Contrat de sous-traitance (DPA) — Loket

Entre :

Le professionnel titulaire du compte Loket, tel qu'identifié dans ses paramètres de compte — le « **Responsable du traitement** » ;

et

Always Late Technologies BV (« Loket »), société de droit belge, Fonteyneweg 2, 1800 Vilvoorde, Belgique, BCE **1039.721.620**, TVA **BE 1039.721.620** — le « **Sous-traitant** » ;

en application de l'**article 28 RGPD**, en complément des conditions générales d'utilisation (le « Contrat principal »). En cas de contradiction sur la protection des données, le présent DPA prévaut.

Le présent contrat est **accepté par voie électronique** lors de la création du compte Loket, en même temps que le Contrat principal. Il ne requiert donc ni signature manuscrite ni exemplaire papier.

1. Définitions

Les termes du RGPD (responsable, sous-traitant, sous-traitant ultérieur, personne concernée, violation de données, etc.) ont le sens que leur donne le Règlement.

2. Objet, rôles et durée

2.1. Le Sous-traitant héberge une application par laquelle **les clients du Responsable** déposent des pièces via un lien, sans créer de compte, en vue de leur collecte et de leur mise à disposition du Responsable, au bénéfice du Responsable.

2.2. **Rôles.** Le Responsable détermine les finalités et les moyens : il est **responsable du traitement**. Loket traite les données **uniquement pour fournir le Service et sur instruction** du Responsable : il est **sous-traitant**.

2.3. **Durée.** Pendant toute la durée du Contrat principal et tant que des données sont traitées pour le compte du Responsable.

3. Description du traitement

Détaillée en **Annexe 1**.

4. Obligations du Sous-traitant

(a) Instructions. Ne traiter que sur instruction documentée du Responsable (le présent DPA et l'usage normal valant instructions), sauf obligation légale (avec information préalable sauf interdiction).

(b) Confidentialité. Astreindre à la confidentialité les personnes autorisées.

(c) Sécurité. Mesures de l'**article 32** — **Annexe 3**.

(d) Sous-traitants ultérieurs. N'y recourir que selon l'**Annexe 2**, sous **autorisation générale**, avec information préalable de **30 jours** de tout changement et droit d'opposition pour motif légitime ; obligations équivalentes imposées par contrat à chaque sous-traitant ultérieur.

(e) Assistance. Aider le Responsable à répondre aux demandes d'exercice des droits (via les fonctions d'**export** et de **suppression**) et à respecter les articles 32 à 36.

(f) Violation de données. Notifier le Responsable **sans retard injustifié** (au plus tard **48 heures**) avec les éléments de l'art. 33 §3 disponibles. La notification à l'autorité et aux personnes concernées incombe au Responsable.

(g) Fin de relation. Supprimer ou restituer les données au choix du Responsable et détruire les copies, sauf obligation légale (art. 6).

(h) Registre & documentation. Tenir le registre (art. 30 §2) et démontrer la conformité à l'art. 28.

(i) Audit. Permettre les audits **annuels** et post-incident, sur préavis raisonnable et sous confidentialité ; peut être satisfait par les rapports des sous-traitants ultérieurs.

5. Obligations du Responsable

Garantir une **base légale**, informer ses propres clients, ne transmettre que les données nécessaires, et paramétrer les durées offertes par le Service.

6. Sort des données en fin de contrat

6.1. **Le choix prévu à l'article 28.3(g) — restitution ou suppression — appartient au Responsable**, et le Service le lui rend exerçable sans passer par le Sous-traitant : la **restitution** s'opère par la fonction d'**export** (une archive complète, base et fichiers), disponible tant que le compte existe, **y compris pendant toute la fenêtre décrite au 6.2**.

6.2. **À défaut de restitution, la suppression est le défaut, à 90 jours.** À la fin de l'abonnement ou de l'essai, le compte est **suspendu** : la collecte s'arrête, les données restent **intactes et exportables**. Le Sous-traitant informe le Responsable **30 jours puis 7 jours** avant l'échéance. Au terme des **90 jours**, le compte est **clôturé** — suppression de la base et des fichiers, copies comprises — sauf obligation légale de conservation.

6.3. **Le Responsable peut clôturer à tout moment** depuis ses paramètres, sans attendre le terme. La clôture anticipée et la clôture automatique empruntent le **même et unique chemin de suppression**. La suppression d'un dossier supprime effectivement les fichiers du stockage.

7. Transferts hors UE

7.1. Données **au repos** hébergées **en UE (Francfort)** — Annexe 2.

7.2. Certains sous-traitants étant établis **aux États-Unis**, les transferts sont encadrés par les **clauses contractuelles types** de la Commission européenne et/ou le **Data Privacy Framework**. Au **28 juillet 2026**, les trois sous-traitants américains disposent d'une certification **active** au Data Privacy Framework : **Vercel Inc.** (UE-US, Suisse-US et extension Royaume-Uni) ; **Neon**, couvert par la certification de **Databricks, Inc.** dont il fait partie ; **Resend** (UE-US et extension Royaume-Uni, recertification en cours à cette date). Ce statut est **revérifié chaque trimestre** et les documents contractuels sont mis à jour s'il change.

8. Responsabilité et droit applicable

8.1. Dans les rapports entre les parties, la responsabilité est répartie selon le Contrat principal et le RGPD, y compris les limitations du Contrat principal, mais uniquement dans la mesure permise par le droit impératif applicable.

8.2. Aucune stipulation du présent DPA ne limite les droits des personnes concernées, les pouvoirs d'une autorité de contrôle, ni la répartition et les recours prévus à l'article 82 du RGPD.

8.3. Droit **belge** ; tribunaux de **Bruxelles**.

Annexe 1 — Description du traitement

Finalité	Collecte, dépôt, stockage et restitution de pièces justificatives entre le Responsable et ses clients.
Nature	Hébergement, stockage, transmission, suppression.
Personnes concernées	Clients du Responsable et tiers dont des documents sont déposés.
Catégories de données	données d'identification et de contact ; contenu des documents déposés (pièces d'identité, actes, documents financiers ou immobiliers). Peuvent inclure des données **sensibles / à haut risque** selon les pièces demandées — voir note DPIA.
Durée	Durée de la relation + 90 jours (fenêtre de restitution, art. 6) ; expiration des liens paramétrable.

> ***Note DPIA :*** *le* ***Responsable*** *doit évaluer si une* ***AIPD (art. 35)*** *est requise de son côté (pièces d'identité, données sensibles, clientèle réglementée). Loket fournit les éléments techniques.*

Annexe 2 — Sous-traitants ultérieurs autorisés

Sous-traitant	Rôle	Localisation données	Transfert
Vercel Inc. (US)	Hébergement app + fichiers (Blob)	Fichiers **fra1 / UE**	DPF **actif** (UE-US, Suisse-US, extension UK)
Neon (société du groupe Databricks) (US)	Base de données	**eu-central-1 / UE**	DPF **actif** via Databricks, Inc.
Resend (US)	Emails transactionnels (liens, notifications)	Adresses + contenu emails	DPF **actif** (recertification en cours au 28/07/2026)

Annexe 3 — Mesures techniques et organisationnelles (art. 32)

- **Chiffrement en transit** : HTTPS/TLS de bout en bout. Neon impose TLS 1.2/1.3 ; Vercel utilise HTTPS/TLS 1.3 ; Resend TLS 1.3.
- **Chiffrement au repos** :
- base de données (**Neon**) : **AES-256** (documenté par Neon) ;
- fichiers déposés (**Vercel Blob**) : **AES-256**, appliqué avant écriture sur disque (documenté par Vercel) ;
- emails (**Resend**) : données chiffrées au repos ; **l'algorithme n'est pas documenté publiquement par Resend**, il n'est donc pas affirmé ici.
- **Cloisonnement par compte** : accès limité au compte titulaire ; tout accès hors périmètre échoue.
- **Liens de dépôt non devinables** : jetons aléatoires, non listables, expiration paramétrable.
- **Authentification** : liens de connexion à usage unique (24 h).
- **Accès restreint** : stockage privé (URL non publiques, suffixe aléatoire). L'accès administrateur se fait via les consoles des hébergeurs, protégées par authentification forte, et limité à une seule personne. **Loket n'implémente pas à ce jour de journal applicatif des accès administrateur** : la journalisation disponible est celle des plateformes (Neon, Vercel).
- **Contrôles des fichiers** : types autorisés, taille maximale de 100 Mo, maximum de 20 fichiers par pièce et quotas d'usage contrôlés avant téléversement ou téléchargement. **Loket n'effectue pas d'analyse antivirus** ; ces contrôles ne garantissent pas qu'un fichier soit exempt de logiciel malveillant.
- **Suppression effective** : dossier supprimé = fichiers supprimés ; compte supprimé = purge base + fichiers.
- **Sauvegardes** :

- base de données (**Neon**) : restauration à un instant donné (*point-in-time restore*) sur une fenêtre de **7 jours**, mesurée le 1 août 2026. La procédure de reprise impose une restauration isolée et une vérification avant toute action sur la production ;
- fichiers déposés (**Vercel Blob**) : stockage répliqué, durabilité annoncée de 99,999999999 % et disponibilité de 99,99 %. **Vercel ne propose pas de restauration de fichier côté client** : un fichier supprimé n'est pas récupérable. La suppression est donc définitive — ce qui est cohérent avec l'obligation d'effacement, mais signifie qu'une suppression accidentelle par le Responsable est irréversible.
- **Certifications des sous-traitants** : Vercel — SOC 2 Type II et ISO 27001:2022 ; Neon — audits SOC 2 Type II et ISO 27001 annuels ; Resend — SOC 2 Type II.

Version 2026-08-01.1 — accepté par voie électronique à la création du compte Loket. Aucune signature manuscrite n'est requise ; la preuve de l'acceptation est l'horodatage conservé par Loket avec le compte du Responsable.