

سياسة الخصوصية

تصف سياسة الخصوصية هذه («السياسة») كيفية قيام F-Tech («الشركة»، «نحن»، «لنا»، «الخاص بنا») بجمع البيانات الشخصية لمستخدمي الموقع <https://kashbi.io>، والتطبيق KashBi، وبوت Telegram، وTelegram Mini App، والنسخة الويب، وواجهة API، وغيرها من الخدمات المرتبطة بالشركة (ويشار إليها فيما يلي باسم «المنصة»)، واستخدامها وتخزينها ونقلها وحمايتها.

تنطبق هذه السياسة على المستخدمين، وزوار الموقع، والحسابات المسجلة، والمشاركين في معاملات P2P، وأصحاب المحافظ، ومقدمي الطلبات إلى خدمة الدعم، وغيرهم من الأشخاص الذين قد تتم معالجة بياناتهم عند استخدام المنصة.

تُعد هذه السياسة جزءاً من شروط المستخدم، وقواعد استخدام المنصة، وسياسات AML/KYC/CTF، وغيرها من وثائق الشركة، إذا كانت تلك الوثائق قابلة للتطبيق. إذا كنت لا توافق على هذه السياسة، يُرجى التوقف عن استخدام المنصة.

1. المصطلحات والتعريفات

1.1. البيانات الشخصية – أي معلومات تتعلق بشخص طبيعي مُعرّف أو قابل للتعريف، بشكل مباشر أو غير مباشر.

1.2. معالجة البيانات الشخصية – أي إجراء أو مجموعة من الإجراءات التي تتم على البيانات الشخصية، بما في ذلك الجمع، والتسجيل، والتنظيم، والتجميع، والتخزين، والتوضيح، والتحديث، والتعديل، والاستخراج، والاستخدام، والنقل، وتوفير الوصول، وإخفاء الهوية، والحجب، والحذف، والإتلاف.

1.3. المستخدم – شخص طبيعي يزور الموقع، أو يسجل في المنصة، أو يستخدم المحفظة، أو يشارك في معاملات P2P، أو يتواصل مع الدعم، أو يتفاعل مع المنصة بأي طريقة أخرى.

1.4. الحساب – حساب المستخدم على المنصة، يتم إنشاؤه عبر Telegram Mini App، أو بوت Telegram، أو النسخة الويب، أو تطبيق الهاتف المحمول، أو أي طريقة أخرى متاحة.

1.5. الأصول الرقمية – العملات المشفرة، والرموز، والعملات المستقرة، وغيرها من وحدات القياس الرقمية التي تدعمها المنصة.

1.6. معاملة P2P – معاملة بين مستخدمين المنصة، يحدد فيها المستخدمون بشكل مستقل شروط التبادل، أو الدفع، أو نقل الأصول الرقمية، أو الأموال الورقية، أو السلع، أو الخدمات، أو غيرها من القيم، إذا كانت هذه الوظيفة متاحة عبر المنصة.

1.7. AML/KYC/CTF – إجراءات مكافحة غسل الأموال، وتمويل الإرهاب، والتحايل على العقوبات، والاحتيال، وغيرها من الأنشطة المحظورة، وكذلك إجراءات تحديد هوية المستخدم والتحقق منه وتقييم المخاطر.

1.8. العلاج – طرف ثالث يعالج البيانات الشخصية بناءً على تعليمات الشركة، أو لمصلحة الشركة، أو لضمان تشغيل المنصة.

2. عن الشركة وبيانات الاتصال

تُعد شركة F-Tech هي المتحكم أو الجهة المسؤولة الأخرى عن البيانات الشخصية التي تتم معالجتها فيما يتعلق باستخدام المنصة، ما لم ينص القانون المعمول به أو خدمة معينة على خلاف ذلك.

بيانات الاتصال:

- الموقع: <https://kashbi.io>

- التطبيق: KashBi

- بريد الدعم الإلكتروني: legal@kashbi.io

- دعم Telegram: kashbi_support

- دولة التسجيل: Kazakhstan

- العنوان القانوني: Al-Farabi Avenue, Apartment 207 44/1

3. المبادئ العامة لمعالجة البيانات الشخصية

نسعى إلى معالجة البيانات الشخصية بصورة قانونية ونزيهة وشفافة. ونسترشد بمبادئ المشروعية، وتحديد الأغراض، وتقليل البيانات، والدقة، وتقييد مدة التخزين، والأمن والسرية.

لا نسعى إلى جمع بيانات أكثر مما هو ضروري لتشغيل المنصة، والامتثال للقانون، والأمن، ومنع الاحتيال، وتسوية النزاعات، وإجراءات AML/KYC/CTF، وحماية حقوق الشركة والمستخدمين.

4. الأسس القانونية للمعالجة

بحسب الغرض المحدد والقانون المعمول به، قد نعالج البيانات الشخصية استناداً إلى الأسس التالية:

- موافقة المستخدم؛

- تنفيذ عقد أو اتخاذ إجراءات قبل إبرام عقد؛

- الامتثال للالتزامات القانونية؛

- المصلحة المشروعة للشركة؛

- حماية المصالح الحيوية للمستخدم أو لأشخاص آخرين، إذا كان ذلك منطبقاً.

إذا كانت المعالجة تتم بناءً على الموافقة، يحق للمستخدم سحب موافقته. ولا يؤثر سحب الموافقة على مشروعية المعالجة التي تمت قبل هذا السحب، ولا يمنع معالجة البيانات استناداً إلى أسس قانونية أخرى.

5. البيانات التي قد نعالجها

5.1. بيانات الحساب والتسجيل:

- Telegram ID

- Telegram username

- الاسم أو اللقب أو الاسم المعروض من Telegram، إذا تم نقلها من Telegram؛

- الصورة الرمزية أو صورة الملف الشخصي، إذا كانت متاحة عبر Telegram أو قام المستخدم بتحميلها؛

- بيانات Telegram WebApp initData اللازمة للتفويض والتحقق من صحة تسجيل الدخول؛

- معلومات ربط حساب Telegram بحساب المنشأ في النسخة الويب؛

- عنوان البريد الإلكتروني؛

- رقم الهاتف؛

- اسم تسجيل الدخول؛

- كلمة المرور في شكل تجزئة تشفيرية للنسخة الويب؛

- رمز PIN في شكل تجزئة تشفيرية أو قيمة تقنية محمية أخرى لـ Telegram Mini App؛

- معلومات تفعيل واستخدام 2FA للنسخة الويب؛

- إعدادات القياسات الحيوية فقط في شكل مؤشر تقني لتفعيل الوظيفة، دون الحصول على قوالب القياسات الحيوية أو تخزينها؛

- عوامل أمان أخرى في شكل معرفات تقنية أو تجزئات أو مؤشرات لتفعيل الوظيفة؛

- تاريخ التسجيل، ودالة الحساب، ولغة الواجهة، وإعدادات الإشعارات؛
- رمز الإحالة، أو ID المستخدم الداعي، أو معلومات برنامج الشركاء، إن وجدت.

5.2. البيانات التقنية:

- عنوان IP؛
- الموقع التقريبي المحدد بناءً على عنوان IP؛
- بيانات الجهاز، والمتصفح، ونظام التشغيل، وإصدار التطبيق، واللغة؛
- معرفات الجلسة؛
- معلومات تسجيل الدخول إلى الحساب؛
- سجلات الأمان؛
- بيانات الأخطاء، والأعطال، وأحداث التطبيق، والتشخيص؛
- تاريخ ووقت ومدة استخدام المنصة؛
- معلومات عن إجراءات المستخدم في الواجهة، بلا قدر اللازم للأمن والتحليلات وتحسين الخدمة.

5.3. بيانات المحفظة والعمليات المتعلقة بالأصول الرقمية:

- المعارف الداخلية للمحافظ والأرصدة؛
- عناوين البلوكشين العامة؛
- memo أو tag أو comment أو غيرها من معرفات الدفع؛
- txid، وhash المعاملة، ورقم الكتلة، وعدد التأكيدات، والشبكة، والأصل، والمبلغ، والرسوم؛
- عناوين المرسل والمستلم على البلوكشين؛
- سجل الإيداعات، والسحوبات، والتحويلات، والتحويلات الداخلية، والاحتجاز، والحظر، والحجز، والتجميد، والاسترداد، والرسوم، والتعديلات؛
- معلومات حالة المعاملة؛
- بيانات مصدر ورود الأصول الرقمية، إذا كانت ضرورية لتحليل AML أو التحقق من مصدر الأموال؛
- نتائج الفحص الآلي أو اليدوي لمخاطر معاملات البلوكشين، إذا كان هذا الفحص مطبقاً.

قد تكون بيانات البلوكشين العامة متاحة في شبكات البلوكشين المعنية بصورة مستقلة عن الشركة. ولا تتحكم الشركة في سجلات البلوكشين العامة ولا يمكنها حذف أو تعديل البيانات التي تم تسجيلها بالفعل في شبكة بلوكشين عامة.

5.4. بيانات معاملات P2P:

- ID الإعلان أو العرض أو المعاملة؛
- دور المستخدم في المعاملة؛
- نوع المعاملة؛
- الأصل الرقمي المختار، والشبكة، وعملة التسوية؛
- المبلغ، والسعر، وسعر الصرف، والهامش، والحدود، والرسوم؛
- حالة المعاملة؛
- تاريخ ووقت الإنشاء، أو القبول، أو الدفع، أو التأكيد، أو الإكمال، أو الإلغاء، أو فتح النزاع؛
- شروط المعاملة، والتعليقات، والتعليمات؛
- طريقة الدفع؛
- بيانات الدفع التي يحددها المستخدم لتنفيذ المعاملة؛
- تأكيدات الدفع، والإيصالات، ولقطات الشاشة، والشيكات، والرسائل، والمرفقات، وغيرها من الأدلة؛
- المراسلات بين المشاركين في المعاملة، إذا كانت هذه الوظيفة متاحة؛
- إجراءات المشرفين أو المحكمين في النزاع؛
- نتيجة النزاع وأسس القرار المتخذ.

لا يجوز للمستخدم نقل بيانات شخصية زائدة، أو بيانات أطراف ثالثة، أو رموز سرية، أو كلمات مرور، أو عبارات seed، أو مفاتيح خاصة، أو أي معلومات سرية أخرى غير لازمة لتنفيذ المعاملة، عبر الدردشة أو وصف المعاملة أو المرفقات أو غيرها من الحقول.

5.5. بيانات المدفوعات بالعملة الورقية

في إطار معاملات P2P، تتم المدفوعات بالعملة الورقية مباشرة بين المستخدمين، ما لم تنص خدمة منفصلة من خدمات المنصة صراحةً على خلاف ذلك. لا تُعد الشركة بنكاً أو مؤسسة دفع أو طرفاً في تحويل العملة الورقية بين المستخدمين؛ ومع ذلك، ولضمان معاملات P2P، وتسوية النزاعات، ومنع الاحتيال، والامتثال للمتطلبات المعمول بها، قد نعالج:

- طريقة الدفع المختارة؛
- اسم صاحب الحساب أو أداة الدفع، إذا قدمه المستخدم؛
- بيانات البطاقة أو الحساب المقتنعة؛
- البنك أو نظام الدفع أو المزود؛
- دولة أداة الدفع؛
- مبلغ الدفع وعملته وتاريخه وحلته؛
- معرف الدفع لدى المزود، إذا قدمه المستخدم؛
- معلومات عن الاسترداد، أو الإلغاء، أو chargeback، أو النزاع، أو العملية المشبوهة.

لا ينبغي لنا طلب أو تخزين بيانات البطاقات المصرفية الكاملة، أو رموز CVV/CVC، أو كلمات مرور التطبيقات المصرفية، أو رموز تأكيد المدفوعات، أو غيرها من بيانات الدفع السرية.

5.6. بيانات AML/KYC/CTF وتقييم المخاطر

نتبع نهجاً قائماً على المخاطر في AML/KYC/CTF. ولا يتم تطبيق تحديد الهوية أو التحقق أو الفحوصات الإضافية أو طلب الوثائق على جميع المستخدمين افتراضياً، بل في الحالات التي يكون فيها ذلك ضرورياً مع مراعاة القانون المعمول به، وقواعد إدارة المخاطر الداخلية، والحدود، ونوع العملية، ومؤشرات النشاط المشبوه، ومتطلبات الشركاء، والنزاع، والتواصل مع الدعم، أو غيرها من عوامل المخاطر.

إذا خضع المستخدم لإجراءات AML/KYC/CTF، فقد نعالج:

- الاسم، واللقب، واسم الأب أو الاسم الكامل الآخر؛
- تاريخ الميلاد؛
- الجنسية؛
- بلد الإقامة؛
- عنوان الإقامة؛
- رقم الهاتف؛
- email؛
- وثيقة الهوية؛
- صورة، أو صورة ذاتية، أو تحقق بالفيديو، أو فحص liveness؛
- معلومات عن الملاك المستفيد، أو مصدر الأموال، أو مصدر الثروة، أو نوع النشاط، أو الغرض من العمليات، إذا كان ذلك منطبقاً؛
- نتائج فحوصات العقوبات، و PEP، و adverse media، وغيرها من الفحوصات؛
- نتائج فحص AML لعناوين ومعاملات البلوكشين؛
- ملف المخاطر الداخلي للمستخدم؛
- الوثائق والتوضيحات التي يقدمها المستخدم بناءً على طلب الشركة؛
- معلومات عن نشاط مشبوه أو غير عادي أو محظور أو علاي المخاطر.

إن مجرد التسجيل في المنصة لا يعني أن المستخدم ملزم في جميع الحالات بإتمام تحقق KYC كامل، ما لم تنص الواجهة أو شروط خدمة معينة أو المتطلبات المعمول بها على خلاف ذلك.

5.7. بيانات خدمة الدعم:

- بيانات الاتصال؛
- محتوى الطلب؛
- المرفقات، ولقطات الشاشة، والوثائق، والرسائل؛
- سجل المراسلات؛
- تسجيلات الطلبات، إذا كانت قناة الاتصال المعنية تنص على التسجيل؛
- معلومات عن حل الطلب؛

- البيانات اللازمة لتأكيد ملكية الحساب.

5.8. بيانات التسويق والاتصالات:

- الموافقات والاعتراضات على الرسائل؛

- email، أو Telegram username، أو Telegram ID، أو أي قناة اتصال أخرى؛

- سجل الإشعارات؛

- تفضيلات اللغة ونوع الرسائل؛

- إحصاءات التسليم والتفاعل مع الرسائل، إذا كان ذلك منطبقاً.

قد نرسل رسائل خدمية ومعلوماتية وتسويقية مرتبطة بلامنصة، والأمن، والتحديثات، والوظائف الجديدة، وتغييرات الشروط، والعروض الترويجية، أو غيرها من عروض الشركة. لا نسعى إلى إرسال رسائل مفرطة أو مضللة أو مزعجة للمستخدم. يجوز للمستخدم رفض الرسائل التسويقية، إذا كان هذا الرفض منصوصاً عليه في القانون المعمول به أو في واجهة المنصة. وقد تُرسل الإشعارات الخدمية وذات الأهمية القانونية بغض النظر عن رفض الرسائل التسويقية.

6. أغراض معالجة البيانات الشخصية

قد نعالج البيانات الشخصية من أجل:

- تسجيل الحساب وإدارته؛

- التفويض، والمصادقة، واستعادة الوصول؛

- توفير المحفظة والعمليات المتعلقة بالأصول الرقمية؛

- معالجة الإيداعات، والسحوبات، والتحويلات الداخلية، والأرصدة، والرسوم، والتأكيدات؛

- توفير وظائف P2P، وإنشاء العروض، وفتح المعاملات وإكمالها؛

- حجز الأصول الرقمية أو احتجازها أو تحريرها؛

- تبادل الرسائل والأدلة بين المشاركين في المعاملة؛

- تسوية النزاعات والتحكيم؛

- تسجيل طريقة الدفع والتحقق من تأكيدات الدفع في نزاعات P2P؛

- AML/KYC/CTF، ومراقبة العقوبات، وإدارة المخاطر؛

- مراقبة المعاملات وفحص عناوين البلوكشين؛

- الأمن، ومنع الاحتيال، وتعدد الحسابات، والرسائل المزعجة، والتصيد، والهجمات، وغيرها من المخالفات؛

- دعم المستخدمين؛

- تحسين المنصة، وإصلاح الأخطاء، واختبار الوظائف، والتحليلات؛

- الأغراض القانونية، وتسوية المطالبات، وحماية حقوق الشركة.

7. ملفات Cookies والتقنيات المماثلة

قد نستخدم local storage، وsession storage، ومعرفات الجلسة التقنية، وسجلات الخادم، والتحليلات الداخلية غير القائمة على cookies، وغيرها من التقنيات المماثلة لأغراض التفويض، وحفظ الإعدادات، وحماية الجلسة، ومنع الاحتيال، والتحليلات، وتشخيص الأخطاء، وتحسين عمل المنصة، والامتثال لمتطلبات الأمن.

إذا بدأت الشركة مستقبلاً في استخدام cookies أو تحليلات cookies الخاصة بأطراف ثالثة، فستنعكس هذه المعالجة في هذه السياسة، أو في سياسة Cookies منفصلة، أو في واجهة الموافقة، إذا تطلب القانون المعمول به ذلك.

8. المعالجة الآلية وإنشاء الملفات التعريفية

قد نستخدم وسائل آلية وشبه آلية لتحليل الأحداث التقنية، والمعاملات، ومخاطر AML، والأنشطة المشبوهة، ومخالفات القواعد، وتعدد الحسابات، وغيرها من عوامل الأمن.

تتموضع المنصة باعتبارها privacy-first: نسعى إلى تقليل جمع البيانات الشخصية، وعدم طلب وثائق الهوية دون ضرورة، واستخدام نهج قائم على المخاطر في الفحوصات. ولا يعني privacy-first إخفاء الهوية بالكامل، ولا

يستبعد معالجة البيانات اللازمة للأمن، والامتثال للقانون، وإجراءات AML/KYC/CTF، وتسوية النزاعات، ومنع الاحتيال، وحماية المنصة.

قد تؤثر هذه المعالجة على إتاحة بعض وظائف المنصة، أو الحدود، أو الحاجة إلى تحقق إضافي، أو تعليق العملية، أو إحالة الحالة إلى مراجعة يدوية.

9. نقل البيانات إلى أطراف ثالثة

لا نبيع البيانات الشخصية للمستخدمين ولا ننقلها إلى أطراف ثالثة لأغراض التسويق المستقل لتلك الأطراف دون موافقة المستخدم.

قد ننقل البيانات الشخصية إلى الفئات التالية من المستلمين:

1. مزودي البنية التحتية؛
2. مزودي خدمات AML/KYC/CTF؛
3. البنوك ومزودي خدمات الدفع والمعالجين، فقط إذا شاركت هذه الجهات في خدمة أو عملية محددة؛
4. مزودي التحليلات والتشخيص؛
5. مزودي خدمات الاتصالات؛
6. المستشارين القانونيين ومراجعي الحسابات ومستشاري الامتثال؛
7. الجهات المرتبطة بالمشركة؛
8. السلطات المختصة؛
9. الأطراف المقابلة في معاملة P2P — فقط بإقرار اللازم لتنفيذ المعاملة؛
10. الخلفاء المحتملين أو الفعليين في حالة التغييرات المؤسسية.

في معاملة P2P العادية، يتم الدفع بالعملة الورقية مباشرة بين المستخدمين، ولا تعالج الشركة الدفع بالعملة الورقية بصفقتها وسيط دفع.

10. النقل العابر للحدود للبيانات

قد تستخدم المنصة بنية تحتية وشركاء ومقاولين ومعالجين موجودين في دول مختلفة. وبناءً على ذلك، قد يتم نقل البيانات الشخصية وتخزينها ومعالجتها خارج بلد إقامة المستخدم أو بلد تسجيل الشركة.

عند النقل العابر للحدود للبيانات، نتخذ تدابير معقولة لضمان مستوى مناسب من حماية البيانات الشخصية، بما في ذلك الالتزامات التعاقدية بالسرية، والتدابير الأمنية التقنية والتنظيمية، والتحقق من الموردين، وغيرها من الآليات المنصوص عليها في القانون المعمول به.

11. تخزين البيانات الشخصية

نحتفظ ببيانات الشخصية للمدة اللازمة للأغراض التي جُمعت من أجلها، وكذلك للامتثال للالتزامات القانونية، وتسوية النزاعات، ومنع الاحتيال، وحماية حقوق الشركة والمستخدمين.

مدد التخزين الإرشادية:

1. بيانات الحساب — طوال مدة وجود الحساب ولمدة معقولة بعد إغلاقه؛
2. بيانات المعاملات، والأرصدة، والإيداعات، والسحوبات، ومعاملات P2P — لمدة لا تقل عن المدة المطلوبة بموجب القانون المعمول به، أو قواعد AML/CTF، أو متطلبات المحاسبة، أو قواعد إدارة المخاطر الداخلية؛
3. بيانات AML/KYC/CTF — خلال المدة التي يحددها القانون المعمول به؛
4. بيانات الدعم — خلال المدة اللازمة لمعالجة الطلب، وتسوية النزاع، وتحسين الخدمة، وحماية حقوق الشركة؛
5. السجلات التقنية وبيانات الأمان — خلال المدة اللازمة للأمن، والتشخيص، والتحقيق في الحوادث، ومنع إساءة الاستخدام؛
6. بيانات التسويق — إلى حين سحب الموافقة أو رفض الرسائل، ما لم يكن التخزين لمدة أطول ضرورياً لإثبات واقعة الموافقة أو الرفض.

لا يعني حذف الحساب أو سحب الموافقة دائماً حذف جميع البيانات فوراً. قد نحتفظ ببيانات إذا كان ذلك ضرورياً

للامتثال للقانون، أو AML/KYC/CTF، أو المحاسبة، أو منع الاحتيال، أو تسوية النزاعات، أو تنفيذ متطلبات قضائية أو تنظيمية، أو حماية حقوق الشركة.

12. بيانات البلوكشين العامة

يدرك المستخدم أن العمليات المتعلقة بالأصول الرقمية قد تُسجل في شبكات بلوكشين عامة أو شبه عامة. ولا تُعد الشركة مشغلاً لهذه الشبكات، ولا تتحكم في عملها، ولا يمكنها حذف أو إخفاء أو تعديل أو تقييد انتشار المعلومات المنشورة بلأفعل على البلوكشين.

13. سرية الحساب ومسؤولية المستخدم

يلتزم المستخدم بإحفاظ بنفسه على سرية بيانات الوصول إلى الحساب، بما في ذلك كلمة مرور النسخة الويب، ورمز PIN الخاص بـ Telegram Mini App، ورموز 2FA، والأجهزة، وemail، وحساب Telegram، وغيرها من وسائل التفويض.

لا يجوز للمستخدم نقل كلمة المرور، أو رمز PIN، أو الرموز لمرة واحدة، أو رموز 2FA، أو عبارة seed، أو المفاتيح الخاصة، أو رموز النسخ الاحتياطي، أو الوصول إلى الجهاز أو حساب Telegram، أو أي بيانات أخرى تتيح الوصول إلى الحساب أو الأصول الرقمية، إلى أطراف ثالثة.

لا تطلب الشركة عبارات seed، أو المفاتيح الخاصة، أو بيانات البطاقات المصرفية الكاملة، أو رموز CVV/CVC، أو كلمات مرور الخدمات الخارجية.

14. بيانات الأطراف الثالثة

لا يجوز للمستخدم نقل بيانات شخصية لأطراف ثالثة إلى الشركة دون أساس قانوني وموافقة هؤلاء الأشخاص، إذا كانت هذه الموافقة مطلوبة. إذا نقل المستخدم بيانات أطراف ثالثة في إطار معاملة P2P، أو طلب دعم، أو نزاع، أو تحميل وثائق، أو أي تفاعل آخر مع المنصة، فإنه يؤكد أن له الحق في نقل هذه البيانات.

15. حقوق المستخدم

بحسب القانون المعمول به، قد يكون للمستخدم الحق في:

- الوصول إلى البيانات الشخصية؛
- الحصول على نسخة من البيانات؛
- تصحيح البيانات غير الدقيقة أو غير الكاملة أو القديمة؛
- حذف البيانات؛
- تقييد المعالجة؛
- الاعتراض على المعالجة؛
- نقل البيانات؛
- سحب الموافقة؛
- تقديم شكوى إلى سلطة رقابية مختصة.

يجوز لنا رفض الحذف الكامل أو الجزئي للبيانات إذا كان الاحتفاظ بها ضرورياً للامتثال للقانون، أو التزامات AML/KYC/CTF، أو المحاسبة، أو منع الاحتيال، أو تسوية النزاعات، أو تنفيذ العقود، أو حماية حقوق الشركة.

16. أمن البيانات الشخصية

نطبق تدابير تقنية وتنظيمية معقولة لحماية البيانات الشخصية، بما في ذلك تشفير نقل البيانات، والتحكم في الوصول، وفصل الصلاحيات، وتسجيل الإجراءات، ومراقبة النشاط المشبوه، والنسخ الاحتياطي، وإجراءات الاستجابة للحوادث، وقواعد أمن المعلومات الداخلية.

وعلى الرغم من التدابير المتخذة، لا توجد أي طريقة لنقل البيانات عبر الإنترنت أو أي نظام تخزين آمن بشكل مطلق. ويجب على المستخدم الالتزام بتدابير الأمن من جانبه.

17. الأطفال والقصّر

لا تستهدف المنصة الأشخاص الذين لم يبلغوا الحد الأدنى من العمر اللازم لاستخدام الخدمات ذات الصلة بصورة مستقلة في بلد إقامة المستخدم.

18. روابط الموارد الخارجية

قد تحتوي المنصة على روابط إلى مواقع، أو تطبيقات، أو محافظ، أو مستكشفات بلوكشين، أو خدمات دفع، أو موارد Telegram، أو غيرها من الخدمات الخارجية التابعة لأطراف ثالثة. ولا تتحكم الشركة في هذه الموارد التابعة لأطراف ثالثة، ولا تتحمل المسؤولية عن سياسات الخصوصية أو الأمن أو المحتوى أو معالجة البيانات الخاصة بها.

19. تعديل السياسة

قد نقوم بتعديل هذه السياسة دورياً لتعكس التغييرات في المنصة، أو التشريعات، أو متطلبات الشركاء، أو التقنيات، أو المخاطر، أو العمليات الداخلية. تُنشر النسخة الحالية من السياسة على الموقع <https://kashbi.io> أو في واجهة المنصة.

20. التواصل معنا

فيما يتعلق بالأسئلة الخاصة بهذه السياسة، أو معالجة البيانات الشخصية، أو ممارسة حقوق المستخدم، أو الشكاوى، يمكن للمستخدم التواصل عبر:

- الشركة: F-Tech
- دولة التسجيل: Kazakhstan
- الموقع: <https://kashbi.io>
- التطبيق: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](https://t.me/kashbi_support)
- العنوان القانوني: Al-Farabi Avenue, Apartment 207 44/1

21. النسخ اللغوية

يجوز نشر هذه الوثيقة بلغات مختلفة. إذا كان القانون المعمول به يتطلب أولوية نسخة لغوية معينة، فتطبق تلك النسخة. وفي غير ذلك من الحالات، عند وجود اختلافات بين النسخ اللغوية، تكون الأولوية للنسخة الإنجليزية.