

الأمن والثقة

آخر تحديث: 14 أكتوبر 2026

كيف نحمي بياناتك

- **التشفير.** تُشفّر البيانات أثناء النقل (TLS 1.2 أو أحدث) وأثناء التخزين في بيئة الإنتاج.
- **الوصول.** حسابات فردية لكل من يصل إلى بيئة الإنتاج، وصلاحيات بالحد الأدنى، ومصادقة متعددة العوامل على لوحات التحكم السحابية، وإلغاء الوصول فور مغادرة الموظف.
- **السجلات.** تسجيل كل وصول إلى بيئة الإنتاج ومراجعة الأنشطة غير المعتادة.
- **النسخ الاحتياطي.** نسخ احتياطية مشفرة ومنظمة مع اختبار الاستعادة.
- **الاستضافة.** تعمل خدماتنا على Amazon Web Services و Microsoft Azure. والمناطق المستخدمة والمعالجون من الباطن مدرجون في صفحة المعالجين من الباطن.
- **الفصل.** تُحفظ بيانات العملاء الذين أوقفوا استخدام بياناتهم في التدريب خارج بيئة تدريب النماذج.

كيف نتعامل مع الذكاء الاصطناعي

- نستخدم بيانات العملاء بعد إزالة الهوية حيثما أمكن، لتدريب نماذجنا وتحسينها، ويمكن لكل عميل إيقاف ذلك في أي وقت من إعدادات حسابه.
- لا نمنح تسجيلات فني الأصوات ولا نماذجهم الصوتية لأي طرف ثالث، ويُدفع لكل فنان مقابل كل استخدام مدفوع لصوته.
- يحمل كل صوت مودّل علامة مائية غير مسموعة، ونحتفظ بسجلات التوليد لمدة تصل إلى 12 شهراً للتحقيق في إساءة الاستخدام.
- لا يُستنسخ أي صوت دون موافقة موثقة من صاحبه، وأصوات الشخصيات العامة محظورة.

الامتثال

- نعمل حالياً، مع شريك متخصص، نحو شهادتي ISO/IEC 27001 و ISO/IEC 42001، والالتزام بقانون حماية البيانات الشخصية الإماراتي، ومعايير ضمان المعلومات الإماراتية، وسياسة أمن الحوسبة السحابية الوطنية، و CSA STAR المستوى الأول. ولا نحمل أي شهادة بعد، وسنحدّث هذه الصفحة عند الحصول عليها.
- سياساتنا الأمنية ونتائج التقييم الأخيرة متاحة للعملاء المؤسسيين بموجب اتفاقية سرية عبر security@echonova.ai.

الإبلاغ عن ثغرة أو حادث

أرسل أي ثغرة أمنية أو حادث مشتبّه به إلى **security@echonova.ai**. نرد خلال يومي عمل. ولن نلاحق قانونياً الباحثين الذين يبلغون بحسن نية، ولا يصلون إلى بيانات غير بياناتهم، ولا يعطلون الخدمة، ويمهلوننا وقتاً معقولاً للإصلاح قبل أي نشر.

Security and Trust.

LAST UPDATED: 14 OCTOBER 2026

How we protect your data

- **Encryption.** Data is encrypted in transit (TLS 1.2 or higher) and at rest in production storage.
- **Access.** Named individual accounts for everyone with production access, least privilege, multi-factor authentication on cloud consoles, and access removed as soon as someone leaves.
- **Logging.** Every production access is logged, and unusual activity is reviewed.
- **Backups.** Regular encrypted backups with tested restores.
- **Hosting.** Our services run on Amazon Web Services and Microsoft Azure. The regions in use and our subprocessors are listed on the subprocessors page.
- **Separation.** Data from customers who have turned training off is kept out of the model-training environment.

How we handle AI

- We use customer data, de-identified where possible, to train and improve our models. Every customer can turn this off at any time in their account settings.
- We never give voice artists' recordings or voice models to any third party, and every artist is paid for each paid use of their voice.
- Every generated audio file carries an inaudible watermark, and we keep generation records for up to 12 months to investigate misuse.
- No voice is cloned without its owner's documented consent, and public figures' voices are blocked.

Compliance

- With a specialist partner, we are working towards ISO/IEC 27001 and ISO/IEC 42001 certification, and alignment with the UAE Personal Data Protection Law, the UAE Information Assurance standards, the National Cloud Security Policy and CSA STAR Level 1. We hold no certification yet, and we will update this page when we do.
- Our security policies and latest assessment results are available to enterprise customers under NDA through security@echonova.ai.

Reporting a vulnerability or incident

Send any security vulnerability or suspected incident to security@echonova.ai. We reply within two business days. We will not take legal action against researchers who report in good faith, access no data other than their own, do not disrupt the service, and give us reasonable time to fix the issue before any disclosure.