Accord relatif au Traitement des Données

Version : Octobre 2026

Ibexa AS, Askekroken 11, 0277 Oslo, Norway

ARTICLE 1. CHAMP D'APPLICATION 3
ARTICLE 2. RÔLES DES PARTIES 3
ARTICLE 3. DÉFINITIONS ET INTERPRÉTATION 4
ARTICLE 4. INSTRUCTIONS DE TRAITEMENT 4
ARTICLE 5. CONFORMITÉ AUX LOIS SUR LA PROTECTION DES DONNÉES 5
ARTICLE 6. CATÉGORIES PARTICULIÈRES DE DONNÉES À CARACTÈRE PERSONNEL 5
ARTICLE 7. CONFIDENTIALITÉ 5
ARTICLE 8. MESURES DE SÉCURITÉ 5
ARTICLE 9. RECOURS À DES SOUS-TRAITANTS 6
ARTICLE 10. UTILISATION DE TIERS PAR LE RESPONSABLE DE TRAITEMENT 6
ARTICLE 11. TRANSFERTS INTERNATIONAUX DE DONNÉES 7
ARTICLE 12. ASSISTANCE AU RESPONSABLE DE TRAITEMENT 7
ARTICLE 13. DIVULGATION RÉGLEMENTAIRE 7
ARTICLE 14. DROITS DES PERSONNES CONCERNÉES 8
ARTICLE 15. VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL 8
ARTICLE 16. AUDIT ET VÉRIFICATION DE CONFORMITÉ 8
16.1 AUDIT 8
16.2 TEST DE PÉNÉTRATION 10
ARTICLE 17. CONSERVATION DES DONNÉES 10
ARTICLE 18. DÉLÉGUÉ À LA PROTECTION DES DONNÉES 10

ARTICLE 1. CHAMP D'APPLICATION

Le présent Accord relatif au Traitement des Données (« DPA ») est conclu entre le Client (« Responsable de traitement ») et le Prestataire (« Sous-traitant »). Le présent DPA fait partie intégrante du Contrat entre les Parties et y est incorporé par référence.

Le présent DPA régit le traitement des données à caractère personnel par le Sous-traitant pour le compte du Responsable de traitement dans le cadre de la fourniture des Services.

Le Sous-traitant n'agit pas en qualité de Responsable de traitement ou de Responsable conjoint pour les traitements couverts par le présent DPA.

ARTICLE 2. RÔLES DES PARTIES

Le Client reconnaît et accepte qu'il est seul responsable de déterminer la base légale du traitement des données à caractère personnel, y compris les données à caractère personnel relatives à ses employés ou à son personnel ainsi que de la fourniture de toutes les notifications requises et de l'obtention de tous les consentements nécessaires, comme l'exigent les lois applicables sur la protection des données.

Le Prestataire peut fournir une assistance directement aux Utilisateurs du Client uniquement dans le but de fournir les Services. Dans ce cadre, le Prestataire traitera toutes les données à caractère personnel échangées en qualité de Sous-traitant agissant pour le compte du Client et n'utilisera pas ces données à caractère personnel à ses propres fins, sauf si ces données sont agrégées et anonymisées ou autrement traitées conformément à la loi applicable.

Le Prestataire peut fournir des services d'authentification sur plusieurs Produits souscrits par le Client, notamment via une fonctionnalité d'authentification unique (SSO). À cette fin, le Prestataire peut traiter les identifiants et les informations de compte associées à des Utilisateurs du Client uniquement pour authentifier les utilisateurs, reconnaître les comptes liés et faciliter l'accès à ces Produits.

Nonobstant ce qui précède, le Prestataire agit en tant que Responsable de traitement indépendant concernant les données à caractère personnel traitées pour ses propres besoins légitimes, y compris mais sans s'y limiter :

- la gestion de compte et l'administration de la relation Client ;
- la facturation et le traitement des paiements ;
- la comptabilité financière, la conformité fiscale et les obligations de tenue de registres ;
- le maintien de la sécurité, de l'intégrité et du fonctionnement de l'infrastructure sous-jacente du Prestataire ;
- la prévention de la fraude, la détection des abus et l'application du Contrat ; et
- le respect des obligations légales et réglementaires applicables.

Pour éviter tout doute, les données à caractère personnel traitées par le Prestataire en sa qualité de Responsable de traitement indépendant sont traitées pour les propres fins du Prestataire et ne sont pas soumises aux termes du présent DPA, sauf si la loi applicable en dispose autrement.

ARTICLE 3. DÉFINITIONS ET INTERPRÉTATION

Tous les termes définis dans le Règlement Général sur la Protection des Données (RGPD - Règlement (UE) 2016/679 du 27 avril 2016) ont le sens qui leur est donné dans le RGPD, sauf disposition contraire dans le présent DPA. En cas de conflit, les lois sur la protection des données prévalent sur les dispositions contractuelles.

ARTICLE 4. INSTRUCTIONS DE TRAITEMENT

Le Sous-traitant ne traite les données à caractère personnel que sur instructions documentées du Responsable de traitement. Les instructions sont réputées documentées à travers le présent DPA, les activités de traitement de données spécifiques aux Produits et l'utilisation légitime des Services. Le Sous-traitant informe le Responsable de traitement si une instruction viole les lois applicables sur la protection des données.

Conformément à la réglementation, le Sous-traitant s'engage à ne traiter les données à caractère personnel que dans la mesure nécessaire aux fins de l'exécution des Services. Sauf accord express, préalable et écrit du Responsable de traitement, le

Sous-traitant s'abstient de traiter les données à caractère personnel à d'autres fins que celles prévues au Contrat.

ARTICLE 5. CONFORMITÉ AUX LOIS SUR LA PROTECTION DES DONNÉES

Chaque Partie doit se conformer à ses obligations respectives en vertu des lois applicables sur la protection des données. Le Sous-traitant doit mettre en œuvre des politiques et mesures internes appropriées pour être conforme au présent DPA et au RGPD.

ARTICLE 6. CATÉGORIES PARTICULIÈRES DE DONNÉES À CARACTÈRE PERSONNEL

Le Responsable de traitement s'abstient de traiter des catégories particulières de données à caractère personnel telles que définies à l'Article 9 du RGPD. Si le Responsable de traitement choisit de traiter de telles données, il le fera sous sa seule responsabilité, en veillant au respect de toutes les exigences applicables, y compris l'obtention du consentement explicite de la personne concernée, la réalisation d'analyses d'impact sur la protection des données (AIPD) et la mise en œuvre de mesures de sécurité techniques et organisationnelles appropriées.

ARTICLE 7. CONFIDENTIALITÉ

Le Sous-traitant s'assure que tout le personnel ayant accès aux données à caractère personnel soit soumis à une obligation de confidentialité et reçoive une formation appropriée à la protection des données.

ARTICLE 8. MESURES DE SÉCURITÉ

Le Sous-traitant met en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris des

mesures garantissant la confidentialité, l'intégrité, la disponibilité et la résilience. Les détails sont décrits dans les Conditions Spécifiques de chaque Produit.

ARTICLE 9. RECOURS À DES SOUS-TRAITANTS

Le Responsable de traitement autorise le Sous-traitant à faire appel aux sous-traitants ultérieurs figurant dans les Conditions Spécifiques des Produits auxquels il a souscrit.

Le Sous-traitant peut désigner des sous-traitants ultérieurs additionnels pour des activités de traitement spécifiques et doit notifier le Responsable de traitement de tout ajout ou remplacement envisagé. Cette notification doit inclure les activités de traitement concernées ainsi que l'identité et les coordonnées du sous-traitant ultérieur. Le Responsable de traitement peut s'opposer dans un délai de trente (30) jours à compter de la réception de la notification, étant entendu que ces objections doivent être de nature raisonnable.

Si le Responsable de traitement s'oppose expressément au changement de sous-traitant ultérieur dans les conditions et délais susmentionnés et si aucune solution ne peut être trouvée, le Responsable de traitement peut décider de résilier le Contrat avec le Sous-traitant avec un préavis écrit de trente (30) jours ouvrés. Dans ce cas, le Responsable de traitement paiera au Sous-traitant tous les Services déjà exécutés pour son compte jusqu'à la date d'effet de la résiliation.

ARTICLE 10. UTILISATION DE TIERS PAR LE RESPONSABLE DE TRAITEMENT

Le Sous-traitant peut recommander certains tiers au Responsable de traitement, notamment pour permettre le transfert de données à caractère personnel entre le Sous-traitant et le tiers. Le Responsable de traitement demeure seul responsable de tout tiers qu'il configure ou active et s'assure de conclure un accord de traitement de données approprié avec ces tiers.

ARTICLE 11. TRANSFERTS INTERNATIONAUX DE DONNÉES

Les transferts de données à caractère personnel en dehors de l'Espace Economique Européen (EEE) ne peuvent avoir lieu que lorsque des mécanismes de transfert légaux sont en place, tels que des décisions d'adéquation ou des clauses contractuelles types.

ARTICLE 12. ASSISTANCE AU RESPONSABLE DE TRAITEMENT

Le Sous-traitant assiste le Responsable de traitement, compte tenu de la nature du traitement, pour :

- répondre aux demandes des personnes concernées ;
- réaliser des analyses d'impact sur la protection des données (AIPD) ;
- mener des consultations auprès des autorités de contrôle ;
- démontrer la conformité au titre des Articles 28 et 32 à 36 du RGPD.

Cette assistance est limitée à ce qui est raisonnable et proportionné et ne saurait exiger du Sous-traitant qu'il déploie des efforts disproportionnés.

ARTICLE 13. DIVULGATION RÉGLEMENTAIRE

Toute communication de données à caractère personnel par le Sous-traitant à une autorité de contrôle est strictement limitée aux cas où cette communication est requise par le droit de l'Union Européenne ou le droit d'un État membre. Le Sous-traitant en informe le Responsable de traitement sans délai injustifié, sauf si la loi l'interdit, et s'assure que toute divulgation est proportionnée, documentée et légalement justifiée.

ARTICLE 14. DROITS DES PERSONNES CONCERNÉES

Le Sous-traitant informe rapidement le Responsable de traitement de toute demande d'une personne concernée reçue directement et n'y répond pas sans autorisation. Le Sous-traitant fournit une assistance raisonnable pour permettre au Responsable de traitement de s'acquitter de ses obligations.

ARTICLE 15. VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel impactant le Responsable de traitement, sans délai injustifié. Ces informations seront aussi complètes que possible pour permettre au Responsable de traitement de respecter ses propres obligations de notification dans un délai de soixante-douze (72) heures. Dans ce cas, le Sous-traitant décrit notamment la nature de la violation de données, le nombre approximatif de personnes concernées, les conséquences probables, ainsi que les mesures prises pour remédier à la violation.

ARTICLE 16. AUDIT ET VÉRIFICATION DE CONFORMITÉ

16.1 AUDIT

Limite et fréquence des audits

Le Responsable de traitement (y compris l'ensemble de ses sociétés affiliées et entités du même groupe) peut effectuer un (1) seul audit par période de douze (12) mois consécutifs.

Modalités

Si le Responsable de traitement demande un audit lié à la protection des données à caractère personnel ou à la sécurité, le Responsable de traitement doit (i) notifier le

Sous-traitant au moins cinq (5) jours ouvrés avant cet audit par courrier électronique à security@ibexa.co et (ii) s'assurer que cette procédure n'interfère pas de manière déraisonnable avec les activités et opérations du Sous-traitant.

La notification sera accompagnée d'un document mentionnant les règles d'engagement qui incluront précisément les points suivants : (i) le périmètre de l'audit ; (ii) l'objectif de l'audit ; (iii) les domaines de l'audit (tels que définis par ISO 27001, ISO 27701, ISAE 3000 ou toute méthodologie d'audit équivalente) ; (iv) le nom et les coordonnées des auditeurs désignés et (v) le calendrier d'audit.

Le Sous-traitant aura le droit de demander une révision des règles d'engagement concernant (i) la compétence et/ou l'indépendance/l'impartialité des auditeurs, (ii) le calendrier de l'audit, (iii) le périmètre de l'audit si le Sous-traitant craint que l'audit n'affecte le service fourni à ses clients.

Questionnaires de sécurité et d'évaluation des risques

Afin d'éviter la multiplication des sollicitations informelles, toutes les demandes d'évaluation, de conformité ou questionnaires de sécurité émis par le Responsable de traitement ou l'une de ses entités/affiliées doivent être centralisées et adressées exclusivement à security@ibexa.co. Le Sous-traitant s'engage à répondre à un (1) questionnaire annuel standard d'évaluation de la sécurité et à la protection des données à caractère personnel par période de douze (12) mois, sous réserve que les informations demandées ne soient pas déjà couvertes par les certifications, rapports d'audit tiers (ex. ISO 27001, ISAE 3000) ou documentations mis à disposition par le Sous-traitant.

Frais et imputation des coûts

Les coûts de tout audit ou de tout questionnaire additionnel seront pris en charge par le Responsable de traitement. Tout audit sur site, audit supplémentaire, ou réponse à des questionnaires de sécurité excédant la limite annuelle susmentionnée (ou nécessitant des réponses sur mesure non couvertes par la documentation standard du Sous-traitant) fera l'objet d'une facturation au Responsable de traitement.

Le Responsable de traitement fournit au Sous-traitant une copie du rapport d'audit et permet au Sous-traitant d'y répondre. L'audit et ses résultats ne sauraient être interprétés comme une reconnaissance de responsabilité, d'une quelconque atteinte

à la sécurité ou à la confidentialité, ou comme un engagement du Sous-traitant à remédier à tout problème identifié lors de l'audit.

16.2 TEST DE PÉNÉTRATION

Sur demande écrite, le Sous-traitant fournit au Responsable de traitement un résumé du dernier rapport de test de pénétration.

Pour protéger l'intégrité, la disponibilité et la sécurité du Produit, le Responsable de traitement s'interdit d'effectuer ou d'autoriser un tiers à effectuer, un test de pénétration sans l'autorisation écrite préalable du Sous-traitant.

ARTICLE 17. CONSERVATION DES DONNÉES

Le Sous-traitant ne conserve les données à caractère personnel que pendant la durée nécessaire à la fourniture des Services et conformément aux instructions du Responsable de traitement, sauf si la conservation est requise par la loi.

À la résiliation du Contrat, le Sous-traitant doit, au choix du Responsable de traitement, restituer ou supprimer de manière sécurisée toutes les données à caractère personnel, à moins que la loi n'exige leur conservation. Une attestation de suppression sera fournie sur demande.

ARTICLE 18. DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Conformément à l'article 37 du RGPD, le Sous-traitant a désigné un délégué à la protection des données, qui peut être contacté à l'adresse électronique suivante : privacy@ibexa.co.

Le Responsable de traitement désignera, le cas échéant, un délégué à la protection des données et partagera cette information avec le Sous-traitant par tout moyen possible. À défaut, la personne de contact du Responsable de traitement sera

enregistrée comme personne de contact pour tout sujet lié à la protection des données.