GDPR Checklist for AI Meeting Tools in 2026 (Vendor Evaluation Guide)

Buyer-side checklist for evaluating AI meeting tools under GDPR: DPA and Article 28, EU Standard Contractual Clauses, Transfer Impact Assessments, Technical/Organizational Measures, sub-processor transparency, and your controller-side obligations.

Published by Julian Pscheid · December 7, 2025 · Updated May 1, 2026
Read this article online: https://www.hedy.ai/post/gdpr-checklist-ai-meeting-tools/

Four colleagues having a focused discussion around a conference table with a city skyline behind them

Quick answer A buyer's guide to evaluating AI meeting tools under GDPR — covers DPA/Article 28, EU Standard Contractual Clauses and Transfer Impact Assessments, Technical/Organizational Measures, sub-processor transparency, and your controller-side obligations (lawful basis, transparency, DPIA, data subject rights). Use this as a vendor checklist before procurement signs off.

A practical guide for professionals who want to use AI-powered meeting assistants without creating compliance headaches. For a comparative evaluation of specific tools, see our deep-dive on the best GDPR-compliant AI meeting tool (/post/best-gdpr-compliant-ai-meeting-tool-record-transcribe-eu-data-protection/) .

Using AI to capture meeting insights, generate summaries, and stay on top of action items has become standard practice for knowledge workers. But if you're subject to GDPR—whether you're based in the EU, work with EU clients, or process EU residents' data—you need to think carefully about how these tools handle personal data.

This checklist helps you evaluate any AI meeting tool and ensure your usage stays compliant. We've also included guidance on what you need to do on your side, because even the most privacy-conscious tool can't handle all your GDPR obligations for you.

Part 1: Evaluating Your AI Meeting Tool

Before adopting any AI meeting assistant, verify these fundamentals:

Data Processing Agreements

What to look for:

• A Data Processing Addendum (DPA) that meets Article 28 GDPR requirements
• Clear documentation of what data is processed and for what purposes
• Defined roles (you as controller, the tool provider as processor)

Why it matters: A DPA is required when a vendor processes personal data on your behalf (Article 28). This is separate from your Article 6 lawful basis for the processing itself—you need both. Using a processor without an Article 28-compliant agreement is non-compliant, regardless of your lawful basis.

International Data Transfers

If your tool provider is based outside the EU (most are US-based), you need additional safeguards:

What to look for:

• EU Standard Contractual Clauses (SCCs) incorporated into the agreement
• A Transfer Impact Assessment (TIA) documenting the legal situation in the destination country and any supplementary measures
• Clear information about which sub-processors handle your data and where
• The option for true EU data residency (/post/eu-data-residency/) — your conversation data stored on infrastructure physically located in the European Union

Why it matters: The Schrems II ruling invalidated the EU-US Privacy Shield. Tools that transfer data to the US typically rely on SCCs, but these require case-by-case assessment and, where needed, supplementary measures to ensure adequate protection.

Technical and Organisational Measures (TOMs)

What to look for:

• Documentation of security measures (encryption, access controls, etc.)
• Information about where and how data is stored
• Data retention policies—how long is data kept?
• Options for local/on-device processing vs. cloud processing

Why it matters: You need to verify that your processor has appropriate security measures for the sensitivity of data you're processing.

AI-Specific Considerations

What to look for:

• Confirmation that your data isn't used to train AI models

• Clear data retention policies with AI sub-processors (ideally zero retention)
• Transparency about which AI services process your data

Why it matters: Many AI tools send conversation data to third-party AI services. You need visibility into who processes your data and on what terms. While GDPR doesn't mandate specific retention periods, data minimisation principles favour shorter retention, and zero-retention commitments from AI sub-processors reduce your risk exposure.

Sub-Processor Transparency

What to look for:

• A complete list of sub-processors with their purposes and locations
• Notification process for sub-processor changes
• Ability to object to new sub-processors

Why it matters: Article 28(2) requires processors to obtain controller authorisation for sub-processors. You need visibility into everyone who touches your data and the ability to assess whether their involvement is appropriate.

Part 2: Your Responsibilities as Data Controller

Even with a fully compliant tool, you have obligations that no software can fulfill for you:

Before You Start Recording

Lawful Basis

• Identify your lawful basis for processing under Article 6 GDPR (legitimate interest, consent, contract performance, etc.)
• Document this basis and be prepared to explain it if asked
• Note: Consent is one option, but legitimate interests or contract necessity may be appropriate depending on your context

Transparency and Notice

• Inform all meeting participants that AI tools will process the conversation
• Explain what will be captured, how it will be processed, and who will have access
• Provide this information clearly and before processing begins
• For practical scripts that satisfy both GDPR transparency and most local recording laws, see How to Ask Permission to Record a Meeting (/post/ask-permission-to-record-meeting-consent-scripts/)

Recording Laws (Separate from GDPR)

• Check local laws on recording conversations—many jurisdictions require consent from participants independent of GDPR
• These requirements vary by country and may be stricter than GDPR itself
• When in doubt, obtaining explicit consent addresses both GDPR transparency requirements and most local recording laws

Risk Assessment

• Consider whether a Data Protection Impact Assessment (DPIA) is required
• DPIAs are mandatory for processing likely to result in high risk to individuals' rights and freedoms

• Factors that may indicate high risk include: large-scale processing, sensitive data, new technologies, and systematic monitoring

• Even when not strictly required, DPIAs are good practice for AI-based processing and help demonstrate accountability

Ongoing Compliance

Privacy Policy Updates

• Update your privacy policy to reflect your use of AI meeting tools

• Include: what data is collected, purposes, lawful basis, retention periods, third parties involved, and data subject rights

Data Subject Rights

• Establish processes to handle access requests (people can ask what data you hold about them)

• Enable deletion requests—you need to be able to remove someone's data from your meeting records

• Document how you'll handle objection requests, particularly if relying on legitimate interests

Retention and Deletion

• Define how long you'll keep meeting data based on your stated purposes

• Implement regular deletion schedules

• Data minimisation principles mean you shouldn't keep data longer than necessary

Record Keeping

• Maintain records of processing activities as required by Article 30

• Document your compliance measures and decisions

Annual Review

GDPR compliance isn't a one-time task:

• Review your tool's updated terms, DPA, and sub-processor list at least annually

• Reassess your lawful basis if your use cases change

• Update your DPIA if processing activities change significantly

• Verify your retention schedules are being followed

Part 3: Configuration Decisions

Most AI meeting tools offer various features that affect your privacy posture. For each feature you enable, consider the compliance implications. (For Hedy-specific configuration guidance — what each setting does and recommended profiles for attorneys, healthcare providers, and coaches — see Hedy Privacy Settings Explained (/post/ai-meeting-privacy-settings-explained/) .)

.gdpr-table { width: 100%; border-collapse: collapse; margin: 1.5em 0; font-size: 1rem; } .gdpr-table th, .gdpr-table td { padding: 12px 16px; text-align: left; border-bottom: 1px solid #e2e8f0; } .gdpr-table th { background-color: #f8fafc; font-weight: 600; color: #1e293b; } .gdpr-table tr:hover { background-color: #f8fafc; } .gdpr-table td:first-child { font-weight: 500; color: #334155; }

Feature	Privacy Consideration
Cloud sync	Data leaves your device and is stored on provider's servers
Live AI coaching/suggestions	Real-time data transmission to AI services
Email summaries	Meeting content transmitted via email (generally unencrypted)
Audio recording storage	Voice recordings are personal data; see note below on biometric data
Sharing/collaboration	Extends data access to additional parties
API integrations	Data flows to additional third-party systems

Note on audio recordings: Voice recordings are personal data. They may qualify as special category biometric data under Article 9 if processed for the purpose of uniquely identifying a person (e.g., voiceprint analysis, speaker identification systems). Standard meeting recordings used for transcription and note-taking typically don't fall into this category, but if you're using voice identification features, Article 9 requirements apply.

General principle: Enable only what you need. Each additional feature expands your data processing footprint and requires justification under data minimisation principles.

Special Categories of Data

If your meetings involve sensitive data under Article 9 GDPR—health information, political opinions, religious beliefs, data processed for unique biometric identification, etc.—you need enhanced protections:

- A specific lawful basis under both Article 6 AND a condition under Article 9(2)
- Explicit consent is commonly used, but other conditions may apply depending on context
- Stronger security measures appropriate to the sensitivity
- DPIA likely required
- Consider whether cloud features are appropriate given the risk profile

Part 4: Practical Implementation

Sample Notice and Consent Language

Before starting any recorded meeting:

> *"I'd like to use an AI assistant to help capture notes and insights from our conversation. This means our discussion will be transcribed and analyzed by AI. The transcript stays under my control and won't be used to train any AI models. Are you comfortable with that?"*

Wait for confirmation before starting. This approach satisfies both GDPR transparency requirements and most local recording consent laws.

Calendar Invite Addition

> *"This meeting will be supported by AI note-taking. If you have concerns about this, please let me know before the meeting."*

Note: This provides advance notice, which is good practice. Depending on your lawful basis and local recording laws, you may still need to confirm consent at the start of the meeting.

Privacy Policy Language (Template)

Include in your privacy policy:

AI Meeting Assistance We use AI-powered tools to transcribe and analyse meetings for the purpose of [capturing action items / improving communication / maintaining accurate records] . This processing is based on [your lawful basis, e.g., legitimate interests in maintaining accurate business records / contract performance / consent] . Meeting data may be processed by our AI meeting tool provider and their sub-processors. Data may be transferred to the United States under EU Standard Contractual Clauses with appropriate supplementary measures. Meeting transcripts and summaries are retained for [X period] and then deleted. You may request access to, correction of, or deletion of your data by contacting [contact details] .

Adapt this to your specific situation and lawful basis.

How Hedy Handles GDPR Compliance

We built Hedy with privacy as a core principle, not an afterthought. For the full breakdown of Hedy's GDPR compliance (/post/hedy-ai-gdpr-compliance/) — including the DPA, SCCs, and Transfer Impact Assessment — see the dedicated post. Here's how we've addressed the requirements in this checklist:

Contractual Framework

• Data Processing Addendum with EU Standard Contractual Clauses included automatically with your account

• Transfer Impact Assessment available documenting US data transfer safeguards and supplementary measures

• Complete Technical and Organisational Measures documentation

• Transparent sub-processor list with change notifications

Privacy-First Architecture

• On-device speech recognition by default—your audio never leaves your device unless you enable cloud features

• Zero data retention agreements with AI sub-processors

• Your data is never used to train AI models

• Granular controls: enable only the features you need

Compliance Documentation

• Full documentation available in our Trust Center

• GDPR compliance guidance for users (controller responsibilities)

• Independent SOC 2 Type I examination and HIPAA assessment complete

User Control

• Local-only mode available for maximum privacy

• Delete your data anytime

• Export your data for portability

• EU data protection region setting to minimise tracking

Access our complete compliance documentation at trust.hedy.ai (https://trust.hedy.ai) .

Frequently Asked Questions

How do I evaluate an AI meeting tool for GDPR compliance?

Check four things: a DPA that meets Article 28 (with EU SCCs if the vendor is outside the EU), a Transfer Impact Assessment documenting US-data-protection laws and supplementary measures, documented Technical/Organizational Measures, and a complete sub-processor list with notification rights. If a vendor can't produce all four, they're not GDPR-ready for your business.

What questions should I ask a vendor about GDPR?

Five baseline questions: (1) Can you provide a DPA with Article 28 clauses? (2) Where is data physically stored, and do you offer EU residency? (3) Are EU Standard Contractual Clauses incorporated for any non-EU transfers, and is a TIA available? (4) Who are your sub-processors and where do they operate? (5) Is my data ever used to train AI models? If any answer is missing, push back.

What is a Standard Contractual Clause and do I need one?

Standard Contractual Clauses (SCCs) are EU-approved contractual templates that bind a non-EU data importer to EU-level protections when personal data is transferred outside the EU. After Schrems II, US-based vendors typically rely on SCCs plus supplementary measures documented in a Transfer Impact Assessment. If your vendor is in the US and processes EU personal data, yes — you need SCCs in place.

Do I need a Data Protection Impact Assessment for AI meeting tools?

A DPIA is mandatory under Article 35 if processing is likely to result in high risk to data subjects — typical triggers include systematic monitoring, large-scale processing, sensitive data, or new technologies. AI-based recording often hits one or more triggers. Even when not strictly required, a DPIA is good practice and demonstrates accountability.

What are my responsibilities as a data controller when using AI meeting tools?

Establish a lawful basis under Article 6 (legitimate interest, consent, contract performance), provide transparency notices to participants before recording, maintain Article 30 records of processing activities, conduct a DPIA where required, handle data subject rights (access, deletion, objection), and update your privacy policy. The vendor handles processor-side obligations; you handle controller-side.

Questions?

GDPR compliance can feel complex, but it doesn't have to be overwhelming. If you have questions about using Hedy in a GDPR-compliant way, reach out to us at privacy@hedy.ai (mailto:privacy@hedy.ai) or consult our help documentation (https://help.hedy.bot) .

For complex compliance questions specific to your organisation, we recommend consulting with a qualified data protection professional or your Data Protection Officer.

This guide provides general information about GDPR compliance for AI meeting tools. It is not legal advice and should not be relied upon as such. Requirements may vary based on your specific situation, jurisdiction, and the nature of data you process. Local laws regarding recording conversations may impose additional requirements beyond GDPR.