E2I VOIP

Solutions de téléphonie IP et communications d'entreprise

E2I VOIP

ACCORD DE SOUS-TRAITANCE RGPD

Document contractuel

Opérateur de services télécom · Spécialiste des DOM

ENTRÉE EN VIGUEUR

30 août 2026

v1.2 · Alban RENIER · E2I

ACCORD DE SOUS-TRAITANCE RGPD

Annexe de conformité RGPD au sens de l'article 28 du Règlement (UE) 2016/679 — conclu entre E2I (sous-traitant) et le Client (responsable de traitement).

Article 1 — Parties et objet

Cette annexe relative au traitement des données (le « DPA ») est conclue entre :

- le Client identifié dans la Commande, en qualité de responsable de traitement pour les Traitements décrits en Annexe 1 (le « Responsable de traitement » ou le « Client ») ;
- Alban RENIER, entrepreneur individuel, sous le nom commercial E2I ASSISTANCE et la marque E2I VOIP, SIRET 517 434 577 00014, 23 chemin Troubiran, 97300 Cayenne, en qualité de sous-traitant (le « Sous-traitant » ou « E2I »).

Le DPA encadre les traitements de Données à caractère personnel qu'E2I réalise pour le compte du Client dans le cadre des Services.

Article 2 — Cadre contractuel et ordre de priorité

Le DPA fait partie du Contrat. Il s'applique pendant toute la durée où E2I traite des Données personnelles pour le compte du Client.

En cas de contradiction sur la protection des Données personnelles traitées pour le compte du Client, le DPA prévaut sur les Conditions particulières, puis sur les CGV. La Commande prévaut si elle renforce expressément les garanties du DPA ou précise le Traitement, sans réduire une obligation impérative.

Si des Clauses contractuelles types de la Commission européenne sont signées pour un transfert international, elles priment sur les questions qu'elles couvrent.

Article 3 — Définitions

Les termes « Données à caractère personnel », « Traitement », « Personne concernée », « Responsable du traitement », « Sous-traitant », « Sous-traitant ultérieur », « Violation de données à caractère personnel » et « Autorité de contrôle » sont définis par le règlement (UE) 2016/679, dit « RGPD ».

Pour le DPA :

- « Données Client » : les Données personnelles traitées par E2I pour le compte du Client ;
- « Instruction documentée » : une instruction relative au Traitement consignée dans le Contrat, la Commande, un ticket, un courrier électronique ou tout autre support écrit accepté ;
- « Services » : les prestations VoIP, IPBX, Trunk SIP, numérotation, support, hébergement, sauvegarde, intégration ou services associés souscrits ;
- « Mesures de sécurité » : les mesures techniques et organisationnelles décrites en Annexe 2.

Article 4 — Rôles respectifs des parties

Le Client définit les finalités et les moyens essentiels des Traitements décrits en Annexe 1. Il agit comme Responsable du traitement.

E2I traite les Données Client pour fournir les Services. Elle agit comme Sous-traitant, selon les Instructions documentées du Client et dans les limites du Contrat.

Chaque partie respecte ses obligations prévues par le RGPD et la législation applicable. Aucune clause ne transfère à E2I les obligations que le RGPD impose au Client en sa qualité de Responsable du traitement.

Article 5 — Traitements pour lesquels E2I agit comme responsable de traitement

Le DPA ne s'applique pas aux Traitements où E2I définit ses propres finalités et agit comme responsable de traitement indépendant, comme :

- gestion des prospects, Clients, contacts et représentants ;
- devis, Commandes, contrats, facturation, comptabilité et recouvrement ;
- gestion de la relation commerciale et du support ;
- sécurité de ses systèmes, contrôle des accès et journalisation de ses interventions ;
- prévention, détection et traitement de la fraude ;
- gestion des réclamations et défense de ses droits ;
- respect de ses obligations légales, fiscales, comptables, réglementaires ou liées aux communications électroniques.

Ces Traitements relèvent de la politique de confidentialité E2I et de la réglementation applicable.

Si un ticket, une pièce jointe ou une intervention de support contient des Données que le Client confie à E2I exclusivement pour diagnostiquer ou administrer son PBX, E2I agit comme Sous-traitant pour ce contenu technique. E2I traite les métadonnées nécessaires à la gestion de la relation, à la preuve des interventions, à la facturation et à la sécurité pour ses propres finalités.

Article 6 — Qualification particulière des CDR et données de trafic

La qualification des relevés de communications, journaux et données de trafic dépend de leur finalité.

E2I agit comme responsable de traitement indépendant pour facturer, prouver les communications, sécuriser, lutter contre la fraude, traiter les contestations et respecter ses obligations propres.

E2I agit comme sous-traitant quand elle met à disposition, héberge, organise ou exploite ces données selon les instructions documentées du Client pour ses propres besoins.

La qualification se détermine par finalité et ne se déduit pas de la seule nature technique de la donnée.

Article 7 — Caractéristiques du Traitement

L'objet, la durée, la nature, les finalités, les catégories de Données et de Personnes concernées sont décrits en Annexe 1 et complétés par la Commande.

Le Client informe E2I avant toute utilisation impliquant des catégories de Données, des finalités ou des risques non prévus. E2I peut refuser cette extension. E2I peut aussi la conditionner à une analyse, des garanties complémentaires, un avenant ou une offre adaptée.

Article 8 — Obligations générales du Client

Le Client garantit comme :

- disposer d'une base légale pour chaque Traitement ;
- respecter les principes de licéité, loyauté, transparence, minimisation et limitation des durées ;
- fournir aux Personnes concernées les informations requises ;
- traiter leurs demandes et respecter leurs droits ;
- définir les habilitations et contrôler ses Utilisateurs ;
- s'assurer que ses Instructions sont licites ;
- réaliser une analyse d'impact relative à la protection des données si elle est requise ;
- accomplir les consultations, formalités et obligations sociales ou sectorielles applicables ;
- ne confier à E2I que les Données nécessaires aux Services.

Le Client est responsable de la licéité des annuaires, contacts, messages, scénarios, enregistrements d'appels, campagnes et données introduits dans l'IPBX.

Article 9 — Instructions documentées

E2I ne traite les Données Client que sur Instruction documentée. Cette règle s'applique aussi aux transferts. E2I peut déroger à cette règle si un droit de l'Union européenne ou d'un État membre applicable à E2I l'y oblige.

Dans ce cas, E2I informe le Client de cette obligation avant le Traitement. Une interdiction légale pour des motifs importants d'intérêt public peut toutefois dispenser E2I de cette information.

Le Contrat, la Commande, la configuration convenue et l'usage normal des Services définissent les instructions initiales. E2I valide toute instruction supplémentaire modifiant le périmètre, les coûts, les risques ou les mesures techniques. Un devis ou un avenant formalise cette validation si nécessaire.

Article 10 — Instruction contraire au droit applicable

E2I avertit immédiatement le Client si elle estime qu'une instruction viole le RGPD ou une autre règle de protection des Données.

E2I peut suspendre l'exécution de l'instruction concernée. Elle attend sa modification, sa confirmation licite ou des preuves levant le doute. Cette suspension n'est pas un manquement de la part d'E2I.

Article 11 — Confidentialité des personnes autorisées

E2I s'assure que les personnes autorisées à traiter les Données Client :

- y accèdent seulement pour accomplir leurs fonctions ;
- respectent une obligation de confidentialité contractuelle ou légale ;
- suivent une formation à la sécurité et à la protection des Données ;
- appliquent les procédures d'accès, d'authentification et de traçabilité.

L'obligation de confidentialité continue après la fin de leur habilitation et du Contrat.

Article 12 — Sécurité du Traitement

E2I met en œuvre des mesures techniques et organisationnelles adaptées au risque, comme prévu par l'article 32 du RGPD. L'Annexe 2 décrit les principales mesures.

Le niveau de sécurité tient compte de l'état des connaissances et des coûts de mise en œuvre. Il dépend aussi de la nature, de la portée, du contexte, des finalités et des risques pour les droits et libertés des personnes.

Les Mesures de sécurité peuvent évoluer pour maintenir ou améliorer la protection.

Article 13 — Sécurité relevant du Client

Le Client reste responsable de la sécurité de son environnement et de l'usage des Services, par exemple :

- Gérer ses Utilisateurs et leurs habilitations ;
- Protéger les comptes, mots de passe et moyens d'authentification ;
- Sécuriser son réseau, pare-feu, postes, terminaux et accès Internet ;
- Configurer les fonctions accessibles à ses administrateurs ;
- Informer et sensibiliser son personnel ;
- Contrôler les exports et destinataires ;
- Réaliser les sauvegardes et archivages non inclus dans le Service.

Le Client notifie sans délai à E2I toute compromission ou anomalie affectant les Données Client.

Article 14 — Gestion des habilitations

E2I applique le principe du moindre privilège. Elle attribue les accès techniques selon les fonctions, les révise périodiquement et les retire quand ils deviennent inutiles.

E2I protège les accès administratifs par des mécanismes d'authentification adaptés au risque. Elle peut imposer au Client une authentification renforcée ou restreindre un accès à risque.

Si le Client dispose d'un accès de co-administration, il assume les traitements et modifications réalisés via cet accès. Il veille à leur traçabilité.

Article 15 — Journalisation et traçabilité

E2I journalise les accès administratifs, les interventions techniques, les anomalies et les événements de sécurité. Cette journalisation tient compte des capacités des Services et du niveau de risque.

Les journaux sont protégés contre tout accès non autorisé. E2I les conserve pendant une durée adaptée aux besoins de sécurité, de preuve et de conformité.

Les journaux peuvent contenir des Données personnelles. Seules les personnes habilitées y accèdent. E2I les communique au Client uniquement quand cela est nécessaire, après avoir protégé les informations sur les tiers et les infrastructures partagées.

Article 16 — Sauvegardes

Quand la sauvegarde managée est incluse, E2I réalise les sauvegardes définies dans les Conditions particulières Services VoIP et IPBX. Cela comprend une sauvegarde quotidienne avec une rétention glissante de sept jours pour les systèmes concernés.

Les sauvegardes sont protégées par des contrôles d'accès et des mesures proportionnées au risque. Elles servent uniquement à assurer la continuité, la restauration, la sécurité et les finalités convenues.

La sauvegarde standard n'est pas un archivage réglementaire. Le Client reste responsable de toute conservation longue durée ou obligation sectorielle non prévue par la Commande.

Article 17 — Sous-traitants ultérieurs : autorisation générale

Le Client autorise E2I à recruter les Sous-traitants ultérieurs nécessaires à la fourniture des Services : opérateurs de communications électroniques, hébergeurs, éditeurs, fournisseurs d'infrastructure, sauvegarde, supervision et support.

E2I sélectionne des prestataires offrant des garanties suffisantes. Elle leur impose, par contrat ou autre acte juridique, des obligations de protection des Données au moins équivalentes pour le périmètre confié.

E2I reste pleinement responsable envers le Client de l'exécution des obligations du Sous-traitant ultérieur, dans les conditions de l'article 28 du RGPD.

Article 18 — Information sur les Sous-traitants ultérieurs

La liste des Sous-traitants ultérieurs figure en Annexe 3. Après publication, E2I la tient à disposition sur une page stable de son site, dans l'espace Client ou par communication écrite.

Cette liste indique, autant que possible, l'identité, la fonction et le lieu principal de Traitement. Elle précise si un transfert hors Espace économique européen existe.

E2I informe le Client de l'ajout ou du remplacement d'un Sous-traitant au moins quinze jours calendaires avant le début du Traitement. En cas d'urgence liée à la sécurité, à la continuité du service ou à une décision du fournisseur, E2I informe le Client dès que possible.

Article 19 — Objection à un Sous-traitant ultérieur

Pendant ce délai, le Client peut s'opposer par écrit. Cette objection doit être précise et fondée sur des motifs sérieux liés à la protection des Données.

Les parties cherchent ensemble et de bonne foi une solution raisonnable. Elles peuvent prévoir une mesure complémentaire, une configuration alternative ou, si cela reste techniquement et commercialement possible, un autre prestataire.

Si aucune solution n'est possible, E2I peut renoncer au Sous-traitant contesté. Chaque partie peut aussi mettre fin au seul Service affecté. Les sommes correspondant aux prestations déjà exécutées et aux engagements irrévocables non liés à la protection des Données restent dues.

Une objection générale, commerciale ou sans motif documenté ne suspend pas le changement.

Article 20 — Lieux de Traitement

Pour les infrastructures qu'elle gère directement, E2I utilise Amazon Web Services dans la région Paris `eu-west-3` et OVHcloud en France, à Roubaix et Gravelines. Ses serveurs de fichiers internes se trouvent dans ses locaux.

Les lieux applicables à chaque Service figurent dans la liste des Sous-traitants ultérieurs, la Commande ou la documentation contractuelle. Le lieu de stockage principal ne détermine pas les accès de support ou les sous-traitants du fournisseur.

Ce DPA ne garantit pas, à lui seul, que toutes les Données et les accès de support restent exclusivement en France ou dans l'Union européenne. Cet engagement n'existe que s'il est expressément stipulé après vérification de toute la chaîne de Traitement.

Article 21 — Transferts hors Espace économique européen

E2I ne transfère pas les Données Client hors de l'Espace économique européen. Elle n'autorise un tel accès que sur Instruction documentée ou quand il est nécessaire au Service et encadré par le chapitre V du RGPD.

Le transfert repose sur l'un des mécanismes suivants :

- une décision d'adéquation de la Commission européenne ;
- les Clauses contractuelles types adoptées par la Commission européenne ;
- des règles d'entreprise contraignantes approuvées ;
- ou tout autre mécanisme légalement valable.

Quand le transfert s'appuie sur l'article 46 du RGPD, E2I réalise ou obtient une analyse d'impact si nécessaire. E2I met alors en œuvre les mesures supplémentaires appropriées.

Certains Services impliquent un accès ou un stockage hors EEE. C'est le cas de Resend, qui stocke certains contenus et journaux d'e-mails transactionnels aux États-Unis. Des sous-traitants ou accès de support hors EEE peuvent aussi intervenir chez certains éditeurs ou fournisseurs cloud. Les garanties applicables sont précisées en Annexe 3 et dans les DPA des fournisseurs.

Article 22 — Demandes d'autorités étrangères

E2I examine toute demande d'accès d'une autorité. Elle ne communique des Données que si la loi l'y oblige.

Si la loi le permet, E2I informe le Client avant toute divulgation. E2I limite la communication aux Données strictement requises et documente la demande et sa réponse.

E2I conteste toute demande manifestement irrégulière quand elle dispose de motifs raisonnables et de voies de recours appropriées.

Article 23 — Droits des Personnes concernées

Selon la nature du Traitement, E2I aide le Client à répondre aux demandes d'exercice des droits. E2I met en place des mesures techniques et organisationnelles appropriées, dans la mesure du possible.

Quand E2I reçoit directement une demande sur un Traitement dont le Client est Responsable, elle la transmet au point de contact désigné. E2I ne répond pas sur le fond, sauf Instruction documentée ou obligation légale.

Le Client reste responsable d'identifier la personne, d'analyser la demande, de prendre la décision et de respecter les délais légaux.

Article 24 — Modalités d'assistance aux droits

E2I met à disposition les fonctions d'accès, d'export, de rectification, de suppression et de restriction dans le Service. Si ces fonctions ne suffisent pas, le Client envoie une demande écrite, précise et sécurisée.

E2I traite la demande dans un délai compatible avec celui du Client. Ce délai tient compte de la complexité de la demande et des informations disponibles.

L'assistance courante prévue par le Service est incluse. Les opérations complexes, répétitives, spécifiques ou liées à une configuration du Client peuvent être facturées. E2I ne fait pas obstacle aux obligations impératives du Client.

Article 25 — Analyses d'impact et consultation préalable

E2I fournit au Client les informations raisonnablement disponibles pour réaliser une analyse d'impact sur la protection des Données ou une consultation préalable. Ces informations dépendent de la nature du Traitement et de celles dont E2I dispose.

Le Client reste responsable de la réalisation, du contenu et de la mise à jour de l'analyse. Il reste aussi responsable de la consultation de l'Autorité de contrôle.

E2I peut établir un devis pour toute assistance approfondie, atelier, questionnaire spécifique ou production documentaire hors standard.

Article 26 — Violation de Données Client

E2I notifie au Client toute Violation de Données Client dès qu'elle en a connaissance.

E2I adresse cette notification au contact de sécurité ou de protection des Données indiqué par le Client. Elle contient, selon les informations disponibles :

- la nature de la Violation ;

- les catégories et le nombre approximatif de Personnes concernées ;
- les catégories et le nombre approximatif d'enregistrements concernés ;
- les conséquences probables ;
- les mesures prises ou proposées pour corriger la Violation et limiter ses effets ;
- le contact pour obtenir des informations complémentaires.

Si toutes les informations ne sont pas disponibles immédiatement, E2I les transmet par étapes et sans retard injustifié.

Article 27 — Gestion et notification réglementaire des Violations

E2I prend les mesures raisonnables de confinement, de remédiation, d'investigation et de prévention dans son périmètre. Elle documente cet incident de façon appropriée.

Le Client décide s'il doit notifier la Violation à une Autorité de contrôle ou informer les Personnes concernées. Il réalise ces formalités dans les délais légaux.

E2I ne notifie pas l'Autorité ni les Personnes au nom du Client. E2I agit seulement si le Client envoie une Instruction écrite et si E2I accepte ses modalités. Cette Instruction ne transfère pas la responsabilité réglementaire du Client.

Les parties coordonnent leurs communications. Elles protègent ainsi la sécurité de l'enquête et la cohérence des informations.

Article 28 — Assistance réglementaire et coopération

E2I coopère raisonnablement avec le Client et l'Autorité de contrôle compétente. Cette coopération porte sur les questions liées aux Traitements couverts par le DPA.

Elle fournit les informations nécessaires pour prouver qu'elle respecte l'article 28 du RGPD.

Article 29 — Registre des activités de Traitement

E2I tient un registre des catégories d'activités de Traitement réalisées pour ses Clients quand la loi l'exige. Ce registre répond aux exigences de l'article 30 du RGPD.

Le Client tient son propre registre en tant que Responsable du traitement. Il y décrit les Services et les Sous-traitants concernés.

Article 30 — Audits

Le Client peut vérifier le respect du DPA une fois par an. Il peut réaliser un contrôle supplémentaire en cas d'incident significatif, de demande d'une Autorité ou d'indice sérieux de non-conformité.

L'audit suit une approche graduée. Il comprend l'examen de la documentation, des réponses à un questionnaire raisonnable et un entretien à distance. L'audit sur site a lieu seulement si nécessaire.

Le Client envoie un préavis d'au moins trente jours. Il définit le périmètre et choisit un auditeur indépendant, qualifié et lié par un accord de confidentialité. L'audit se

déroule pendant les heures ouvrées. Il ne perturbe pas les Services. Il n'ouvre pas l'accès aux Données d'autres Clients, aux secrets de sécurité ou aux infrastructures partagées.

Article 31 — Coûts et conclusions d'audit

Le Client supporte l'intégralité des coûts de l'audit, y compris les frais d'auditeur externe, de déplacement et de vérification. Ce principe s'applique à tous les audits, sans exception : audit initial, audit de suivi, deuxième passage pour vérifier la correction des non-conformités, ou contrôle supplémentaire. E2I ne prend en charge aucun coût d'audit, de remédiation externe ou de revérification, quel qu'en soit le motif ou le résultat. Le Client demandeur assume seul l'ensemble des frais liés à la demande et au déroulement de l'audit.

Le Client communique le rapport à E2I. Les parties définissent ensemble un plan de remédiation proportionné. Les informations recueillies restent confidentielles. Elles servent uniquement à assurer la conformité et la sécurité.

Article 32 — Sort des Données à la fin du Service

À la fin du Service, E2I restitue ou rend accessibles les Données Client exportables. Cette accessibilité dure pendant la période de réversibilité de trente jours prévue par les CGV. Elle suit le choix et les Instructions du Client.

À la fin de cette période, E2I supprime ou anonymise les Données Client devenues inutiles. E2I conserve ces données uniquement en cas d'obligation légale ou d'Instruction licite contraire.

Les copies des sauvegardes sont supprimées selon leur cycle de rotation. Pour les sauvegardes standard, ce délai ne dépasse pas sept jours. Pendant cette période, ces copies restent protégées et ne servent à aucune autre fin.

Article 33 — Données conservées par E2I pour ses finalités propres

La suppression prévue à l'article 32 ne s'applique pas aux Données qu'E2I conserve légitimement comme responsable de traitement indépendant. Il s'agit des factures, pièces comptables, preuves contractuelles, éléments de sécurité, prévention de la fraude, contentieux et CDR nécessaires à ses obligations propres.

Ces Données sont isolées du Service actif. Leurs durées de conservation sont définies par finalité et encadrées par la politique de confidentialité d'E2I.

Article 34 — Réversibilité et moyens d'export

E2I fournit les exports natifs et les informations nécessaires prévus par les CGV et les Conditions particulières.

E2I ne transmet pas les comptes fournisseurs, secrets API, identifiants mutualisés, outils internes, informations d'autres Clients et secrets de sécurité.

Un devis peut être établi pour la conversion vers un format non disponible nativement, l'assistance à la migration ou la reconstitution de Données.

Article 35 — Données sensibles et secteurs réglementés

Le Client informe E2I avant d'utiliser les Services pour traiter à grande échelle des catégories particulières de Données, des données relatives aux condamnations ou des données soumises à un régime sectoriel renforcé.

Les parties vérifient avant activation que les Services, hébergeurs, mesures et certifications répondent aux exigences applicables. Cette vérification concerne les données de santé, les services d'urgence, les établissements médico-sociaux, les services financiers et toute activité soumise à des exigences spécifiques.

Un Service standard n'implique aucun engagement de certification HDS, de qualification SecNumCloud ou de conformité à un référentiel sectoriel non mentionné dans la Commande.

Article 36 — Modifications du DPA

E2I peut mettre à jour le DPA pour refléter toute évolution légale, réglementaire, technique ou organisationnelle.

Le sous-traitant notifie au Client toute modification substantielle d'un Contrat en cours sur un support durable avec un préavis raisonnable. Cette modification ne réduit pas les droits impératifs du Client ni le niveau global de protection sans base contractuelle valable.

Article 37 — Responsabilité

Chaque partie répond de ses propres manquements. La répartition contractuelle de responsabilité n'affecte pas les droits des Personnes concernées ni les pouvoirs des Autorités de contrôle.

Dans les relations entre les parties, les limitations et exclusions des CGV s'appliquent si le RGPD et le droit applicable le permettent. Aucune limitation ne s'applique si la loi l'interdit.

Article 38 — Contact relatif à la protection des Données

Les parties adressent les notifications relatives au DPA aux contacts désignés dans la Commande ou à ceux qu'elles désignent par écrit ultérieurement.

Le Client maintient à jour un contact opérationnel pour les demandes de droits et un contact disponible pour les incidents de sécurité.

E2I propose un formulaire de réclamation RGPD sur son site Internet. C'est le canal officiel pour les demandes liées à la protection des Données. E2I ne publie pas d'adresse e-mail dédiée au RGPD. Ce choix limite le spam, l'hameçonnage et les sollicitations automatisées.

Les Personnes concernées conservent tous leurs droits sans adresse e-mail dédiée. Elles peuvent aussi envoyer leurs demandes par courrier postal au siège d'E2I.

Article 39 — Entrée en vigueur

Ce DPA prend effet le 30 août 2026. Il porte le numéro de version v1.1.