

ESA GPT – Traitement de mandat selon l'art. 9 LPD

L'ESA – organisation d'achat de la branche suisse de l'automobile et des véhicules à moteur société coopérative (ci-après «la mandataire») met à la disposition du mandant (ci-après «le mandant») la prestation ESA GPT, qui comprend également le traitement de données personnelles et constitue un traitement de mandat au sens de l'art. 9 LPD. La présente convention de traitement de mandat s'applique de manière informelle à l'utilisation d'ESA GPT.

Version 1.0 du 28 avril 2025. Cette version peut être remplacée par des versions futures.

Catégories de personnes concernées: clientes et clients, collaboratrices et collaborateurs, partenaires commerciaux du mandant.

Catégories de données: coordonnées, données d'utilisation et données fournies par le mandant.

Transfert de données autorisé (pays): les données sont traitées en Suisse et dans l'EEE (Allemagne, Irlande, Suède).

Sous-traitants autorisés (nom, finalité): Microsoft Ireland Operations, hébergement d'Azure OpenAI (Suisse et Suède) et Statworx GmbH, partenaire d'implémentation (Allemagne).

Obligations de la mandataire

1. La mandataire ne traite les données qu'à des fins établies par le mandant et sur instruction documentée de ce dernier (mise à disposition d'un environnement IA, p. ex.); si elle estime qu'elles ne sont pas licites, elle en informe le mandant.
2. La mandataire veille toujours à ce que les données soient sécurisées de manière adéquate, conformément à la législation en vigueur en matière de protection des données et aux mesures techniques et organisationnelles (MTO). Elle signale sans délai toute violation de la sécurité des données en fournissant toutes les informations nécessaires.
3. La mandataire enjoint à tous les auxiliaires, collaboratrices et collaborateurs de garder le secret, dans la mesure où la loi ne l'exige pas déjà.
4. La mandataire ne fait appel à des sous-traitants qu'avec autorisation de le faire (voir ci-dessus). Tout autre sous-traitant doit être communiqué et est réputé approuvé en l'absence de contestation dans un délai de 30 jours. Ceux-ci sont également tenus de respecter la protection des données.
5. La mandataire n'exporte aucune donnée du mandant sans son autorisation et, le cas échéant, uniquement dans le respect de la législation en vigueur en matière de protection des données.
6. Si nécessaire, la mandataire aide le mandant à respecter la législation sur la protection des données, en particulier ce qui concerne le respect des droits des personnes concernées et les analyses d'impact relatives à la protection des données personnelles.
7. Une fois la collaboration terminée, les données sont détruites à l'expiration des délais de conservation légaux.
8. La mandataire apporte la preuve du respect de la présente convention de traitement de mandat et le mandant peut la vérifier.

Sécurité de l'information (MTO)

Vous trouverez ci-après nos mesures techniques et organisationnelles (MTO) relatives à la sécurité des données.

- Contrôles des accès
- Vidéosurveillance de l'entrepôt de marchandises et de la salle des serveurs
- ASI
- IAM
- Accès aux données uniquement avec authentification
- MFA pour tous les accès
- Mots de passe forts
- Principe du moindre privilège
- Principe du besoin d'en connaître
- Principe «Zero Trust»
- Terminaux cryptés
- TLS enforced
- Tests d'intrusion
- Audits de sécurité ext.
- ISMS
- Sauvegardes
- Plan de continuité d'activité (PCA)
- Pare-feux
- Système de détection d'intrusion
- EDR/XDR
- MDM
- Protection contre les malwares
- Gestion des correctifs
- Séparation des systèmes productifs et des autres systèmes
- Installation de logiciels contrôlée
- SOC
- Directive sur la sécurité de l'information
- Security Awareness Trainings
- Enregistrement des événements relevant de la sécurité

MTO détaillées disponibles sur demande