Contrat de sous-traitance de données personnelles

Annexe aux Conditions générales d'utilisation du service fluctuat, au sens de l'art. 28 RGPD et de l'art. 9 nLPD.

Le Responsable du traitement (le « Client »)

L'organisation titulaire du compte fluctuat, identifiée par les informations de son compte et de son tenant Microsoft 365.

Le Sous-traitant (le « Prestataire »)

Dizzus GmbH, Chamerstrasse 172, 6300 Zoug, Suisse. IDE CHE-469.903.322. Contact : formulaire à l'adresse portal.fluctuat.io/contact.

Le présent contrat (le « DPA ») fait partie intégrante des CGU du service fluctuat. Il est réputé conclu entre le Client et le Prestataire dès la création du compte, sans signature séparée. En cas de contradiction avec les CGU, le DPA prévaut pour ce qui concerne la protection des données.

1. Objet et durée

Le DPA encadre les traitements de données personnelles que le Prestataire effectue pour le compte du Client dans le cadre du service fluctuat : l'acheminement du courrier électronique des applications du Client via l'API Microsoft Graph, avec dépôt d'une copie dans les Éléments envoyés de l'expéditeur. Il s'applique pendant toute la durée du contrat de service et jusqu'à l'effacement des données visé à l'article 11.

2. Nature et finalité du traitement

Réception de messages soumis par les applications du Client (SMTP authentifié ou API), contrôle de l'expéditeur contre la liste blanche du Client lorsque celui-ci en déclare une, mise en file durable, émission via Microsoft Graph au nom de l'expéditeur, journalisation de l'acheminement, et mise à disposition de ce journal dans la console du Client. Aucune autre finalité : pas d'analyse du contenu, pas de publicité, pas de revente.

3. Données traitées et personnes concernées

Catégorie	Détail	Conservation
Contenu des messages	Corps et pièces jointes, chiffrés dès l'acceptation	Transitoire : purgé après remise à Microsoft 365, au plus 7 jours en cas d'échec
Métadonnées d'acheminement	Expéditeur, destinataires, objet, horodatage, statut	Selon le plan du Client : 30 jours à 12 mois
Données de compte		Durée de la relation contractuelle

	E-mail, hachage de mot de passe (argon2id), expéditeurs et identifiants configurés	

Personnes concernées : les collaborateurs et systèmes du Client au nom desquels les messages sont envoyés, et les destinataires de ces messages.

4. Instructions du Client

Le Prestataire ne traite les données que sur instruction documentée du Client. La configuration du service par le Client (expéditeurs autorisés, identifiants, restrictions IP/FQDN, durée de rétention du plan, demandes via la console ou le formulaire de contact) constitue l'instruction documentée. Le Prestataire informe le Client si, selon lui, une instruction viole le droit applicable.

5. Confidentialité

Les personnes autorisées à traiter les données sont soumises à une obligation de confidentialité. L'accès opérateur est limité au strict nécessaire à l'exploitation et au support ; les actions d'administration sont journalisées.

6. Mesures techniques et organisationnelles

Le Prestataire met en œuvre les mesures décrites à l'Annexe 1, qu'il peut faire évoluer sans en réduire le niveau de protection.

7. Sous-traitants ultérieurs

Le Client autorise le recours aux sous-traitants ultérieurs listés à l'Annexe 2. Le Prestataire informe le Client de tout changement prévu (ajout ou remplacement) avec un préavis raisonnable, par la console ou par message au titulaire du compte ; le Client peut s'y opposer pour motif légitime, l'issue pouvant être la résiliation sans pénalité. Le Prestataire impose à ses sous-traitants ultérieurs des obligations équivalentes au présent DPA et demeure responsable de leur exécution.

8. Assistance au Client

Compte tenu de la nature du traitement, le Prestataire assiste le Client pour répondre aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, limitation, portabilité) : les métadonnées sont consultables et exportables depuis la console, le reste sur demande via le formulaire de contact. Le Prestataire assiste également le Client pour ses obligations de sécurité et, le cas échéant, d'analyse d'impact.

9. Violation de données

Le Prestataire notifie au Client toute violation de données personnelles le concernant sans retard injustifié après en avoir pris connaissance, avec les informations raisonnablement disponibles : nature de la violation, catégories et volume approximatif de données et de

personnes concernées, mesures prises ou proposées. La notification est adressée au titulaire du compte.

10. Localisation et transferts

Les données sont hébergées au Royaume-Uni (OVHcloud, Londres), pays reconnu comme offrant un niveau de protection adéquat par la Suisse et par l'Union européenne. L'émission des messages s'effectue au sein du tenant Microsoft 365 du Client, selon la localisation choisie par le Client auprès de Microsoft. Tout autre transfert est encadré par des garanties appropriées.

11. Suppression et restitution

À la clôture du compte, le Prestataire supprime les données du Client : le contenu résiduel immédiatement, les métadonnées et données de compte au plus tard 30 jours après la clôture, sous réserve des conservations exigées par la loi (pièces comptables notamment). Le Client peut exporter ses données de compte depuis la console avant la clôture. La copie des messages dans les Éléments envoyés réside dans le tenant Microsoft du Client et n'est pas affectée.

12. Audit et information

Le Prestataire tient à la disposition du Client les informations nécessaires pour démontrer le respect du présent DPA : la présente documentation, la page Sécurité du site, et des réponses écrites aux questionnaires de sécurité raisonnables (une fois par période de douze mois, via le formulaire de contact). Un audit sur site peut être convenu pour motif légitime, aux frais du Client, avec un préavis de 30 jours et sans accès aux données des autres clients.

13. Responsabilité, droit applicable et for

La responsabilité des parties au titre du DPA suit le régime des CGU. Le DPA est soumis au droit suisse ; le for exclusif est à Zoug, sous réserve d'un for impératif.

Annexe 1 : mesures techniques et organisationnelles

- **Moindre privilège Microsoft** : permission Mail.Send uniquement, aucune lecture des boîtes ; consentement révocable à tout moment par le Client depuis son tenant.
- **Chiffrement en transit** : TLS sur tous les canaux (SMTP STARTTLS ou TLS implicite, HTTPS pour la console et l'API).
- **Chiffrement et purge du contenu** : corps et pièces jointes chiffrés dès l'acceptation, purgés après remise, jamais journalisés en clair.
- **Journal minimisé** : en-têtes et statut d'acheminement seulement, rétention bornée selon le plan puis purge automatique.
- **Isolation par client** : cloisonnement au niveau de la base de données (row-level security forcée), sous-domaine et identifiants propres à chaque client.
- **Contrôle d'envoi** : liste blanche d'expéditeurs facultative par client (si déclarée, aucun envoi hors liste) ; restriction optionnelle des sources par IP/FQDN ; isolation entre clients toujours absolue (jeton Microsoft par tenant).
- **Authentification** : mots de passe et secrets hachés en argon2id, secrets affichés une seule fois, double authentification (TOTP) sur la console.
- **Durabilité** : file d'attente durable, relances automatiques, file morte avec alerte, jamais de suppression silencieuse ; sauvegardes quotidiennes vers un site distant.
- **Traçabilité** : journalisation des actions d'administration et des événements de facturation affectant l'envoi.

Annexe 2 : sous-traitants ultérieurs autorisés

Sous-traitant	Rôle	Localisation
Microsoft Ireland Operations Ltd / Microsoft Corp.	Émission des messages via l'API Graph, au sein du tenant Microsoft 365 du Client	Selon le tenant du Client
OVHcloud	Hébergement de l'infrastructure	Londres, Royaume-Uni
Stripe Payments Europe Ltd	Traitement des paiements (aucune donnée de carte ne transite par fluctuat)	UE / États-Unis (clauses types)