POLITIQUE 08 • KRB-POL-08

Politique de Confidentialité et de Sécurité de l'Information

NOM DU DOCUMENT	N° DU DOCUMENT	DATE DE PUBLICATION
Politique de Confidentialité et de Sécurité de l'Information	**KRB-POL-08**	**03.03.2025**
N° / DATE DE RÉVISION	**PRÉPARÉ PAR**	**APPROUVÉ PAR**
1 / 11.08.2026	**Service Juridique et Conformité**	**Conseil d'administration**

8.1 Objet

La présente Politique a pour objet de définir les principes, règles et responsabilités relatifs à la protection des informations confidentielles, des secrets d'affaires, des actifs de propriété intellectuelle et des données à caractère personnel détenus par Karub Enerji ou confiés par des tiers, et de garantir la confidentialité, l'intégrité et la disponibilité de l'information.

Pour Karub Enerji, société technologique à forte intensité de R&D, l'information — telle que les recettes de production de cellules et de modules, les paramètres de procédé, les données d'essai, les fichiers de conception et les informations clients — compte parmi ses actifs les plus précieux.

8.2 Champ d'application

La présente Politique couvre toutes les informations appartenant à la Société ou sous son contrôle, quel que soit leur support (papier, électronique, oral ou visuel), ainsi que tous les salariés, dirigeants, stagiaires, consultants, fournisseurs et partenaires commerciaux ayant accès à ces informations. Les obligations subsistent après la fin de la relation d'affaires.

8.3 Fondement juridique

- Loi n° 6698 sur la protection des données à caractère personnel et sa réglementation d'application, ainsi que les décisions du Conseil de protection des données à caractère personnel
- Contrats types, règles d'entreprise contraignantes et mécanismes de consentement explicite relatifs aux transferts à l'étranger en vertu de l'art. 9 de la loi n° 6698
- Loi n° 5651 sur la réglementation des publications sur internet
- Art. 396 (interdiction de concurrence) et dispositions relatives à la concurrence déloyale (art. 54 et suiv.) du Code de commerce turc n° 6102
- Art. 396 (obligation de loyauté du salarié) et art. 444-447 (clause de non-concurrence) du Code des obligations turc n° 6098
- Art. 135-140 (infractions relatives aux données à caractère personnel) et art. 239 (divulgation d'informations constituant des secrets d'affaires) du Code pénal turc n° 5237
- Loi n° 6769 sur la propriété industrielle et loi n° 5846 sur les œuvres intellectuelles et artistiques
- Règlement général sur la protection des données de l'Union européenne (RGPD) — dans la mesure où il s'applique
- Norme ISO/IEC 27001 Système de management de la sécurité de l'information

8.4 Définition et classification des informations confidentielles

Est confidentielle toute information non publique dont la divulgation pourrait porter préjudice à la Société, à ses salariés, à ses clients ou à ses partenaires commerciaux. En font notamment partie : les recettes de production et paramètres de procédé, les dessins et conceptions techniques, les résultats des projets de R&D et des essais, les inventions n'ayant pas encore fait l'objet d'une demande de brevet, les données de coûts et de tarification, les informations relatives aux offres et appels d'offres, les listes de clients et de fournisseurs, les conditions contractuelles, les données financières et plans d'affaires, les informations relatives au personnel et aux salaires, et les informations de sécurité relatives aux systèmes d'information.

Les informations sont classifiées en quatre niveaux : « Public », « Usage interne », « Confidentiel » et « Strictement confidentiel ». Pour chaque classe, des règles d'accès, de conservation, de transmission, de reproduction et de destruction sont définies séparément et les documents sont étiquetés en conséquence.

8.5 Obligations fondamentales de confidentialité

- Les informations confidentielles ne sont utilisées que dans la mesure requise par le travail et dans le cadre du principe du « besoin d'en connaître » (need-to-know).
- Les informations confidentielles ne peuvent être partagées avec des personnes non autorisées — y compris les autres salariés de la Société.
- Le partage d'informations avec des tiers doit reposer sur un accord de confidentialité écrit (NDA) signé au préalable.
- Les informations confidentielles ne peuvent être copiées sur des appareils personnels, des comptes de messagerie personnels, des services cloud non approuvés ou des supports amovibles.
- Les informations confidentielles ne peuvent être partagées sur les réseaux sociaux, lors de conférences, dans des communiqués de presse ou dans des outils d'intelligence artificielle ouverts au grand public.
- À la fin de la relation d'affaires, toutes les informations confidentielles et tous les supports les contenant sont restitués à la Société ; aucune copie ne peut être conservée.
- L'obligation de confidentialité subsiste sans limitation de durée après la fin du contrat de travail.
- L'obtention et l'utilisation d'informations sur les concurrents auprès de tiers par des moyens illicites sont interdites.

8.6 Protection des données à caractère personnel

En sa qualité de responsable du traitement, la Société respecte les principes généraux énoncés à l'art. 4 de la KVKK pour les données à caractère personnel qu'elle traite : licéité et loyauté ; exactitude et, si nécessaire, mise à jour ; traitement pour des finalités déterminées, explicites et légitimes ; caractère adéquat, pertinent et limité à la finalité ; conservation pendant la durée prévue par la législation ou nécessaire à la finalité du traitement.

- Les données à caractère personnel ne sont traitées qu'en présence de l'une des conditions de traitement énumérées aux art. 5 et 6 de la KVKK.
- Les personnes concernées sont informées conformément à l'art. 10 de la KVKK avant toute activité de traitement ; le consentement explicite est recueilli lorsque nécessaire et il est indiqué que ce consentement peut être retiré.
- Un inventaire des traitements de données à caractère personnel est établi et tenu à jour ; l'obligation d'enregistrement au VERBİS est remplie dans la mesure où la Société y est assujettie.
- Les durées de conservation sont fixées conformément à la Politique de conservation et de destruction des données à caractère personnel ; à l'expiration du délai, les données sont effacées, détruites ou anonymisées.

- Des contrats de traitement des données conformes à la KVKK sont conclus avec les prestataires intervenant en qualité de sous-traitant.
- Les transferts à l'étranger sont effectués dans le cadre de l'art. 9 de la KVKK sur la base d'une décision d'adéquation, de garanties appropriées (contrats types, règles d'entreprise contraignantes) ou de dispositions dérogatoires, et les obligations de notification à l'Autorité sont respectées.
- Les demandes des personnes concernées sont traitées dans un délai maximal de trente jours, conformément au Communiqué relatif aux modalités de saisine du responsable du traitement.
- Les activités de surveillance des salariés (caméras, journaux de connexion, géolocalisation des véhicules, contrôle des courriels) ne sont menées qu'à des fins légitimes, de manière proportionnée et après information préalable des salariés.
- L'utilisation de cookies sur le site internet de l'entreprise est gérée de manière transparente au moyen d'une Politique de cookies distincte et d'un outil de gestion des cookies ; le consentement explicite est recueilli pour les cookies non essentiels.

8.7 Protection des droits de propriété intellectuelle et industrielle

Les droits sur les inventions, dessins, logiciels et œuvres réalisés par les salariés dans le cadre de leur prestation de travail appartiennent à la Société dans le cadre de la législation et des dispositions contractuelles. Les procédures de déclaration et de rémunération relatives aux inventions de salariés sont menées conformément aux dispositions de la loi sur la propriété industrielle. Les solutions techniques pour lesquelles une demande de brevet est envisagée ne sont en aucun cas divulguées avant la date de dépôt ; des restrictions d'accès sont appliquées aux informations dont la protection en tant que secret d'affaires est privilégiée. Les droits de propriété intellectuelle des tiers sont respectés ; l'utilisation de logiciels sans licence est interdite.

8.8 Mesures de sécurité de l'information

- **Mesures techniques :** pare-feu et segmentation du réseau, protection des terminaux et détection des logiciels malveillants, chiffrement des disques et des transmissions, authentification multifacteur, gestion des habilitations et des accès par rôles, journalisation et surveillance, gestion des correctifs et des vulnérabilités, sauvegardes régulières et tests de restauration.
- **Mesures organisationnelles :** formations de sensibilisation à la sécurité de l'information, simulations d'hameçonnage (phishing), pratique du bureau propre et de l'écran vide, engagements de confidentialité, processus d'habilitation à l'entrée et à la sortie, évaluation de la sécurité des fournisseurs.
- **Mesures physiques :** contrôle d'accès par badge aux zones de production, salles serveurs et laboratoires de R&D, enregistrement et accompagnement des visiteurs, vidéosurveillance des zones critiques, utilisation d'armoires verrouillées et de destructeurs de documents pour les documents papier.
- La prise de photographies et de vidéos non autorisée dans les zones de production et de laboratoire est interdite.
- Des plans de continuité d'activité et de reprise après sinistre sont établis et testés régulièrement.

8.9 Gestion des incidents

Tout incident de sécurité de l'information ou violation de données, avéré ou suspecté, est signalé sans délai au Service des Technologies de l'Information et au Service Juridique/Conformité. Les incidents sont gérés selon une procédure de réponse comprenant les phases de détection, de confinement, d'analyse des causes profondes, de remédiation et de reporting. En cas de violation de données à caractère personnel, le Conseil de protection des données à caractère personnel est notifié dans les meilleurs délais et en tout état de cause dans les soixante-douze

heures ; les personnes concernées sont informées dans les plus brefs délais raisonnables. Les registres d'incidents sont tenus et des mesures sont prises pour prévenir la récurrence d'incidents similaires.

8.10 Sanctions, suivi et entrée en vigueur

La violation de la présente Politique peut entraîner des sanctions disciplinaires pouvant aller jusqu'à la rupture du contrat de travail pour motif légitime, une responsabilité indemnitaire et, pour les faits constitutifs d'une infraction, une responsabilité pénale. En cas de violation par des tiers, des sanctions contractuelles sont appliquées et la relation peut être rompue.

L'efficacité de la Politique est suivie au moyen du nombre d'incidents et du délai de réponse, du taux d'achèvement des formations de sensibilisation, du taux de réussite des simulations d'hameçonnage, du nombre de demandes des personnes concernées et du délai de réponse, ainsi que des constats d'audit. La Politique est révisée au moins une fois par an ou immédiatement en cas de modification de la législation, et entre en vigueur après approbation du Conseil d'administration.

PRÉPARÉ PAR	APPROUVÉ PAR
Service Juridique et Conformité	**Conseil d'administration**
Nom – Prénom / Signature / Date	Nom – Prénom / Signature / Date