Sovereignty Risk Scorecard

Twelve questions to measure how exposed your meetings are today — to foreign law, to opaque AI processing and to voice deepfakes. It takes about ten minutes and applies to the tools you use now, whatever they are.

How to use it. Tick one answer per question and add up the points shown in purple (0, 1 or 2). The lower the total, the lower the risk. Answer for the tool your organisation actually uses for sensitive meetings — board, finance, legal, HR, client negotiations. If you don't know an answer, tick the riskiest one: what you cannot verify, you cannot defend in front of a regulator.

A. Jurisdiction

1. Where is your meeting provider's parent company incorporated?

A provider's legal home decides which governments can compel it, wherever the servers are.

☐ In the EU **0** ☐ EU subsidiary of a non-EU group **1** ☐ Outside the EU, or don't know **2**

2. Could a non-EU authority compel your provider to hand over meeting content (for example under the US CLOUD Act)?

An "EU data region" settles where data sits, not who can be ordered to produce it.

☐ No **0** ☐ Not sure **1** ☐ Yes **2**

3. Where are recordings, transcripts and meeting minutes stored?

Minutes often hold more sensitive information than the meeting itself: decisions, amounts, names.

☐ In the EU with an EU provider, or on our own servers **0** ☐ In an EU region of a non-EU provider **1**

☐ Outside the EU, or don't know **2**

B. AI processing

4. Who runs the AI that transcribes, translates and summarises your meetings?

Open-weight models run in Europe settle location, not control: licence, hardware, roadmap and recourse remain foreign. What matters is who operates the model and where the content goes.

☐ Our provider, self-hosted in the EU or on our premises **0** ☐ Hosted in the EU but supplied by a third party **1**

☐ An external API outside the EU, or don't know **2**

5. Can your meeting content be used to train AI models?

Once content has trained a model, it cannot be taken back.

☐ Contractually excluded **0** ☐ Excluded only if we opt out **1** ☐ Allowed, or don't know **2**

6. Who controls the encryption keys for your stored meeting data?

Whoever holds the keys can be compelled to use them.

☐ We do (customer-managed keys) **0** ☐ An EU provider **1** ☐ A non-EU provider, or don't know **2**

C. Voice and identity

7. Could a cloned voice join one of your meetings without anyone noticing?

A few seconds of public audio — an earnings call, a podcast, a conference talk — are enough to clone an executive's voice.

☐ No: voices are checked live, in the meeting **0** ☐ Only manual call-back procedures **1** ☐ Nothing in place **2**

8. Do the people who can approve a payment, an order or a contract have a verified voice identity?

The attack targets the person who says yes, not your network.

☐ Yes **0** ☐ Some of them **1** ☐ No **2**

9. When you translate speech, whose voice is used, and who holds a model of it?

Sending your executives' voices to an outside voice service creates a model of their voice that you do not control.

☐ No synthetic voice, or the speaker's own voice processed by our provider **0**

☐ A third-party voice service in the EU **1** ☐ A third-party voice service outside the EU, or don't know **2**

D. Compliance and control

10. Is AI-generated or AI-altered audio in your meetings disclosed to participants and marked in machine-readable form?

Article 50 of the EU AI Act has applied since 2 August 2026, with fines up to €15 million or 3% of worldwide turnover. It requires marking synthetic content; it does not require detecting deepfakes — that protection is a separate decision.

☐ Yes **0** ☐ Partly **1** ☐ No, or don't know **2**

11. If required, could you run your meeting platform on your own servers, including air-gapped?

Some meetings — defence, investigations, M&A — should never touch a shared cloud.

☐ Yes **0** ☐ Only as a private cloud instance **1** ☐ No **2**

12. Could you show an auditor or regulator, today, every subprocessor that handles your meeting data and where it processes it?

GDPR, NIS2 and DORA all expect you to know your supply chain, not just your main supplier.

☐ Yes **0** ☐ Partly **1** ☐ No **2**

Your total: _____ / 24

What your score means

0 – 6 · Low exposure
Your meetings are well protected. Keep evidence of each answer ready for your auditors.

7 – 14 · Moderate exposure
Gaps remain — usually AI processing, keys or voice identity. Fix the questions where you scored 2 first.

15 – 24 · High exposure
Sensitive decisions are exposed to foreign law, opaque AI or voice fraud. Treat it as a priority risk.

Three things to do next

1. **Map your sensitive meetings.** List the meetings where a decision, a payment or confidential information is at stake, and the tool each one uses.
2. **Ask your provider for evidence** on every question where you scored 2: parent company, subprocessors, AI models, key management, training policy.
3. **Protect the people who say yes.** Add a voice-identity check for anyone who can approve a payment or an order by call or video.

About Kizwork. Kizwork is a French company (Sophia Antipolis, with an establishment in Lisbon). Its meeting platform runs in the EU (Scaleway — Paris, Amsterdam, Warsaw), on your own servers (air-gap capable) or in your own cloud. It flags cloned voices live in the meeting — 99.1% accuracy on a balanced test set, alert in 2–3 seconds; independent validation commissioned — and offers a certified voice identity and speech-to-speech translation in each speaker's own voice, in 47 languages, with no third-party AI voice. Send us your completed scorecard at **contact@kizwork.com** and we will go through it with you.

This scorecard is a self-assessment aid, not legal advice. Kizwork S.A.S., RCS Grasse 891 606 519 · www.kizwork.com