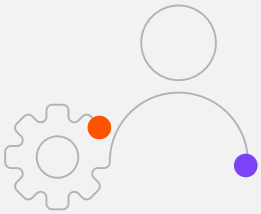
SQUIRE PATTON BOGGS

Pensions quick guide

AI notetakers in trustee meetings



What is an AI notetaker?

An AI notetaker is a software tool designed to join online meetings to record, transcribe and summarise the discussions which take place. AI tools may be built into platforms (such as Microsoft Teams or Zoom), or enabled by meeting participants using third-party apps such as Knowa.

A tool that captures trustee discussions and produces meeting minutes may increase efficiency and reduce the cost of manually drafting minutes. However, trustees should be aware of the risks associated with the use of AI notetakers to record and store decisions made in trustee meetings, particularly in circumstances where commercially sensitive information is being discussed. Unless properly managed, it could be the same as letting an unknown person take notes and share them with all their contacts!

How does an AI notetaker work?

Often, the software tool records the online meeting and sends audio, as well as chat to external cloud services for processing and storage out of the trustees' control.

What are the risks associated with AI notetakers?

- Confidentiality and personal data breaches may occur as a result of (a) transcript data being used to train the AI platform to produce minutes in a specific format, and/or (b) transcripts leaving secure environments. Privileged data may be stored by providers and shared with others, which can damage trust and harm reputation. In order to mitigate this risk, trustees who use AI for governance purposes should ensure that they understand:
  - (a) How the platform is trained
  - (b) How data is processed
  - (c) What data protection/security measures are in place
- AI transcriptions can be inaccurate, leading to incorrect or misleading information being stored and shared. To avoid any discrepancies, it is imperative that draft minutes are circulated to all meeting attendees for review and sign off prior to being finalised.
- Recording or transcribing without proper consent can create legal dangers, and such records may be discoverable in legal proceedings. Where personal or commercially sensitive data is being disclosed in a trustee meeting, it is important that consent is obtained from those in attendance.
- Even if the primary meeting participants are not intending to record or use an AI notetaker, participants can join trustee meetings with their own unapproved notetakers (including third-party tools) leading to the potential exposure of privileged conversations to unknown systems.

Some practical points

Do	Don't
Do scan the meeting's participant list for unknown names such as "Notetaker", "Fireflies", "Zoom AI Companion", "AI Assistant", "Otter" or others ending in "bot", "AI" or "assistant", and be aware of banners and chat notifications such as "Recording started" or "Transcription enabled", which indicate that the meeting is being recorded.	Don't install or enable external notetaker services – only ever use approved meeting tools.
Do request confirmation as to whether any AI tools are being used to record and/or transcribe the meeting. If necessary, opt-out of AI notetaking or leave the meeting and continue discussions offline.	Don't assume that an AI notetaker is not present in the meeting on the basis that the trustee has not enabled AI. It is crucial to stay alert as to what other participants might add.
Do split out the meeting agenda into commercially sensitive items (such as discussions surrounding the sponsoring employer and member complaints) and non-commercially sensitive items. If the meeting is being recorded and/or transcribed, turn off the recording/transcription when discussing any commercially sensitive items.	Don't discuss commercially sensitive details until privacy is confirmed.
If privileged, commercially sensitive information or personal data is inadvertently captured, consider whether this comes within the scope of the Trustees' data protection and cyber security policy/data breach and cyber incident response plan and if so, follow the relevant policy guidance and consider whether the incident is reportable to the Information Commissioner's office (ICO), and/or the data subject.	If you wouldn't discuss an issue in a public place, don't do it online unless you know who and what is listening.

Contacts

Matthew Giles
Partner, Birmingham
T +44 121 222 3296
matthew.giles@squirepb.com

Gemma Hanley
Partner, Leeds
T +44 113 284 7000
gemma.hanley@squirepb.com

71291/06/26