DIRECTIVE (UE) 2022/2555 · RÈGLEMENT (UE) 2022/2554

Note NIS 2 et DORA à l'usage des clients assujettis

Ce que REVIEWIT SAS fournit aux clients soumis à la directive NIS 2 ou au règlement DORA pour remplir leurs obligations envers leurs prestataires (notification des incidents, registre d'information, audit, sortie, tests). Le texte qui fait foi est l'annexe 5 de l'accord de traitement des données.

VERSION
1.0 · Novembre 2026

PÉRIMÈTRE
REVIEWIT SAS · solution SaaS REVIEWIT, toutes régions

DIFFUSION
Public

SOMMAIRE

01 Quand l'annexe 5 s'applique
02 Notification des incidents
03 Sécurité de la chaîne d'approvisionnement
04 Registre d'information (DORA, art. 28)
05 Accès, audit et coopération avec les autorités
06 Résiliation et stratégie de sortie
07 Continuité, niveaux de service et tests

OBJET

Cette note est informative et ne crée aucun engagement. Les engagements de REVIEWIT figurent à l'annexe 5 de l'accord de traitement des données (DPA), « Sécurité des services et résilience opérationnelle numérique », dont les articles sont cités entre parenthèses, et, pour la sortie, à l'annexe 6. En cas d'écart, le texte de ces annexes prévaut.

SECTION 01 Quand l'annexe 5 s'applique

VOLET	CLIENT CONCERNÉ	CONTENU
Volet A	Entité essentielle ou importante au sens de NIS 2, ou entité financière au sens de DORA, déclarée aux conditions particulières (art. 1.2).	Sécurité de la chaîne d'approvisionnement (NIS 2, art. 21 et 23) : mesures, incidents, vulnérabilités, fournisseurs TIC, autorités.

VOLET	CLIENT CONCERNÉ	CONTENU
Section B1	Toute entité financière au sens de DORA (art. 1.3).	Clauses de l'article 30.2 de DORA : description, localisations, protection des données, restitution, niveaux de service, assistance, coopération, résiliation, formation, registre.
Section B2	Entité financière qui désigne par écrit le Service comme soutenant une fonction critique ou importante (art. 1.3).	Clauses de l'article 30.3 de DORA : niveaux chiffrés, rapports, continuité, TLPT, sous-traitance, audit sans restriction, stratégie de sortie.

La qualification de la fonction soutenue relève du seul Client ; REVIEWIT ne peut pas la refuser. Une désignation en cours de contrat fait l'objet d'un avenant (art. 1.3). L'annexe est une obligation contractuelle envers le Client : elle ne vaut pas reconnaissance que REVIEWIT serait lui-même une entité soumise à NIS 2 (art. 1.5).

SECTION 02 Notification des incidents

Pour vos propres notifications aux autorités (NIS 2, art. 23 ; DORA, art. 19), REVIEWIT vous informe de tout incident notifiable : indisponibilité ou dégradation grave du Service pendant plus de soixante minutes consécutives, atteinte à vos données, à votre piste d'audit ou aux preuves produites, accès non autorisé aux systèmes de production, ou menace imminente de l'un de ces cas. En cas de doute, l'incident est notifié (art. 5.1).

ÉTAPE	DÉLAI MAXIMAL	CONTENU
Alerte	24 heures après la prise de connaissance (art. 5.2)	Nature, dates, fonctions et données affectées, cause malveillante présumée, impact sur d'autres clients ou transfrontière, premières mesures, contact de suivi.
Mise à jour	72 heures après la prise de connaissance (art. 5.3)	Évaluation initiale, gravité, impact, indicateurs de compromission disponibles.
Point d'étape	Sur demande, notamment d'une autorité (art. 5.4)	État de l'incident et de son traitement.
Rapport final	Un mois après l'alerte (art. 5.5)	Cause première probable, mesures d'atténuation, impact transfrontière ; rapport d'avancement si l'incident est encore en cours.

Une violation de données à caractère personnel vous est notifiée au plus tard 24 heures après sa prise de connaissance (DPA, art. 8) ; une même communication peut valoir pour les deux régimes (art. 3.2). Les communications partent de **security@we-reviewit.com** vers le contact de sécurité que vous désignez aux conditions particulières et sont doublées dans l'espace de support (art. 5.6, 9.2). REVIEWIT vous assiste pour l'analyse, le confinement, le rétablissement et vos notifications (art. 5.8, 15).

SECTION 03 Sécurité de la chaîne d'approvisionnement

- **Mesures.** L'annexe 1 du DPA décrit les mesures techniques et organisationnelles et indique, mesure par mesure, si elle est en service, partielle ou prévue, pour que vous appréciiez les pratiques de cybersécurité de REVIEWIT (NIS 2, art. 21.3). Le niveau de sécurité n'est pas diminué pendant le contrat (art. 4.1).

- **Développement et publication.** 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 pour le canal stable (art. 4.2).
- **Vulnérabilités.** Correction ou atténuation sous quatorze jours pour une vulnérabilité critique, trente jours pour une vulnérabilité élevée, à compter de la qualification ; information du Client lorsqu'une vulnérabilité exploitable ne peut être corrigée dans ce délai (art. 6.1, 6.2). La politique de divulgation responsable de REVIEWIT décrit la réception des signalements (art. 6.3).
- **Information sur demande.** Annexe 1 en vigueur et changements d'état de ses mesures, état de la démarche de certification, réponse à votre questionnaire de sécurité une fois par période de douze mois (art. 4.3).
- **Fournisseurs TIC.** Liste des prestataires informatiques de REVIEWIT, y compris ceux qui ne traitent aucune donnée du Client, publiée dans l'espace client du Trust Center ; évaluation de leur sécurité avant de les retenir puis chaque année (art. 7.2, 7.3).

SECTION 04 Registre d'information (DORA, art. 28)

REVIEWIT vous communique les informations nécessaires à votre registre d'information sur les prestataires tiers de services TIC : dénomination, identifiants, pays d'établissement, services fournis, localisations et chaîne de sous-traitance (art. 19).

- REVIEWIT SAS est votre prestataire direct ; ses propres prestataires figurent, avec leur identification, le service rendu, le lieu des données, les transferts et leur criticité, dans « Prestataires informatiques de REVIEWIT » (espace client du Trust Center).
- Le Service est fourni dans la région d'hébergement que vous choisissez, par défaut Paris, Union européenne ; elle n'est pas changée sans votre instruction. Tout changement de pays d'un prestataire vous est annoncé trente jours à l'avance, ou dès que REVIEWIT en a connaissance si le prestataire décide avec un préavis plus court (art. 11).
- Il vous appartient de qualifier la fonction que REVIEWIT soutient (fonction critique ou importante au sens de DORA) et de l'inscrire comme telle.

SECTION 05 Accès, audit et coopération avec les autorités

- **Tout client.** Audit documentaire ou sur place une fois par an, avec un préavis de trente jours ; pour les sous-traitants ultérieurs d'infrastructure, vérification par leurs rapports et certifications indépendants (DPA, art. 10).
- **Fonction critique ou importante (B2).** Droit d'accès, d'inspection et d'audit sans restriction pour vous, le tiers que vous désignez et l'autorité compétente, y compris la prise de copie sur place ; préavis de dix jours ouvrés hors urgence et hors demande d'une autorité ; audit groupé ou rapport de tiers indépendant lorsque les droits d'autres clients sont en cause (art. 25).
- **Autorités.** Coopération avec les autorités compétentes, les autorités de résolution et les CSIRT dont vous relevez ; information du Client de toute demande d'autorité qui le concerne, sauf interdiction légale (art. 8, 16).

SECTION 06 Résiliation et stratégie de sortie

- **Résiliation sans pénalité** dans les cas de l'article 28.7 de DORA : violation significative, circonstances relevées lors du suivi du risque, faiblesses avérées dans la gestion du risque lié aux TIC, impossibilité de supervision par l'autorité (art. 17.1). Préavis minimal de REVIEWIT lorsqu'il met fin au contrat : trois mois, six mois pour une fonction critique ou importante (art. 17.3).

- **Sortie (annexe 6).** Période de transition pendant laquelle le Service continue d'être fourni ; paquet de restitution (archive ZIP de fichiers CSV et JSON documentés, avec manifeste d'empreintes SHA-256) ; période d'extraction de trente jours au moins ; effacement et attestation. Pour une entité financière, en cas d'insolvabilité, de résolution ou de cessation d'activité de REVIEWIT, le paquet est mis à disposition sans frais (art. 13.2).
- **Fonction critique ou importante.** Période de transition portée, sur notification, jusqu'à six mois ; information utile à votre plan de sortie et test de ce plan avec vous, dans des conditions convenues (art. 26) ; paquet de restitution remis chaque trimestre (art. 13.2).

SECTION 07 Continuité, niveaux de service et tests

- **Niveaux de service (B2).** Disponibilité mensuelle de 99,5 % mesurée par la page de statut publique, maintenance programmée encadrée, délais de prise en compte du support, perte de données maximale de vingt-quatre heures et délai de rétablissement de quarante-huit heures, délais de notification ; rapport de service trimestriel (art. 20, 21).
- **Continuité.** Sauvegardes automatiques des bases et export de souscription vérifié par une restauration réelle sont en service (annexe 1). Le plan de continuité et le test de restauration chronométré exigés pour la section B2 (art. 22) sont à l'état « prévu » de l'annexe 1.
- **Test d'intrusion.** L'annexe 5 prévoit un test d'intrusion annuel du Service par un tiers indépendant, dont la synthèse vous est communiquée sur demande et sous confidentialité (art. 6.4). À la date de la présente note, aucun test d'intrusion n'a encore été réalisé.
- **TLPT.** Lorsque vous êtes tenu de réaliser des tests de pénétration fondés sur la menace (DORA, art. 26 et 27), REVIEWIT y participe à votre demande, selon des règles convenues par écrit, avec la possibilité d'un test groupé (art. 23).
- **Sensibilisation.** Participation à vos programmes de sensibilisation et de formation à la résilience opérationnelle numérique, une session à distance par an sans frais (art. 18).

REVIEWIT SAS · Sécurité et incidents : **security@we-reviewit.com** · Délégué à la protection des données : **dpo@we-reviewit.com**. L'annexe 5 est conclue avec le DPA ; l'annexe 1 et la liste des prestataires informatiques sont disponibles dans l'espace client du Trust Center. Version 1.0 · Novembre 2026 · la version française fait foi.