période pendant laquelle le paquet de restitution final reste à la disposition du Client.
- **Frais de changement** : les frais, autres que les frais de service standard et les pénalités de résiliation anticipée, imposés au Client pour le changement de fournisseur, y compris les frais de sortie de données.

Déroulement de la sortie

Article 4 — Notification de sortie et préavis

4.1 Le Client notifie sa décision par écrit, par courriel au contact de REVIEWIT désigné aux conditions particulières et par l'espace de support. Il y indique l'option choisie :

(a) passer à un autre fournisseur de services de traitement de données, dont il communique les coordonnées utiles au changement ;

(b) passer à une infrastructure TIC sur site ;

(c) faire effacer ses données exportables et ses actifs numériques, sans changement de fournisseur.

4.2 La période de transition commence à la date choisie par le Client dans sa notification, au plus tard deux mois après la réception de celle-ci. À défaut de date, elle commence deux mois après cette réception.

4.3 REVIEWIT accuse réception de la notification sans retard injustifié et confirme au Client le calendrier qui en résulte : début et fin de la période de transition, J, période d'extraction, date d'effacement.

4.4 Lorsque le Client choisit l'option (c), il n'y a pas de période de transition : le contrat prend fin à l'expiration de la période de préavis, qui constitue alors J, et l'article 10.2 s'applique.

4.5 Lorsque la sortie intervient avant l'échéance du terme annuel en cours, le prix de ce terme reste dû, sans autre pénalité. Il n'est remboursé au prorata de la période non consommée que lorsque la sortie résulte d'un manquement de REVIEWIT, ou d'une résiliation pour motif réglementaire au titre de l'article 17 de l'annexe 5. Le prix ainsi dû rémunère le Service et n'est pas un frais de changement (art. 12.3).

Article 5 — Période de transition

5.1 La période de transition dure trente jours calendaires au plus. Le contrat principal reste applicable pendant toute sa durée.

5.2 Pendant la période de transition, REVIEWIT :

(a) fournit une assistance raisonnable au Client et aux tiers qu'il autorise, dans les conditions de l'article 7 ;

(b) agit avec la diligence requise pour assurer la continuité de l'activité, et continue de fournir les fonctions et services prévus au contrat ;

(c) informe clairement le Client des risques connus pour la continuité du Service ;

(d) maintient un niveau élevé de sécurité, notamment des données pendant leur transfert, puis pendant la période d'extraction.

5.3 À la demande du Client, REVIEWIT met à sa disposition, pendant la période de transition et sans interrompre le Service, un paquet de restitution intermédiaire établi à partir d'une copie des données à la date de la demande, dans les formats de l'article 6. Le paquet final, établi à J, fait foi.

5.4 Lorsque la période de trente jours est techniquement impossible à respecter, REVIEWIT le notifie au Client dans les quatorze jours ouvrés suivant la notification de sortie, justifie dûment l'impossibilité et indique une autre période de transition, qui ne peut excéder sept mois. La continuité du Service est assurée pendant toute cette période.

5.5 Le Client peut prolonger une fois la période de transition, pour la durée qu'il juge appropriée, par notification adressée avant son terme ; le Service continue alors aux conditions du contrat principal. Pour une fonction critique ou importante au sens de DORA, l'article 26 de l'annexe 5 s'applique.

Article 6 — Données exportables, formats et exclusions

6.1 **Liste exhaustive.** Les catégories de données exportables et d'actifs numériques que le Client peut emporter sont les suivantes :

CATÉGORIE	CONTENU	FORMAT
1. Annuaire collecté	Identités et comptes, groupes et appartenances, ressources et permissions collectées, couverture de collecte, compléments importés et absences confirmées, traces des fichiers importés	CSV et JSON
2. Comptes de la souscription	Rôles de workspace et attributions, préférences, progression des guides, acceptations des conditions d'utilisation, cycle de vie des comptes	CSV et JSON
3. Campagnes et revues	Périmètres figés, cohortes, évolutions et couverture de périmètre, demandes et éléments de revue, appartenances revues, décisions et motifs, affectations et leur historique, demandes d'avis, contestations, lots, simulations, alertes et constats	CSV et JSON
4. Délégations et exceptions	Délégations et leurs cibles, entrées du sanctuaire, demandes de suppression d'accès	CSV et JSON

5. Preuves et attestations	Attestations de revue et leur contenu, instantanés de scellement, clôtures de campagne, rapports émis	CSV et JSON
6. Actes d'administration	Éléments supprimés et restaurés, destinations de diffusion vers le SIEM	CSV et JSON
7. Assistant RITA	Invites enregistrées ; journal des questions de données, dans la limite de sa durée de conservation de trente jours (DPA, art. 12)	CSV et JSON
8. Notifications	Notifications émises par le Service	CSV et JSON
9. Piste d'audit	Événements (horodatage, acteur, action, résultat) avec leur séquence et leurs empreintes chaînées, tête de chaîne et sceaux signés ; adresse réseau tronquée (clause, art. 8.2 b)	CSV et JSON
10. Configuration de la souscription	Workspaces, solutions et connecteurs raccordés (sans leurs secrets), périmètres de collecte, définitions et modèles de campagnes, règles de certification, profil de rétention, réglages de RITA, destinations SIEM, modèles de courriels personnalisés	JSON
11. Documentation	Notice en français et en anglais (rubriques, colonnes, séparateur, encodage, procédure de vérification) ; manifeste donnant l'empreinte SHA-256 et le nombre de lignes de chaque fichier	Markdown et JSON

6.2 **Formats.** Le paquet de restitution est une archive ZIP. Les fichiers CSV sont encodés en UTF-8 avec indicateur d'ordre des octets, séparés par des points-virgules, entre guillemets selon la RFC 4180 ; les fichiers JSON sont encodés en UTF-8. Ces formats sont structurés, couramment utilisés et lisibles par machine. Les rubriques et colonnes portent des identifiants stables documentés dans la notice ; aucun nom interne de base, de table ou de colonne n'y figure.

6.3 **Exclusions.** Sont seuls exclus des données exportables :

(a) la structure interne des bases du Service (schémas, noms de bases, de tables et de colonnes) et l'archive d'export, propres au fonctionnement interne du Service et couvertes par le secret des affaires de REVIEWIT ; cette exclusion n'empêche ni ne retarde le changement de fournisseur, les données qu'elles contiennent figurant au paquet de restitution ;

(b) le code du Service et les catalogues, référentiels, guides et modèles standard fournis par REVIEWIT, protégés par ses droits de propriété intellectuelle ;

(c) les secrets d'authentification des connecteurs et les clés privées conservées dans le coffre de signature, jamais exportés pour des raisons de sécurité ; le Client conserve ses propres secrets et la clé qu'il a importée ;

(d) les données dont REVIEWIT est responsable du traitement (clause, art. 1.3) : journaux de sécurité de la plateforme, télémétrie technique, comptes internes, données contractuelles et comptables ;

(e) les conversations avec l'assistant RITA, que REVIEWIT ne conserve pas (DPA, art. 12).

Les exclusions (c) et (d) sont admises pour les raisons suivantes : au (c), le Client détient déjà ses propres secrets et la clé qu'il a importée, de sorte que l'exclusion n'empêche ni ne retarde le changement de fournisseur ; au (d), ces données n'entrent pas dans la définition des données exportables (art. 3).

6.4 **Vérification.** Le Client vérifie l'intégrité du paquet au moyen du manifeste, et celle de la piste d'audit au moyen de sa chaîne d'empreintes et de ses sceaux, selon la procédure décrite dans la notice.

Article 7 — Assistance et stratégie de sortie

7.1 REVIEWIT soutient la stratégie de sortie du Client et lui fournit toute information pertinente.

7.2 L'assistance raisonnable comprend : la remise des paquets intermédiaire et final ; l'explication des formats et de la procédure de vérification, y compris lors d'une réunion de travail avec le Client et le fournisseur de destination ; les réponses aux questions techniques sur les données exportées ; l'information sur les risques connus pour la continuité ; la coordination du calendrier de bascule.

7.3 REVIEWIT met gratuitement à la disposition du Client et du fournisseur de destination, dans les mêmes conditions pour tous, l'interface de programmation ouverte et documentée du Service en lecture, pour faciliter la portabilité des données.

7.4 Les prestations qui excèdent le changement de fournisseur, telles que la transformation des données dans un format propre au fournisseur de destination ou un développement spécifique, font l'objet d'un devis accepté par le Client.

Article 8 — Fin du contrat

8.1 Le contrat principal prend fin, et REVIEWIT en informe le Client par écrit :

(a) pour les options (a) et (b) de l'article 4.1, à la fin de la période de transition, le cas échéant prolongée ; le changement de fournisseur est réputé achevé à cette date, sauf si le Client notifie avant ce terme qu'il n'a pu l'achever du fait de REVIEWIT, auquel cas la période de transition est prolongée d'autant ;

(b) pour l'option (c), à l'expiration de la période de préavis.

8.2 À J, l'accès au Service prend fin. REVIEWIT produit l'archive d'export, la vérifie par une restauration réelle, établit le paquet de restitution final, puis supprime les bases de la souscription des systèmes actifs. L'export et la suppression sont approuvés par deux opérateurs distincts et tracés.

Article 9 — Période d'extraction

9.1 REVIEWIT met le paquet de restitution final à la disposition du Client au plus tard deux jours ouvrés après J. La période d'extraction court de cette mise à disposition et dure trente jours calendaires au moins.

9.2 Le paquet est remis par un lien de téléchargement signé, de courte durée de validité, envoyé au destinataire désigné par le Client. La remise est tracée (date, destinataire, empreinte du paquet) et renouvelée à la demande du Client pendant toute la période d'extraction.

9.3 Pendant la période d'extraction, le paquet et l'archive d'export sont conservés chiffrés dans la région d'hébergement du Client et ne font l'objet d'aucun autre traitement.

Article 10 — Effacement complet

10.1 À l'expiration de la période d'extraction, REVIEWIT efface l'archive d'export et le paquet de restitution, sauf instruction contraire du Client donnée selon l'article 11.

10.2 Lorsque le Client a choisi l'effacement (art. 4.1 c), REVIEWIT ne lui remet pas de paquet et efface l'archive d'export dès la fin du contrat, et au plus tard trente jours après J.

10.3 Les sauvegardes ne sont pas modifiées individuellement ; elles expirent selon leur cycle glissant de trente-cinq jours (clause, art. 3.2 et 3.6). L'effacement complet de toutes les données exportables et de tous les actifs numériques du Client est acquis au plus tard soixante-cinq jours après J ou, en cas de conservation prolongée, au plus tard trente-cinq jours après l'effacement de l'archive d'export.

10.4 Ne subsistent, après l'effacement complet, que les données que la clause permet de maintenir : données couvertes par une conservation opposable (clause, art. 6.3 et 6.4), données dont REVIEWIT est responsable du traitement (clause, art. 1.3), registre de suppression, qui ne contient aucun identifiant d'objet purgé, et l'attestation elle-même.

10.5 REVIEWIT remet au Client une attestation de suppression générée par la plateforme à partir de ses registres, conservée hors du cycle des sauvegardes : une attestation intermédiaire après l'effacement de l'archive d'export, puis une attestation complète après l'expiration des sauvegardes. Elle décrit le périmètre effacé et inventorie les données maintenues avec, pour chacune, son fondement, la restriction d'usage appliquée et sa prochaine échéance (clause, art. 7.2).

Article 11 — Conservation prolongée sur instruction du Client

11.1 REVIEWIT ne conserve aucune donnée du Client au-delà de la période d'extraction sans instruction écrite du Client.

11.2 Le Client peut demander, avant l'expiration de la période d'extraction, que l'archive d'export et le paquet de restitution soient conservés pour une durée qu'il fixe, notamment pour les besoins de ses propres audits, dans la limite du plafond de dix ans de l'article 2.3 de la clause. L'instruction est enregistrée avec son motif, sa durée, son approbateur et sa date de réexamen (clause, art. 2.4).

11.3 Pendant cette conservation, les données ne font l'objet d'aucun autre traitement que leur stockage chiffré dans la région d'hébergement et leur remise au Client sur demande, selon l'article 9.2. Le Client peut y mettre fin à tout moment ; REVIEWIT efface alors l'archive et le paquet dans les conditions de l'article 10.

11.4 Cette conservation est fournie sans frais.

Frais et information

Article 12 — Frais de changement

12.1 REVIEWIT n'impose au Client aucun frais de changement, y compris de sortie de données, pour un changement de fournisseur ou un effacement régi par la présente annexe, quelle que soit la date à laquelle il intervient.

12.2 Cet engagement s'applique dès la signature. Il va au-delà de l'article 29 du Data Act, qui interdit ces frais à compter du 12 janvier 2027 et les limite, d'ici là, aux coûts directement liés au changement.

12.3 Les frais de service standard dus pour le Service fourni pendant la période de transition ne sont pas des frais de changement.

Article 13 — Information du Client

13.1 REVIEWIT met à la disposition du Client, avant la conclusion du contrat et pendant celui-ci : les procédures disponibles pour le changement de fournisseur et la portabilité, avec les méthodes, les formats et les restrictions et limites techniques connues (la présente annexe et sa documentation) ; une référence à un

registre en ligne à jour, tenu par REVIEWIT, décrivant les structures et formats de données, ainsi que les normes et spécifications ouvertes d'interopérabilité pertinentes, dans lesquels les données exportables sont disponibles.

13.2 REVIEWIT publie sur son site la juridiction dont relève l'infrastructure TIC utilisée pour le Service, et une description générale des mesures techniques, organisationnelles et contractuelles adoptées pour empêcher l'accès des autorités publiques de pays tiers aux données non personnelles détenues dans l'Union, ou leur transfert, lorsqu'il serait contraire au droit de l'Union (Data Act, art. 28 et 32). Les transferts de données à caractère personnel restent régis par l'article 11 du DPA.

Article 14 — Bonne foi et sécurité

14.1 Les parties coopèrent de bonne foi, entre elles et avec le fournisseur de destination, pour que le changement soit effectif, réalisé en temps utile et sans interruption de l'activité du Client.

14.2 Les communications et remises prévues par la présente annexe sont tracées dans la piste d'audit de la plateforme.

Article 15 — Services exclus

15.1 Les souscriptions de démonstration, fournies en version de non-production, à des fins d'essai et d'évaluation et pour une durée limitée, ne relèvent pas du chapitre VI du Data Act (art. 31.2) ; REVIEWIT en informe le prospect avant la souscription.

15.2 Lorsqu'une prestation est développée sur mesure pour le Client, les conditions particulières précisent, avant la conclusion du contrat, les obligations de la présente annexe qui ne s'y appliquent pas (Data Act, art. 31.1 et 31.3).

Durée

Article 16 — Durée

La présente annexe produit ses effets pendant la durée du DPA et survit à la fin du contrat principal jusqu'à l'effacement complet et la remise de l'attestation complète (DPA, art. 13).

SIGNATURES

Approbation

POUR LE CLIENT

Nom _____

Qualité _____

Date _____

SIGNATURE

POUR REVIEWIT SAS

Nom _____

Qualité _____

Date _____

SIGNATURE

REVIEWIT SAS · Délégué à la protection des données : dpo@we-reviewit.com.
Le présent accord est revu annuellement et après tout changement majeur de la solution ou de ses sous-traitants ultérieurs.