



السياسة 08 • KRB-POL-08

سياسة السرية وأمن المعلومات



اسم الوثيقة	رقم الوثيقة	تاريخ الإصدار
سياسة السرية وأمن المعلومات	KRB-POL-08	03.03.2025
رقم / تاريخ المراجعة	إعداد	اعتماد
1 / 11.08.2026	إدارة الشؤون القانونية والامتثال	مجلس الإدارة

8.1 الغرض

الغرض من هذه السياسة هو تحديد المبادئ والقواعد والمسؤوليات المتعلقة بحماية المعلومات السرية والأسرار التجارية وأصول الملكية الفكرية والبيانات الشخصية التي تملكها Karub Enerji أو المؤتمنة عليها من أطراف ثالثة، وضمان سرية المعلومات وسلامتها وإتاحتها.

تُعَدُّ المعلومات — مثل وصفات إنتاج الخلايا والوحدات ومعاملات العمليات وبيانات الاختبار وملفات التصميم ومعلومات العملاء — من أئمن أصول Karub Enerji بصفتها شركة تكنولوجية كثيفة البحث والتطوير.

8.2 النطاق

تشمل هذه السياسة جميع المعلومات المملوكة للشركة أو الخاضعة لسيطرتها بغض النظر عن الوسط الذي توجد فيه (مطبوع أو إلكتروني أو شفهي أو مرئي)، وجميع الموظفين والمديرين والمتدربين والمستشارين والموردين وشركاء الأعمال الذين لهم حق الوصول إلى هذه المعلومات. وتستمر الالتزامات بعد انتهاء علاقة العمل.

8.3 الأساس القانوني

- قانون حماية البيانات الشخصية رقم 6698 ولوائحه التنفيذية وقرارات مجلس حماية البيانات الشخصية
- العقود النموذجية وقواعد الشركات الملزمة وآليات الموافقة الصريحة المتعلقة بالنقل إلى الخارج بموجب المادة 9 من القانون رقم 6698
- قانون تنظيم المنشورات على الإنترنت رقم 5651
- المادة 396 (حظر المنافسة) وأحكام المنافسة غير المشروعة (المادة 54 وما يليها) من قانون التجارة التركي رقم 6102
- المادة 396 (واجب الإخلاص على العامل) والمواد 447-444 (حظر المنافسة) من قانون الالتزامات التركي رقم 6098
- المواد 140-135 (الجرائم المتعلقة بالبيانات الشخصية) والمادة 239 (إفشاء المعلومات ذات طبيعة السر التجاري) من قانون العقوبات التركي رقم 5237
- قانون الملكية الصناعية رقم 6769 وقانون المصنفات الفكرية والفنية رقم 5846
- اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) — بالقدر الذي تنطبق فيه
- معيار نظام إدارة أمن المعلومات ISO/IEC 27001

8.4 تعريف المعلومات السرية وتصنيفها

المعلومات السرية هي كل معلومة غير متاحة للعموم قد يؤدي إفشاؤها إلى الإضرار بالشركة أو موظفيها أو عملائها أو شركاء أعمالها. ويشمل ذلك على وجه الخصوص: وصفات الإنتاج ومعاملات العمليات، والرسومات والتصاميم الفنية، ومخرجات مشاريع البحث والتطوير ونتائج الاختبارات، والاختراعات التي لم تُقدّم بشأنها طلبات براءات، وبيانات التكلفة والتسعير، ومعلومات العروض والمناقصات، وقوائم العملاء والموردين، وشروط العقود، والبيانات المالية وخطط الأعمال، وملفات الموظفين ومعلومات الأجور، والمعلومات الأمنية المتعلقة بنظم المعلومات.

تُصنّف المعلومات على أربعة مستويات: «عام» و«للاستخدام الداخلي» و«سري» و«سري للغاية». وتُحدّد لكل فئة على حدة قواعد الوصول والحفظ والنقل والنسخ والإتلاف، وتُوسم الوثائق بشكل مناسب.

8.5 التزامات السرية الأساسية

- تُستخدم المعلومات السرية فقط بالقدر الذي يتطلبه العمل وفي إطار مبدأ «الحاجة إلى المعرفة» (need-to-know).
- لا يجوز مشاركة المعلومات السرية مع أشخاص غير مخولين — بمن فيهم الموظفون الآخرون داخل الشركة.
- يجب أن تستند مشاركة المعلومات مع الأطراف الثالثة إلى اتفاقية سرية مكتوبة (NDA) موقعة مسبقاً.
- لا يجوز نسخ المعلومات السرية إلى الأجهزة الشخصية أو حسابات البريد الإلكتروني الشخصية أو الخدمات السحابية غير المعتمدة أو وسائط التخزين المحمولة.
- لا يجوز مشاركة المعلومات السرية على وسائل التواصل الاجتماعي أو في المؤتمرات أو البيانات الصحفية أو في أدوات الذكاء الاصطناعي المتاحة للاستخدام العام.
- عند انتهاء علاقة العمل تُعاد جميع المعلومات السرية وجميع الوسائط التي تحتويها إلى الشركة؛ ولا يجوز الاحتفاظ بنسخ.
- يستمر التزام السرية إلى أجل غير مسمى بعد انتهاء عقد العمل.
- يُحظر الحصول على معلومات عن المنافسين من أطراف ثالثة بطرق غير مشروعة واستخدامها.

8.6 حماية البيانات الشخصية

تلتزم الشركة بصفتها مسؤولاً عن البيانات بالمبادئ العامة المنصوص عليها في المادة 4 من KVKK فيما يتعلق بالبيانات الشخصية التي تعالجها؛ الامتثال للقانون وقواعد حسن النية؛ والدقة والتحديث عند الاقتضاء؛ والمعالجة لأغراض محددة وواضحة ومشروعة؛ والارتباط بالغرض والمحدودية والتناسب؛ والحفظ للمدة المنصوص عليها في التشريعات أو اللازمة لغرض المعالجة.

- تُعالج البيانات الشخصية فقط عند توافر أحد شروط المعالجة المذكورة في المادتين 5 و6 من KVKK.
- يُبلغ أصحاب البيانات وفقاً للمادة 10 من KVKK قبل نشاط المعالجة؛ وتُؤخذ الموافقة الصريحة عند الاقتضاء ويُبلغون بإمكانية سحبها.
- يُعدّ جرد معالجة البيانات الشخصية ويُحدّث؛ ويُنفّذ التزام التسجيل في VERBİS بالقدر الذي تدخل فيه الشركة ضمن نطاقه.
- تُحدّد مدد الحفظ وفقاً لسياسة حفظ البيانات الشخصية وإتلافها؛ وعند انتهاء المدة تُحذف البيانات أو تُتلف أو تُجهّل.
- تُبرم مع الجهات التي تُتلقى منها الخدمات بصفة معالج للبيانات عقود معالجة بيانات متوافقة مع KVKK.
- يُنفّذ النقل إلى الخارج في إطار المادة 9 من KVKK استناداً إلى قرار الكفاية أو الضمانات المناسبة (العقود النموذجية، قواعد الشركات الملزمة) أو أحكام الاستثناء، مع مراعاة التزامات الإبلاغ إلى الهيئة.
- يُبثّ في طلبات أصحاب البيانات خلال ثلاثين يوماً على الأكثر وفقاً للبلاغ الرسمي بشأن أصول وقواعد التقدم بطلب إلى المسؤول عن البيانات.

- ◆ تُنفَّذ أنشطة مراقبة الموظفين (الكاميرات، سجلات الدخول، تتبع المركبات، مراقبة البريد الإلكتروني) لأغراض مشروعة فقط وبشكل متناسب ومع إبلاغ الموظفين مسبقاً.
- ◆ يُدار استخدام ملفات تعريف الارتباط على الموقع الإلكتروني للشركة بشفافية من خلال سياسة منفصلة لملفات تعريف الارتباط وأداة لإدارتها؛ وتُؤخذ الموافقة الصريحة لملفات تعريف الارتباط غير الضرورية.

8.7 حماية حقوق الملكية الفكرية والصناعية

تعود إلى الشركة، في إطار التشريعات وأحكام العقود، حقوق الاختراعات والتصاميم والبرمجيات والمصنفات التي ينتجها الموظفون في نطاق أداء عملهم. وتُدار عمليات الإبلاغ والمكافأة المتعلقة باختراعات الموظفين وفقاً لأحكام قانون الملكية الصناعية. ولا يُفصح مطلقاً عن الحلول الفنية المزمع تقديم طلبات براءات بشأنها قبل تاريخ التقديم؛ وتُطبَّق قيود الوصول على المعلومات التي يُفضَّل حمايتها كسر تجاري. وتُحترم حقوق الملكية الفكرية للغير؛ ويُحظر استخدام البرمجيات غير المرخصة.

8.8 تدابير أمن المعلومات

- ◆ **التدابير التقنية:** جدار الحماية وتجزئة الشبكة، وحماية نقاط النهاية واكتشاف البرمجيات الخبيثة، وتشفير الأقراص والنقل، والمصادقة متعددة العوامل، وإدارة الصلاحيات والوصول القائم على الأدوار، وتسجيل السجلات والمراقبة، وإدارة التحديثات والثغرات، والنسخ الاحتياطي المنتظم واختبارات استعادة النسخ الاحتياطية.
- ◆ **التدابير الإدارية:** تدريبات التوعية بأمن المعلومات، ومحاكاة التصيد الاحتيالي (phishing)، وممارسة المكتب النظيف والشاشة النظيفة، وتعهدات السرية، وعمليات منح الصلاحيات وسحبها عند الالتحاق بالعمل ومغادرته، وتقييم أمن الموردين.
- ◆ **التدابير المادية:** التحكم في الدخول بالبطاقات إلى مناطق الإنتاج وغرف الخوادم ومختبرات البحث والتطوير، ونظام تسجيل الزوار ومرافقتهم، والمراقبة بالكاميرات في المناطق الحرجة، واستخدام الخزائن المقفلة وأجهزة إتلاف الأوراق للوثائق الورقية.
- ◆ يُحظر التصوير الفوتوغرافي والمرئي غير المصرح به في مناطق الإنتاج والمختبرات.
- ◆ تُعدّ خطط استمرارية الأعمال والتعافي من الكوارث وتُختبر بانتظام.

8.9 إدارة الحوادث

يُبلَّغ دون تأخير عن أي حادث أمن معلومات أو خرق بيانات فعلي أو مشتبه به إلى إدارة تكنولوجيا المعلومات وإدارة الشؤون القانونية/الامتثال. وتُدار حوادث الخرق وفق إجراء استجابة يشمل مراحل الاكتشاف والاحتواء وتحليل السبب الجذري والمعالجة والإبلاغ. وفي حالة خرق البيانات الشخصية يُبلَّغ مجلس حماية البيانات الشخصية في أقرب وقت ممكن وفي جميع الأحوال خلال اثنتين وسبعين ساعة؛ ويُبلَّغ أصحاب البيانات المعنيون في أقصر وقت معقول. وتُحفظ سجلات الحوادث وتُتخذ التدابير لمنع تكرار الحوادث المماثلة.

8.10 العقوبات والمتابعة والنفاد

قد يترتب على انتهاك هذه السياسة عقوبات تأديبية تصل إلى فسخ عقد العمل لسبب مشروع، ومسؤولية عن التعويض، ومسؤولية جنائية فيما يتعلق بالأفعال التي تشكل جريمة. وفي حالة انتهاكات الأطراف الثالثة تُطبَّق العقوبات التعاقدية ويجوز إنهاء العلاقة.

تُتابع فعالية السياسة من خلال عدد حوادث الخرق ومدة الاستجابة، ومعدل إتمام تدريبات التوعية، ومعدل النجاح في محاكاة التصيد الاحتيالي، وعدد طلبات أصحاب البيانات ومدة الرد عليها، ونتائج التدقيق. تُراجع السياسة مرة واحدة على الأقل سنوياً أو فوراً عند تغيير التشريعات وتدخل حيز النفاذ باعتماد مجلس الإدارة.

اعتماد

مجلس الإدارة

الاسم واللقب / التوقيع / التاريخ

إعداد

إدارة الشؤون القانونية والامتثال

الاسم واللقب / التوقيع / التاريخ