

Accord de sous-traitance (DPA)

Traitement de données à caractère personnel — RGPD (article 28)

Version 1.0 — 30 juillet 2026

1. Objet et rôles

Le présent Accord de sous-traitance (« DPA ») encadre le traitement des données à caractère personnel effectué par **TILVA** (SAS, RCS Paris 107 858 854, siège social 47 rue Vivienne, 75002 Paris — « le Sous-traitant »), éditeur du service Agend'Élus, pour le compte de la **Collectivité** (« le Responsable de traitement ») dans le cadre de l'utilisation du Service. Il s'inscrit dans le cadre de l'article 28 du Règlement (UE) 2016/679 (« RGPD »).

La Collectivité détermine les finalités et les moyens du traitement ; elle agit en qualité de responsable de traitement. TILVA traite les données sur instruction documentée de la Collectivité, en qualité de sous-traitant.

2. Nature et finalités du traitement

Le traitement a pour finalités : la gestion des invitations aux événements de la Collectivité, le recueil et le suivi des réponses de présence, la réalisation de sondages de disponibilité, l'envoi de notifications (courrier électronique et notifications push), l'authentification des utilisateurs, l'administration du compte et la production de récapitulatifs.

3. Catégories de personnes et de données

Personnes concernées : les élus, agents et invités inscrits par la Collectivité, ainsi que les administrateurs du compte.

Catégories de données traitées :

- **Identification** : nom, prénom.
- **Coordonnées** : adresse électronique (principale et secondaire), numéro de téléphone.
- **Fonction** : catégorie de fonction ou mandat (maire, adjoint, conseiller municipal, communautaire, départemental, régional, direction des services, cabinet, etc.) et précisions associées.
- **Données d'activité** : réponses de présence, disponibilités, dates et sources de réponse, nombre de relances, envois.
- **Données de compte** : adresse électronique et mot de passe (haché) des administrateurs.
- **Données techniques d'authentification** : codes à usage unique et jetons (stockés hachés), identifiants d'appareil pour les notifications push.
- **Contenu déposé par la Collectivité** : intitulés d'événements, lieux, descriptions, signatures, et pièces jointes (ordres du jour, cartons) dont le contenu est déterminé et maîtrisé par la seule Collectivité.

Absence de données sensibles. Le Service ne collecte pas volontairement de catégories particulières de données au sens de l'article 9 du RGPD. La Collectivité s'engage à ne pas déposer, notamment via les pièces jointes ou l'intitulé des groupes qu'elle crée librement, de données susceptibles de révéler de telles catégories, sauf base légale appropriée dont elle assume la responsabilité.

4. Obligations du Sous-traitant

TILVA s'engage à :

- ne traiter les données que sur instruction documentée de la Collectivité, y compris pour les transferts ;
- garantir la confidentialité des données et veiller à ce que les personnes autorisées à les traiter s'y soient engagées ;

- mettre en œuvre les mesures techniques et organisationnelles appropriées décrites à l'article 6 ;
- respecter les conditions de recours à un sous-traitant ultérieur (article 5) ;
- aider la Collectivité à répondre aux demandes d'exercice des droits des personnes concernées ;
- assister la Collectivité pour la sécurité, la notification de violations et, le cas échéant, les analyses d'impact ;
- à la fin des prestations, restituer ou supprimer les données selon le choix de la Collectivité (article 7) ;
- mettre à disposition les informations nécessaires pour démontrer le respect de ces obligations.

5. Sous-traitants ultérieurs

La Collectivité autorise TILVA à recourir aux sous-traitants ultérieurs listés ci-dessous. TILVA informe la Collectivité de tout changement envisagé, lui permettant d'émettre des objections.

Sous-traitant	Rôle	Données concernées	Localisation
Railway	Hébergement, base de données	Ensemble des données de la base	Union européenne (Amsterdam)
Cloudflare R2	Stockage des pièces jointes	Fichiers déposés et leur contenu	Union européenne (juridiction UE)
Resend	Courriers électroniques transactionnels	Nom, e-mail, contenu des invitations et pièces jointes	États-Unis — encadré (EU-US DPF + clauses types)
Google (FCM)	Notifications push Android	Identifiant d'appareil, contenu de la notification	États-Unis — encadré (clauses types / DPF)
Apple (APNs)	Notifications push iOS	Identifiant d'appareil, contenu de la notification	États-Unis — encadré (clauses types / DPF)

Transferts hors Union européenne. Les données au repos (base de données et pièces jointes) sont hébergées dans l'Union européenne, respectivement chez Railway (Amsterdam) et Cloudflare R2 (juridiction UE). Certains sous-traitants (Resend, Google, Apple) peuvent traiter des données aux États-Unis pour l'envoi des courriers et des notifications. Ces transferts sont encadrés par les garanties appropriées prévues par le RGPD : clauses contractuelles types de la Commission européenne et, le cas échéant, certification au titre du cadre de protection des données UE-États-Unis (Data Privacy Framework). DPA des sous-traitants : railway.com/legal/dpa, cloudflare.com/legal, resend.com/legal/dpa (sous-traitants : resend.com/legal/subprocessors), et les addenda de traitement des données de Google et d'Apple.

6. Mesures techniques et organisationnelles

TILVA met en œuvre notamment les mesures suivantes :

- **Chiffrement en transit** : communications sécurisées (HTTPS) sur l'ensemble du Service ; en-têtes de sécurité.
- **Authentification** : mots de passe administrateurs hachés (argon2) ; authentification des élus par code à usage unique sans mot de passe ; jetons stockés hachés ; secrets distincts et révocables ; verrouillage temporaire après échecs répétés.
- **Cloisonnement** : isolation stricte des données entre Collectivités (architecture multi-locataires), vérifiée par des tests automatisés d'isolation.
- **Contrôle d'accès** : gestion des rôles (administrateur local, super-administrateur).
- **Sauvegardes** : restauration de la base de données à un instant donné (PITR) et sauvegardes planifiées.
- **Contrôles applicatifs** : limitation de débit, contrôle du type des pièces jointes, échappement des contenus, tests automatisés.

7. Durée de conservation, restitution et suppression

Les données sont conservées pendant la durée de la relation contractuelle. Mécanismes en place :

- **Codes et jetons d'authentification** : durées courtes (code de connexion : 10 min ; lien de réinitialisation : 1 h ; lien d'activation : 7 jours).
- **Suppression d'un contact** : retrait des listes actives ; les réponses passées peuvent être conservées pour l'intégrité de l'historique.
- **Fermeture d'un compte** : suppression des données de la Collectivité (contacts, événements, invitations, administrateurs, fichiers joints), sous réserve du délai de restitution.

À la fin des prestations, TILVA restitue les données dans un format exploitable ou les supprime, selon le choix de la Collectivité, dans le délai convenu.

8. Violation de données

TILVA notifie à la Collectivité toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance, et lui fournit les informations nécessaires pour lui permettre de procéder, le cas échéant, aux notifications qui lui incombent auprès de l'autorité de contrôle et des personnes concernées.

9. Droits des personnes concernées

TILVA met à disposition de la Collectivité les fonctionnalités et l'assistance nécessaires pour répondre aux demandes d'exercice des droits (accès, rectification, effacement, limitation, portabilité, opposition). Les demandes reçues directement par TILVA sont transmises à la Collectivité.

10. Audit

TILVA met à disposition les informations nécessaires pour démontrer le respect de ses obligations et permet la réalisation d'audits, dans des conditions raisonnables préservant la sécurité et la confidentialité des autres Collectivités.

11. Durée et fin

Le présent DPA prend effet à l'acceptation du Service et demeure en vigueur pendant toute la durée du traitement. Les obligations relatives à la confidentialité, à la restitution et à la suppression des données survivent à son terme.

12. Contact

Pour toute question relative à la protection des données : contact@agendelus.fr.

Signatures

Pour la Collectivité (Responsable de traitement)

Nom : _____

Fonction : _____

Date et signature :

Pour TILVA (Sous-traitant)

Nom : _____

Fonction : _____

Date et signature :