

ANIKOP, SAS au capital de 69 000 euros, 150 Allée des Frênes, 69760 Limonest, RCS Lyon 493 220 479.

1. Objet

Le présent accord fixe les conditions dans lesquelles ANIKOP traite des données à caractère personnel pour le compte de ses clients, dans le cadre des solutions qu'elle leur fournit, conformément à l'article 28 du Règlement (UE) 2016/679 (« RGPD »).

Il fait partie intégrante du contrat conclu entre ANIKOP et le client (devis, bon de commande et conditions générales de la solution concernée). En cas de contradiction sur la protection des données personnelles, le présent accord prévaut.

2. Rôles des parties

Pour les traitements décrits en annexe, le client agit en qualité de **responsable de traitement** et ANIKOP en qualité de **sous-traitant**.

Le présent accord ne concerne pas les données qu'ANIKOP traite pour son propre compte (gestion de la relation commerciale, facturation, prospection), qui relèvent de la politique de confidentialité d'ANIKOP.

3. Description des traitements

La nature et la finalité des traitements, les catégories de données et de personnes concernées, ainsi que la durée des traitements, sont décrites dans l'annexe propre à chaque solution.

4. Instructions du client

ANIKOP traite les données uniquement sur instruction documentée du client. Le contrat, la configuration de la solution par le client et l'usage qu'il en fait constituent ces instructions.

Si ANIKOP estime qu'une instruction constitue une violation du RGPD ou d'une autre règle applicable en matière de protection des données, elle en informe immédiatement le client.

5. Confidentialité

ANIKOP veille à ce que les personnes autorisées à traiter les données soient tenues à une obligation de confidentialité et reçoivent la formation nécessaire en matière de protection des données.

6. Sécurité

ANIKOP 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 sont décrites dans l'annexe de chaque solution.

Le client reste responsable de la sécurité des accès qui lui sont confiés, notamment de la confidentialité de ses identifiants, ainsi que de la licéité des données qu'il saisit dans la solution.

7. Sous-traitants ultérieurs

Le client autorise ANIKOP à faire appel aux sous-traitants ultérieurs listés dans l'annexe de chaque solution.

ANIKOP informe le client de tout ajout ou remplacement de sous-traitant ultérieur au moins trente (30) jours avant sa prise d'effet. Le client peut s'y opposer par écrit pour un motif légitime lié à la protection des données ; à défaut d'accord, il peut résilier la solution concernée.

ANIKOP impose à chaque sous-traitant ultérieur des obligations de protection des données équivalentes à celles du présent accord et reste responsable de leur exécution envers le client.

8. Transferts hors de l'Union européenne

Les données sont hébergées dans l'Union européenne. Lorsqu'un sous-traitant ultérieur traite des données hors de l'Union européenne, le transfert est encadré par les garanties prévues par le RGPD, notamment les clauses contrac-

tuelles types adoptées par la Commission européenne. Les transferts concernés sont indiqués dans l'annexe de chaque solution.

9. Droits des personnes concernées

Le client est l'interlocuteur des personnes concernées. ANIKOP l'aide, dans la mesure du possible, à répondre aux demandes d'exercice de leurs droits (accès, rectification, effacement, portabilité, opposition, limitation).

Si une personne concernée adresse directement sa demande à ANIKOP, celle-ci la transmet au client sans délai et n'y répond pas elle-même, sauf instruction du client.

10. Violation de données

ANIKOP notifie au client toute violation de données personnelles dans les meilleurs délais, et au plus tard quarante-huit (48) heures après en avoir pris connaissance. La notification précise, dans la mesure du possible, la nature de la violation, les catégories et le nombre approximatif de personnes et de données concernées, ses conséquences probables et les mesures prises ou envisagées.

Il appartient au client, en tant que responsable de traitement, de notifier la violation à la CNIL et, le cas échéant, aux personnes concernées. ANIKOP l'assiste dans ces démarches.

11. Assistance et contrôle

ANIKOP aide le client, en tenant compte des informations dont elle dispose, à respecter ses obligations en matière de sécurité, d'analyse d'impact et de consultation préalable de la CNIL.

ANIKOP met à la disposition du client les informations nécessaires pour démontrer le respect du présent accord. Le client peut réaliser un audit, à ses frais, moyennant un préavis écrit de trente (30) jours, au plus une fois par an sauf violation de données, dans des conditions préservant la confidentialité des informations d'ANIKOP et de ses autres clients.

12. Fin du contrat

À la fin du contrat, ANIKOP restitue ou efface les données selon les modalités prévues par les conditions générales de la solution concernée et rappelées en annexe, sauf obligation légale de conservation.

Pour toute question relative au présent accord ou à la protection des données : **dpo@anikop.com**

Annexe 1 : Com'play

Logiciel d'affichage dynamique fourni en mode SaaS, avec ou sans player

Nature et finalité du traitement

Hébergement et traitement des données du client pour lui permettre de gérer ses écrans et de diffuser ses contenus : gestion des comptes utilisateurs, stockage des médias, planification et diffusion des contenus, statistiques de diffusion, supervision du parc d'écrans, assistance et maintenance, y compris au moyen d'un assistant d'intelligence artificielle intégré à la solution.

Catégories de personnes concernées

- Les utilisateurs de la solution désignés par le client (ses salariés ou collaborateurs).
- Les personnes dont le client saisit les données dans la solution, notamment ses salariés lorsqu'il utilise le module d'anniversaires.
- Les personnes éventuellement visibles ou citées dans les contenus diffusés par le client, sous sa seule responsabilité.

Catégories de données

- **Comptes utilisateurs** : nom, prénom, adresse e-mail, téléphone, photo de profil, langue, mot de passe (stocké sous forme hachée, jamais en clair), date de dernière connexion.
- **Société cliente** : raison sociale, adresse, e-mail, téléphone, éléments de charte graphique, nombre d'écrans autorisés, date de fin de contrat.
- **Contenus** : fichiers déposés par le client (images, vidéos, documents), leur nom d'origine et l'utilisateur qui les a déposés ; playlists, compositions, modèles, bandeaux et modules tactiles créés par le client.
- **Données saisies par le client sur des tiers** : pour le module d'anniversaires, prénom, nom, service, date de naissance, date d'embauche et photo des personnes concernées, transmis aux écrans pour affichage.
- **Parc matériel** : adresse postale et coordonnées géographiques des sites, identifiants de connexion au Wi-Fi le cas échéant ; pour chaque écran, nom, matériel, versions logicielles, adresse IP, dernière connexion et dernière capture de l'affichage.
- **Journaux et statistiques** : connexions, actions sur les contenus et les comptes, historique de diffusion, consultations des modules tactiles, analyses antivirus, erreurs techniques.
- **Assistance** : tickets, messages, pièces jointes, recherches dans l'aide en ligne, échanges avec l'assistant d'intelligence artificielle.

Durée du traitement et fin du contrat

Les données sont conservées pendant toute la durée du contrat. À la fin du contrat, conformément à l'article 18 des conditions générales Com'play :

- le client peut exporter ses données (formats CSV et JSON, avec ses fichiers d'origine) ;
- les données sont effacées automatiquement trente (30) jours après la notification de la résiliation, sauf demande écrite contraire du client ;
- les données effacées disparaissent des sauvegardes au plus tard soixante (60) jours après l'effacement ;
- une attestation d'effacement est remise au client sur demande ;
- les tickets d'assistance sont également conservés dans l'outil interne de gestion du support d'ANIKOP ; leur effacement est traité séparément, sur demande du client.

Hébergement

Les données, les fichiers et les sauvegardes sont hébergés sur un serveur dédié chez Hetzner Online GmbH, en Allemagne.

Sous-traitants ultérieurs

PRESTATAIRE	RÔLE	LOCALISATION
Hetzner Online GmbH	Hébergement de la plateforme, des données, des fichiers et des sauvegardes	Allemagne (UE)
Brevo	Envoi des e-mails de la plateforme (invitations, réinitialisation de mot de passe, réponses aux tickets, alertes)	France (UE)
New Relic	Supervision technique de l'application (journaux, hors en-têtes sensibles)	Région européenne (UE)
OpenRouter	Fonctionnement de l'assistant d'intelligence artificielle et de la réponse aux tickets : reçoit les textes saisis par les utilisateurs et le contenu des tickets. Les modèles utilisés sont fournis par Anthropic, Google et OpenAI ; la liste des sous-traitants d'OpenRouter est publiée sur trust.openrouter.ai	Hors UE (États-Unis), transfert encadré par les clauses contractuelles types de la Commission européenne

Services tiers

Les services suivants ne sont pas des sous-traitants d'ANIKOP :

- **Services connectés par le client** : Canva (accès en lecture seule aux designs du client), Instagram (affichage des publications du client), connexion par compte Google et affichage des avis Google. Ils ne sont utilisés que si le client ou l'utilisateur choisit de les connecter, et relèvent de sa relation directe avec ces services. Les jetons de connexion sont stockés de manière chiffrée. En cas de déconnexion, il appartient au client de retirer également l'autorisation donnée depuis son compte chez ce tiers.
- **Géolocalisation des sites** : l'adresse postale des sites du client est transmise à la Base Adresse Nationale et, à défaut, à OpenStreetMap, pour les placer sur la carte.

Mesures de sécurité

- **Échanges chiffrés** : toutes les communications passent en HTTPS, avec une politique interdisant au navigateur de revenir à une connexion non chiffrée.
- **Mots de passe** : stockés sous forme hachée, longueur minimale de douze caractères ; double authentification par application mobile disponible.
- **Cloisonnement** : chaque client n'accède qu'à ses propres données, contrôle effectué côté serveur ; cinq niveaux de droits, avec possibilité de limiter un utilisateur à certains sites.
- **Fichiers déposés** : taille limitée, vérification du type réel du fichier et analyse antivirus de chaque dépôt.
- **Protection contre les attaques automatisées** : limitation du nombre de tentatives de connexion, de réinitialisation de mot de passe et d'appairage d'écran.
- **Traçabilité** : enregistrement des connexions, journalisation des actions sur les contenus et les comptes, traçage des exports et des effacements.
- **Données sensibles de connexion** : jetons des services tiers et identifiants Wi-Fi stockés de manière chiffrée.
- **Sauvegardes** : sauvegarde quotidienne de la base, conservée quatorze (14) jours ; sauvegarde avant chaque mise en production et copie continue des fichiers, conservées cinquante-cinq (55) jours ; réalisées sur l'infrastructure d'hébergement.
- **Supervision** : remontée automatique des erreurs de l'application et des écrans à l'équipe technique, alertes en cas de comportement anormal du parc d'écrans.