Accord de traitement des données (DPA)

Annexe au contrat de services — article 28 du RGPD

Dernière mise à jour : 18/11/2026

Plateforme de gestion des ressources humaines

> Le présent accord de traitement des données (« DPA ») encadre le traitement, par Antorya en qualité de sous-traitant, des données à caractère personnel confiées par le Client responsable de traitement dans le cadre de l'utilisation de la plateforme Antorya.
>
> Il fait partie intégrante des Conditions Générales de Services et est conclu conformément à l'article 28 du Règlement (UE) 2016/679 (RGPD).

1. Parties et objet

Le présent accord de traitement des données (« DPA ») est conclu entre :

- Toovent, SASU au capital de 1 000 €, immatriculée au RCS de Paris sous le numéro 102 094 067, dont le siège social est situé 200 rue de la Croix-Nivert, 75015 Paris, éditrice de la plateforme Antorya, agissant en qualité de sous-traitant (ci-après « Antorya ») ;
- le Client, tel qu'identifié dans les Conditions Générales de Services ou la proposition commerciale acceptée, agissant en qualité de responsable de traitement (ci-après le « Client »).

Ensemble les « Parties ». Le présent DPA a pour objet de définir les conditions dans lesquelles Antorya traite, pour le compte et sur instruction du Client, les données à caractère personnel nécessaires à la fourniture des Services, dans le respect de l'article 28 du RGPD.

1.1 Documents contractuels. Le présent DPA fait partie intégrante des Conditions Générales de Services (« CGS »). En cas de contradiction entre le DPA et les CGS s'agissant du traitement des données à caractère personnel, le DPA prévaut. Les définitions du RGPD s'appliquent aux termes employés (« responsable de traitement », « sous-traitant », « traitement », « données à caractère personnel », « violation de données », « personne concernée »).

1.2 Durée. Le présent DPA prend effet à la date d'acceptation des CGS par le Client et demeure en vigueur pendant toute la durée du traitement des données pour le compte du Client. Il expire automatiquement à l'achèvement des opérations de suppression ou de restitution prévues à l'article 12.

2. Description du traitement

L'objet, la nature, la finalité et la durée du traitement, les catégories de données et de personnes concernées ainsi que les obligations et droits du Client sont décrits à l'Annexe 1 du présent DPA. Le traitement est réalisé exclusivement dans le cadre de la fourniture des Services de gestion des ressources humaines.

Données de santé — périmètre limité

Le traitement peut inclure une catégorie particulière de données au sens de l'article 9 du RGPD : l'information relative à l'absence d'un collaborateur pour arrêt de travail (volet destiné à l'employeur), à l'exclusion de tout motif médical ou diagnostic. Ce traitement est réalisé pour le compte du Client, sur le fondement de ses obligations en matière de droit du travail et de sécurité sociale (article 9.2.b du RGPD). Les mesures de cloisonnement applicables figurent à l'Annexe 3.

3. Traitement sur instruction documentée

Antorya traite les données à caractère personnel uniquement sur instruction documentée du Client, y compris en ce qui concerne les transferts éventuels, sauf obligation légale contraire ; dans ce cas, Antorya informe le Client de cette obligation avant le traitement, sauf si la loi l'interdit pour des motifs d'intérêt public.

Les CGS, le présent DPA et l'utilisation des fonctionnalités de la plateforme conformément à sa documentation constituent les instructions initiales du Client. Toute instruction complémentaire doit être formulée par écrit.

Antorya informe immédiatement le Client si, à son avis, une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données. Antorya peut suspendre l'exécution de l'instruction concernée jusqu'à sa confirmation ou sa modification par le Client.

4. Obligations d'Antorya

Antorya s'engage à :

- ne traiter les données que pour les finalités décrites à l'Annexe 1, et ne pas les utiliser à ses propres fins ni les céder à des tiers ;
- garantir que les personnes autorisées à traiter les données sont soumises à une obligation de confidentialité appropriée, contractuelle ou légale ;
- mettre en œuvre les mesures techniques et organisationnelles appropriées prévues à l'article 8 et détaillées à l'Annexe 3 ;
- respecter les conditions relatives au recours à un autre sous-traitant prévues à l'article 5 ;
- aider le Client, par des mesures appropriées, à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (article 6) ;
- aider le Client à garantir le respect des obligations de sécurité, de notification des violations et d'analyse d'impact (articles 7 à 9) ;
- supprimer ou restituer les données au terme de la prestation, dans les conditions de l'article 12 ;
- mettre à la disposition du Client les informations nécessaires pour démontrer le respect des obligations de l'article 28 du RGPD et permettre la réalisation d'audits, dans les conditions de l'article 11.

5. Sous-traitants ultérieurs

Le Client autorise Antorya à recourir aux sous-traitants ultérieurs listés à l'Annexe 2 pour l'exécution de traitements spécifiques. Cette autorisation constitue une autorisation générale écrite au sens de l'article 28.2 du RGPD.

Antorya conclut avec chaque sous-traitant ultérieur un contrat imposant des obligations de protection des données substantiellement équivalentes à celles du présent DPA. Antorya demeure pleinement responsable devant le Client de l'exécution par ce sous-traitant de ses obligations.

Antorya informe le Client de tout projet d'ajout ou de remplacement d'un sous-traitant ultérieur, par tout moyen approprié, au moins trente (30) jours avant sa mise en œuvre. Le Client peut s'opposer à ce changement pour des motifs légitimes tenant à la protection des données dans un délai de quinze (15) jours à compter de cette information. Les Parties recherchent alors une solution ; à défaut d'accord, le Client peut résilier la partie des Services concernée.

6. Droits des personnes concernées

Antorya met à la disposition du Client, dans la mesure du possible, les fonctionnalités et l'assistance raisonnable lui permettant de donner suite aux demandes d'exercice des droits des personnes concernées — droit d'accès, de rectification, d'effacement, de limitation, de portabilité et d'opposition.

Si une demande est adressée directement à Antorya par une personne concernée, Antorya la transmet sans délai au Client et n'y répond pas de sa propre initiative, sauf instruction du Client ou obligation légale.

7. Sécurité du traitement

Compte tenu 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, Antorya met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD.

Ces mesures, décrites à l'Annexe 3, incluent notamment le cloisonnement des données par organisation cliente, le cloisonnement renforcé des données de santé, le chiffrement au repos et en transit, le contrôle des accès et la journalisation. Antorya peut faire évoluer ces mesures à condition de maintenir un niveau de sécurité au moins équivalent.

8. Notification des violations de données

Antorya notifie au Client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance, sans délai injustifié et au plus tard dans les quarante-huit (48) heures, afin de permettre au Client de respecter son obligation de notification à la CNIL dans les soixante-douze (72) heures prévue à l'article 33 du RGPD.

La notification décrit, dans la mesure des informations disponibles, la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables et les mesures prises ou proposées pour y remédier. Antorya apporte au Client une assistance raisonnable dans la gestion de la violation et dans ses éventuelles obligations d'information des personnes concernées.

La notification d'une violation ou la réponse apportée par Antorya ne vaut pas reconnaissance d'une faute ou d'une responsabilité.

9. Analyse d'impact et consultation préalable

Compte tenu de la nature du traitement et des informations à sa disposition, Antorya aide le Client à réaliser les analyses d'impact relatives à la protection des données (AIPD) requises par l'article 35 du RGPD, ainsi que les consultations préalables de la CNIL prévues à l'article 36, lorsqu'elles sont nécessaires.

> Le traitement de données de santé, même limité au volet employeur des arrêts de travail, peut rendre une AIPD nécessaire du côté du Client. Antorya fournit à cet effet les informations utiles sur les mesures techniques et organisationnelles décrites à

10. Localisation des données et absence de transfert hors UE

L'ensemble des données à caractère personnel traitées dans le cadre des Services est hébergé et conservé au sein de l'Union européenne, et à ce jour en France. Les sous-traitants ultérieurs listés à l'Annexe 2 assurent l'hébergement et le traitement de ces données dans des centres situés dans l'Union européenne.

Le présent DPA n'emporte pas de transfert de données à caractère personnel vers un pays tiers au sens du chapitre V du RGPD à des fins d'hébergement ou de conservation. Lorsqu'un sous-traitant ultérieur relève d'un groupe établi hors de l'Union européenne, tout accès aux données depuis un pays tiers, notamment à des fins de support ou d'exploitation, est encadré par un mécanisme de transfert approprié — décision d'adéquation ou clauses contractuelles types de la Commission européenne.

Si un transfert vers un pays tiers devait être envisagé à l'avenir pour d'autres finalités, il serait préalablement encadré par un mécanisme de transfert approprié et le Client en serait informé conformément à l'article 5.

11. Information et audits

Antorya met à la disposition du Client les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD. Le Client peut, à ses frais, procéder à un audit une fois par année civile, sur préavis écrit raisonnable d'au moins trente (30) jours, pendant les heures ouvrées et sans perturbation excessive de l'activité d'Antorya.

Antorya peut satisfaire à cette obligation en fournissant au Client une documentation à jour décrivant ses mesures techniques et organisationnelles, ou toute attestation ou certification pertinente. Les informations obtenues à l'occasion d'un audit sont couvertes par la confidentialité prévue aux CGS.

12. Sort des données en fin de traitement

Au terme de la fourniture des Services, le Client dispose d'un délai de quatre-vingt-dix (90) jours pour extraire l'ensemble de ses données au moyen des fonctionnalités d'export mises à sa disposition.

À l'expiration de ce délai, Antorya procède à la suppression définitive de l'ensemble des données à caractère personnel traitées pour le compte du Client, ainsi que des copies existantes, sauf obligation légale de conservation. Des durées de conservation spécifiques par catégorie de données figurent à l'Annexe 1. Antorya atteste par écrit de cette suppression sur demande du Client.

13. Responsabilité et dispositions générales

Chaque Partie répond des dommages causés par un traitement qui ne respecte pas les obligations du RGPD lui incombant. La responsabilité d'Antorya au titre du présent DPA s'inscrit dans les limites prévues par les Conditions Générales de Services, dans la mesure permise par la loi.

Le présent DPA est régi par le droit français. Tout différend relatif à son interprétation ou à son exécution suit le régime prévu par les Conditions Générales de Services. Les Parties conviennent de négocier de bonne foi toute modification rendue nécessaire par une évolution de la réglementation applicable.

14. Point de contact

Pour toute question relative au présent DPA ou au traitement des données à caractère personnel, le point de contact d'Antorya est joignable à l'adresse rgpd@tolipo.fr.

> À ce stade, Toovent n'est pas soumise à l'obligation de désigner un délégué à la protection des données (DPO). Le point de contact ci-dessus assure le suivi des questions relatives à la protection des données. Cette désignation sera réévaluée si l'activité

Annexe 1 — Description des traitements

Finalité et nature

Finalité : héberger et faire fonctionner un logiciel de gestion des ressources humaines pour le compte du Client (gestion des collaborateurs, contrats, temps de travail, absences, obligations sociales, documents RH).

Nature des opérations : collecte, enregistrement, structuration, conservation, consultation, modification, extraction et suppression des données, réalisées sur instruction du Client.

Durée du traitement : durée du contrat de services, sous réserve des durées de conservation ci-dessous.

Catégories de personnes concernées

Collaborateurs des clients d'Antorya : salariés, stagiaires, alternants, intérimaires et prestataires externes ; utilisateurs administrateurs désignés par le Client.

Catégories de données à caractère personnel

- données d'identification et de contact des collaborateurs ;
- données professionnelles : poste, contrat, rémunération ;
- données administratives RH : absences, congés, temps de travail ;
- information d'absence pour arrêt maladie (volet destiné à l'employeur) ;
- documents RH téléversés par le Client.

Catégories particulières de données (article 9 RGPD)

> **Périmètre limité**
>
> Données de santé limitées : information de l'absence pour arrêt maladie (volet employeur, sans motif médical) et justificatif d'arrêt de travail correspondant, à l'exclusion de tout diagnostic ou donnée médicale détaillée.

Durées de conservation

Pendant toute la durée du contrat. À la fin du contrat : mise à disposition pour extraction pendant quatre-vingt-dix (90) jours, puis suppression définitive.

Des purges internes complémentaires s'appliquent par domaine, sans préjudice des obligations légales de conservation incombant au Client en sa qualité d'employeur :

Catégorie	Durée de conservation
Données de recrutement (candidats non retenus)	2 ans à compter du dernier contact
Documents résiduels après départ d'un collaborateur	Sortie + 90 jours
Journaux d'envoi d'e-mails	30 jours
Ensemble des données, après fin du contrat client	Extraction 90 jours, puis suppression définitive

Annexe 2 — Sous-traitants ultérieurs

Les sous-traitants ultérieurs suivants interviennent dans la fourniture des Services. L'ensemble héberge et traite les données au sein de l'Union européenne.

Sous-traitant	Rôle	Localisation	Transfert hors UE
Scaleway (SAS, France)	Hébergement de l'application (Serverless Containers)	Paris (FR)	Non
Supabase	Base de données, authentification, stockage de fichiers	eu-west-3 (Paris)	Non
Amazon SES (AWS)	Envoi des e-mails transactionnels	eu-west-3 (Paris)	Non
Mistral AI (SAS, France)	Assistant IA : compréhension des questions et rédaction des réponses, uniquement pour les Clients qui l'activent	Union européenne	Non

Chaîne de sous-traitance intégralement située dans l'Union européenne : aucun transfert hors UE à déclarer.

Chaque sous-traitant ultérieur est lié à Antorya par un accord de traitement conforme à l'article 28 du RGPD (DPA Scaleway, DPA Supabase, AWS DPA, DPA Mistral AI). Antorya conserve une copie de ces accords et les tient à disposition du Client sur demande.

Conditions particulières à l'assistant IA (Mistral AI)

Mistral AI n'intervient que pour les Clients qui activent l'assistant IA depuis leur espace. Cette activation, horodatée et rattachée à l'administrateur qui l'effectue, vaut autorisation spécifique du recours à ce sous-traitant ultérieur au sens de l'article 28.2 du RGPD, pour les administrateurs comme pour les salariés du Client. Le Client peut en demander la désactivation à tout moment.

Finalité : comprendre les questions des administrateurs du Client et, depuis leur espace collaborateur, de ses salariés, puis rédiger les réponses ; les chiffres sont calculés par Antorya. Données transmises : la question et les seules données nécessaires à la réponse, dans la limite des droits de l'administrateur qui interroge l'assistant (modules autorisés), notamment soldes de congés, absences et leur type (y compris l'arrêt maladie, sans aucun motif médical), effectifs, contrats, rémunérations et notes de frais. Pour un salarié, l'assistant ne traite que les données qui le concernent personnellement et la convention collective applicable. Lorsque ce salarié est désigné dans la plateforme comme responsable hiérarchique, l'assistant traite en outre, pour les seuls salariés qu'il encadre directement, leurs soldes de congés, leurs absences, leur type et leur statut (y compris l'arrêt maladie, sans motif ni justificatif), les éléments de leur contrat et ses échéances, et les demandes en attente de sa validation, à l'exclusion de toute rémunération. Il ne traite jamais les données d'un autre salarié. Ne sont jamais transmis : les justificatifs, les informations médicales, les dossiers disciplinaires et les comptes rendus d'entretien.

Conservation : Antorya ne conserve pas les conversations ; seul un compteur du nombre de questions par mois est tenu, par organisation pour les administrateurs et par salarié pour les salariés. Mistral AI s'engage contractuellement à ne pas utiliser ces données pour entraîner ses modèles et ne les conserve que le temps strictement nécessaire à la détection des abus, dans la limite de trente (30) jours, puis les supprime.

Annexe 3 — Mesures techniques et organisationnelles

Conformément à l'article 32 du RGPD, Antorya met en œuvre les mesures de sécurité suivantes.

Cloisonnement et contrôle d'accès

- Cloisonnement par organisation cliente : Row Level Security (RLS) activée sur l'ensemble des tables, selon un modèle « deny by default » ; contrôle d'accès fondé sur l'identité authentifiée de l'utilisateur, jamais sur un identifiant fourni par le client.
- Cloisonnement des données de santé : le justificatif d'arrêt de travail est réservé au collaborateur concerné et aux administrateurs RH habilités du Client ; le responsable hiérarchique n'a accès qu'au fait de l'absence, non au justificatif.
- Gestion des secrets : la clé de service est strictement cantonnée au serveur ; seules les variables non sensibles sont exposées au navigateur.

Chiffrement

- Chiffrement des données au repos (AES-256), y compris des sauvegardes.
- Chiffrement des données en transit (HTTPS/TLS).

Authentification et sessions

- Authentification par jetons avec rotation des jetons d'accès et de rafraîchissement ; mots de passe stockés sous forme hachée ; invalidation complète de la session à la déconnexion.
- Limitation du débit (rate limiting) sur les points d'accès par lien (jetons d'onboarding et de signature), ne comptabilisant que les tentatives en échec afin de bloquer le balayage de jetons sans gêner un accès légitime. L'authentification est en outre protégée nativement par le fournisseur d'identité.

Gestion des documents téléversés

- Stockage dans des espaces privés (jamais publics), accès uniquement par liens signés de courte durée générés côté serveur ; noms de fichiers aléatoires générés côté serveur.
- Validation du type réel des fichiers par analyse de signature binaire (et non du type déclaré par le client) ; taille maximale par fichier.
- Analyse antivirus de tous les fichiers téléversés, réalisée au sein de l'infrastructure d'Antorya sans transmission à un tiers. Tant qu'un fichier n'a pas été déclaré sain, son accès est refusé ; tout fichier détecté comme infecté est bloqué et supprimé.
- Minimisation : les pièces éphémères (justificatif d'identité, attestation…) sont supprimées après extraction de la donnée utile.

Journalisation, confidentialité et effacement

- Messages d'erreur génériques en production ; aucune donnée personnelle dans les journaux applicatifs.
- Droit à l'effacement : suppression réelle (hard-delete) de la fiche du collaborateur et du compte d'authentification associé ; purges automatiques planifiées.

Sécurité de l'infrastructure

- En-têtes de sécurité HTTP (CSP, HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy).
- Automatisation de la purge des données à l'expiration du délai de 90 jours suivant la fin du contrat.
- Hébergement auprès de prestataires assurant un haut niveau de disponibilité et des sauvegardes chiffrées régulières (voir Annexe 2).

Signatures

Fait en deux exemplaires, chaque Partie reconnaissant avoir reçu le sien.

Pour Antorya (Toovent) — sous-traitant	Pour le Client — responsable de traitement
Nom :	Nom :
Qualité :	Qualité :
Date :	Date :
Signature :	Signature :

Toovent — 200 rue de la Croix-Nivert, 75015 Paris · rgpd@tolipo.fr