Equalis OpsReg

Accord de traitement des données

Version 1.0 · 2 novembre 2026 · EqualisTech OpsReg Limited, CRO 814298

Synthèse

Le présent accord s'applique à compter de la disponibilité générale de la plateforme, prévue pour février 2027. Avant la disponibilité générale, toute preuve de concept portant sur les abonnements Azure d'un client est encadrée par un accord écrit distinct comprenant les clauses de l'article 28 du RGPD. Pour les clients de la plateforme, EqualisTech OpsReg Limited agit en qualité de sous-traitant, au sens de l'article 28 du RGPD, pour les métadonnées d'abonnements Azure traitées par le service ; les données de compte sont traitées en qualité de responsable du traitement, comme indiqué dans la politique de confidentialité. Personnes concernées : le personnel du client et les autres personnes dont les identifiants figurent dans la configuration Azure (attributions de rôles, étiquettes de ressources et contacts d'alerte, par exemple). Données personnelles : noms, noms d'utilisateur principaux (UPN), adresses e-mail, identifiants d'objet et adresses IP contenus dans ces métadonnées (y compris les alertes de sécurité) et dans les preuves. Finalité : évaluer la configuration Azure au regard des règles de la plateforme et produire des preuves et des rapports. Durée : la durée du contrat. Principaux engagements :

- Localisation : les données de la plateforme sont traitées et hébergées dans Azure North Europe (Irlande), avec des sauvegardes géo-redondantes dans West Europe (Pays-Bas), et la correspondance de support est conservée dans Microsoft 365, avec des données stockées dans l'UE. EqualisTech n'effectue aucun transfert hors de l'EEE, en dehors de l'envoi des constats aux destinations configurées par le client. Microsoft documente des cas limités dans lesquels les services Microsoft que nous utilisons (Microsoft Azure, y compris le réseau périphérique d'Azure Front Door, Microsoft Entra External ID, Azure Communication Services et Microsoft 365) peuvent traiter des données ou y accéder hors de l'UE, par exemple pour l'accès à distance par le personnel de Microsoft, les opérations de sécurité mondiales et le support ; ces transferts sont encadrés par les clauses contractuelles types de l'UE figurant dans l'avenant sur la protection des données de Microsoft (Data Protection Addendum). Les constats ne sont envoyés qu'aux destinations configurées par le client ; le lieu où un outil connecté conserve les constats relève du contrat du client avec son fournisseur.
- Accès en lecture seule aux abonnements Azure du client ; aucune information d'identification Azure du client n'est stockée. Les clés de connecteurs fournies par le client sont chiffrées dans Azure Key Vault.
- Sous-traitant ultérieur : Microsoft Ireland Operations Limited, pour l'hébergement de la plateforme (Microsoft Azure), l'authentification (Microsoft Entra External ID), les e-mails de notification (Azure Communication Services) et la messagerie du support (Microsoft 365), ainsi que les sociétés affiliées et sous-traitants ultérieurs que Microsoft indique pour ces services. Nous informons les

clients au moins 30 jours à l'avance de tout ajout ou remplacement envisagé d'un sous-traitant ultérieur ; le client peut s'y opposer pour des motifs raisonnables et, à défaut de solution convenue, résilier le service concerné. Nous imposons à chaque sous-traitant ultérieur les mêmes obligations de protection des données que celles prévues par le présent accord et restons pleinement responsables envers le client de leur exécution.

- Les preuves sont stockées en écriture unique et ne sont jamais modifiées. Pendant toute la durée du contrat, chaque preuve est conservée sept ans à compter de sa création. À la fin du contrat, le client peut récupérer ses exports pendant 30 jours ; toutes les données personnelles du client sont ensuite supprimées, y compris des sauvegardes dans un délai supplémentaire de 35 jours, sauf si le droit de l'Union ou d'un État membre en exige la conservation.
- À la disponibilité générale, les mesures techniques et organisationnelles comprennent l'isolation des clients au niveau de la base de données, l'authentification par identités managées, un réseau privé pour les services de données et une exposition publique protégée par un pare-feu applicatif web (Azure Front Door Premium).
- Nous ne traitons les données personnelles du client que sur ses instructions documentées, y compris en ce qui concerne les transferts, sauf si le droit de l'Union ou d'un État membre l'exige, auquel cas nous en informons préalablement le client, sauf si ce droit l'interdit ; informons immédiatement le client si, selon nous, une instruction constitue une violation du droit de la protection des données ; veillons à ce que les personnes autorisées à les traiter soient soumises à une obligation de confidentialité ; mettons en œuvre les mesures de sécurité requises par l'article 32 du RGPD ; aidons le client à répondre aux demandes des personnes concernées et à respecter ses obligations au titre des articles 32 à 36 du RGPD ; notifions au client toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance, et au plus tard dans les 48 heures ; et mettons à disposition les informations nécessaires pour démontrer le respect de ces obligations, ainsi que pour permettre la réalisation d'audits et y contribuer.

Signature du DPA

Le DPA complet fait partie des conditions générales de service et s'applique à tout client de la plateforme dès la création du compte. Son texte intégral, avec les clauses de l'article 28, la description des traitements et l'annexe sur les mesures techniques et organisationnelles, vous est remis avant la souscription ; un exemplaire contresigné est disponible sur demande pour les clients et prospects : contact@equalistech.com.