

Tigermeeting

Compliance by Architecture:

How Tigermeeting maps to GDPR, NIS2, the Cyber Resilience Act and ISO/IEC 27001

White Paper

Zoltan Arpadffy, CTO

Contents

Contents 2
Introduction 3
Executive Summary 3
Why meeting-room data is in regulatory scope 4
Data map: what Tigermeeting processes and where it lives 4
GDPR mapping 6
NIS2 mapping 7
Cyber Resilience Act mapping 8
ISO/IEC 27001:2022 Annex A mapping 9
Shared responsibility: what Tigermeeting does not change 9
Data sovereignty and international transfers 10
Procurement and audit checklist 11
Conclusion 12
References 12
Contact information 14
Social media 14

Introduction

Tigermeeting is the leading on-premises solution for meeting room management, digital signage and access control — fully decentralized, serverless, and built for extreme scalability.
Designed for enterprise-grade reliability, it offers a perpetual licensing model with no hidden costs or cloud dependencies.

How could we achieve this? The answer is simple: We listen to our customers.

We own the technology. We know the industry. We are passionate about what we do. We consider customer needs. We adjust our product and service roadmap accordingly. Our consistent Blue Ocean strategy and focus on the market earned us respect from both customers and competitors.

We see that our products are able to provide great and affordable service for schools, universities, offices and organizations with simple, functional, efficient and reliable meeting room management solution - that is already highly appreciated worldwide.

Executive Summary

Tigermeeting narrows compliance scope by keeping meeting data on the customer's own network, but it does not make an organisation compliant on its own.

This paper maps the product's architecture to four frameworks that procurement, security and data-protection teams ask about most: GDPR, NIS2, the Cyber Resilience Act (CRA) and ISO/IEC 27001:2022. For each one it states what the architecture contributes, what remains the customer's job, and where the answer depends on the calendar system behind Tigermeeting.
Tigermeeting architecture is sovereign and air-gapped by design.

Three points to take away:

- **Meeting data stays on your network.** Screens fetch from your calendar system only the minimum needed to show the next meetings, cache it, and sync their configuration with each other over the local network. Tigermeeting's own cloud,

hosted in the EU, holds only account, licence and optional service data, never meeting or personal content.

- **Tigermeeting uses your existing calendar system.** If that is Microsoft 365 or Google Workspace, the provider's data location and legal exposure still apply. If it is on-premises Exchange, Domino, Garoon, Nextcloud, Odoo, Zimbra, Carbonio, another self-hosted server or Tigermeeting's built-in local calendar, the whole data path can stay inside your perimeter.
- **Compliance belongs to the operator, not the product.** This paper is a mapping aid. It is not legal advice and not a certification.

Why meeting-room data is in regulatory scope

Meeting-room data is personal data, and the screens that show it are part of your ICT estate.

A booking records who met, when, where and often why. Subjects can reveal sensitive matters such as a disciplinary hearing, a patient case review or a merger working group, and the pattern of bookings shows who works with whom. Under GDPR that is personal data about employees and visitors, whatever product holds it.

The room screens are also networked devices inside your perimeter. NIS2 and ISO/IEC 27001 treat them as assets and their vendor as a supplier. Under the CRA, the vendor is the manufacturer of a product with digital elements.

Three questions follow: where does the data live, who can reach it, and who is accountable for the device and its updates. The architecture answers the first two directly. The third is shared.

Data map: what Tigermeeting processes and where it lives

Meeting data stays on your network. Tigermeeting's own cloud services, hosted in the European Union, hold only account, licence and optional service data. Your devices query that cloud. It never connects in, and it is not needed for basic calendar operation, which is why Tigermeeting can run air-gapped.

Data	Where it lives	Leaves your network?
Bookings: the minimum needed to show current and next meetings. Attendee names are never shown.	Fetched by each screen from your calendar system for up to the next seven days and held on the screen	Only to and from your calendar provider, never to Tigermeeting
Configuration: rooms, policies, themes	Encrypted database replicated across the screens. The admin app joins as a temporary peer and then leaves.	No, unless you choose the optional encrypted network backup in the Tigermeeting cloud
Calendar sign-in	Calendar caches, API tokens and server connection strings on each screen. Cloud calendars use revocable OAuth2 tokens, not stored passwords.	Token exchange goes to your calendar provider only
Admin account and licence data	Held in the Tigermeeting cloud in hashed form for admin login, and cached on the screens so an admin can log in offline	Yes, to Tigermeeting, under its Privacy Policy
Licence validation and update checks	Devices contact tigermeeting.app over TCP port 443 for licence validation and for software and firmware update checks	Yes. No meeting data is sent. Closed environments can block this after setup.
Optional analytics	Anonymous usage events tied to a device's MAC address or Android ID, sent only if you enable the feature. They carry no meeting titles, organisers or rooms.	Yes, to Tigermeeting, only if enabled
Optional cloud services	Themes and backgrounds, overview maps, weather, NFC validation if hosted by Tigermeeting, the AI assistant and the file store for logos and backgrounds. File-store files are protected by their URL but not encrypted.	Yes, only if you use them
Meeting content in the Tigermeeting cloud	None	Not applicable

Screens find each other by broadcast inside one network segment and sync over UDP ports 6024, 6025, 6030 and 6031 and TCP port 6026, using encrypted payloads. No inbound connection from the internet is needed or possible, because the Tigermeeting cloud is only ever queried by your devices. After an initial online setup, a system with an on-premises calendar can run fully air-gapped - that means the built-in local calendar, CalDAV, Odoo, iCalendar or Webcal feeds, or on-premises Exchange, HCL Domino or Garoon.

Cloud calendars cannot sign in offline, and updates then arrive by USB or a short, controlled opening of access to tigermeeting.app. Technical details of the encryption are available from Tigermeeting on request.

GDPR mapping

The architecture helps most with data minimisation, security and data protection by design. Everything else stays with the controller, which is your organisation.

A product cannot be "GDPR compliant" on its own, because compliance depends on how a controller configures and operates it. The table shows how the architecture supports each duty and what you still do.

GDPR article	What it asks	What the architecture contributes	What you still do
Art. 5(1)(c) Data minimisation	Process only what is needed	No vendor-side copy of bookings, and screens can hide meeting titles. Private meetings never show theirs, and attendee names are never shown.	Decide which booking details appear on screens, for example hide subjects in corridors
Art. 5(1)(f) and Art. 32 Security of processing	Appropriate technical and organisational measures	Encrypted screen-to-screen sync, revocable tokens for cloud calendars, no inbound connections from the internet	Segment the network, patch the screens' operating system, control physical access
Art. 25 Data protection by design and by default	Build protection in from the start	No central or external database for meeting data. Cloud services are optional.	Set protective defaults such as minimal display and check-in rules
Art. 28 Processors	Contract anyone who processes data for you	Tigermeeting AB is not a processor of your meeting data. It neither hosts nor accesses it, and its support staff never access customer screens or systems. Its own account and optional analytics data fall under its Privacy Policy.	Record Tigermeeting as a supplier and review its Privacy Policy
Arts. 44 to 49 Transfers	Safeguards for transfers outside the EEA	Meeting data is not sent to Tigermeeting, whose cloud is hosted in the EU	Assess your calendar provider's transfers
Art. 30 Records of processing	Keep a register	Not applicable	Add room booking to your register: names, subjects, times

GDPR article	What it asks	What the architecture contributes	What you still do
Arts. 15 to 17 Access, correction, erasure	Honour individuals' requests	The calendar system stays the record, and changes there reach the screens by sync	Handle requests in the calendar system
Art. 33 Breach notification	Notify the authority within 72 hours where required	No vendor-held meeting data to breach. A stolen screen holds a short window of cached bookings and calendar tokens.	Revoke the screen's tokens, reset the device, assess, notify if required
Art. 35 Data protection impact assessment	Assess high-risk processing	Low-risk profile in most settings. Use this paper as input.	Decide whether an assessment is needed

NIS2 mapping

NIS2 puts its duties on the entity, not the vendor, so Tigermeeting helps mainly by being a low-risk supplier with a small attack surface.

Article 21(2) of Directive (EU) 2022/2555 lists the minimum risk-management measures. Five of them bear on room-display systems.

Art. 21(2) measure	What the architecture contributes	What you still do
(c) Business continuity	No central server. One failed screen affects one room, and a replacement screen rejoins the mesh and syncs.	Keep the calendar system itself resilient
(d) Supply chain security	Few parties in the data path: no relay, and no meeting data in the vendor's cloud	Include Tigermeeting AB in supplier assessments and ask for its security documentation
(e) Secure maintenance and vulnerability handling	The vendor's own duties arise under the CRA (next section)	Track updates and apply them on a schedule
(h) Cryptography	Encrypted screen-to-screen sync and OAuth2 tokens for cloud calendars	Manage certificates and tokens on the calendar side
(i) Access control and asset management	No permanent admin connection. The admin app joins the mesh only when needed, and only one may be active per network.	Inventory the screens and restrict who holds the admin app

For network placement, follow Tigermeeting's own security instructions. Put the screens

on an isolated IoT or signage VLAN, open UDP 6024, 6025, 6030 and 6031 and TCP 6026 inside that segment, allow outbound TCP 443 only to your calendar provider and, if you use them, to tigermeeting.app, and block inbound connections from outside. Run the admin app behind a firewall or VPN, use dedicated least-privilege service accounts for calendar access, and apply critical security updates within 14 days of release.

Cyber Resilience Act mapping

Under the CRA, Tigermeeting AB is the manufacturer of a product with digital elements, and its obligations are phasing in now.

Regulation (EU) 2024/2847 entered into force on 10 December 2024. Reporting of actively exploited vulnerabilities and severe incidents applies from 11 September 2026, and most other obligations apply from 11 December 2027.

Manufacturer obligation	What Tigermeeting states
Security by design and by default	Security instructions for administrators: isolate the screens on their own VLAN, change default passwords and use least-privilege service accounts
Vulnerability handling	A coordinated disclosure policy with a contact, security@tigermeeting.app. Acknowledgement within 48 hours, a first status update within five working days, and safe harbour for good-faith researchers.
Security updates	At least five years from each release date, with the current version supported until at least 31 December 2031. Security updates stay available for at least ten years from their release.
Software bill of materials	Maintained internally and available to market surveillance authorities on lawful request
Reporting	Actively exploited vulnerabilities are reported to the national CSIRT and ENISA within 24 hours of confirmation
Conformity	An EU declaration of conformity issued by Tigermeeting AB on 13 September 2026, using the internal control procedure

Perpetual licences make the support period matter more, because the product stays in service for years. A perpetual licence includes all future upgrades, and releases are cumulative, so customers stay supported by moving to the latest release. The current statements are on Tigermeeting's compliance page (https://tigermeeting.app/compliance).

ISO/IEC 27001:2022 Annex A mapping

ISO/IEC 27001 certifies an organisation's management system, not a product, so the useful question is which Annex A controls Tigermeeting helps you evidence. Tigermeeting AB makes no certification claim.

Annex A control	What Tigermeeting contributes	Evidence to keep for the audit
5.15 Access control	The admin app joins the mesh only when needed. There is no permanent remote access.	List of people who hold the admin app
5.19 to 5.22 Supplier relationships and ICT supply chain	Small supplier footprint: no relay, and no meeting data in the vendor's cloud	Supplier file for Tigermeeting AB, including its security documentation
5.23 Cloud services	Not a cloud service itself. Your calendar provider still falls under this control.	Assessment of the calendar provider
5.34 Privacy and protection of PII	Data stays on your network	Record of processing entry
7.8 Equipment siting and protection	Applies to the room screens	Mounting and tamper-protection standard
8.5 Secure authentication	OAuth2 tokens in place of stored passwords for cloud calendars	Token revocation test result
8.8 Management of technical vulnerabilities	Vendor patching, with duties under the CRA	Update log and patch schedule
8.20 and 8.22 Network security and segregation	No inbound connections from the internet. Sync confined to one network segment.	Network diagram showing the screen segment
8.24 Use of cryptography	Encrypted screen-to-screen sync	Vendor statement on encryption, with technical details on request
8.15 Logging	Admin and device logs can be downloaded from the admin app	Downloaded admin and device logs

Shared responsibility: what Tigermeeting does not change

Tigermeeting removes the vendor from your data path, but it does not remove your own duties.

Area	Tigermeeting	You
Where meeting data is stored	The minimum booking data needed for the next-meetings view, cached on the screens, no vendor copy	The calendar system: its location, retention and backup
Calendar provider	Connects to it directly	Choose it, contract it and assess its jurisdiction and transfers
Room-screen operating system	Software runs on the screens	Where you supply the display, you patch and lock down its operating system
Network	Needs no inbound connections from the internet	Segmentation, firewall rules, time synchronisation
Physical security	None	Mount screens securely and revoke tokens if one is lost or stolen
Admin access	The admin app joins only when needed	Control who holds it and secure the laptop it runs on
Software updates	Provides security updates	Apply critical updates within 14 days of release, as Tigermeeting's guidance asks. Closed networks update by USB or a short, controlled opening of access to tigermeeting.app.
Incident response	Handles vulnerability disclosure and reporting as manufacturer	Run your own incident process

Two cases show why the split matters. A Microsoft 365 customer keeps Microsoft's data location and legal exposure for calendar content, whatever sits on the wall. A customer on on-premises Exchange, HCL Domino, Odoo, Garoon, Nextcloud, Zimbra or Tigermeeting's built-in local calendar can keep the entire path inside the building.

Data sovereignty and international transfers

Sovereignty depends on the calendar system you choose, because Tigermeeting itself sends nothing to a vendor.

Calendar backend	Where calendar data lives	Foreign-law exposure
Self-hosted: Tigermeeting's built-in local calendar, on-premises Exchange, Zimbra, Carbonio, HCL Domino, Garoon, self-hosted Odoo, Nextcloud, OX and other servers	Inside your perimeter	None beyond your own jurisdiction

Calendar backend	Where calendar data lives	Foreign-law exposure
Hosted in the EU by an EU-owned provider	The provider's EU data centres	EU law, subject to the provider's ownership
Microsoft 365, Zoho or Google Workspace with EU data location	EU data centres	The US CLOUD Act can still reach US-headquartered providers, wherever the data sits
Any provider hosting outside the EU (like Lark, Feishu, Ding Talk, WeCom, Cybozu, Yandex 360)	A third country	A transfer mechanism is required, such as an adequacy decision or standard contractual clauses

Transfers to US providers currently rely on the EU-US Data Privacy Framework adequacy decision of July 2023, which remains open to legal challenge. Check its status when you assess a provider.

Tigermeeting AB is a Swedish company, and its cloud services are hosted in the European Union.

Procurement and audit checklist

Use these questions to assess any room-booking vendor, Tigermeeting included, and keep the answers as audit evidence.

Data

- ☐ Where is meeting data stored, and does any copy exist at the vendor?
- ☐ Is data encrypted at rest on the screens and in transit between them, and with which algorithms?
- ☐ What traffic leaves the network: licensing, updates, diagnostics, analytics?

Access

- ☐ How are calendar credentials stored, and can access be revoked centrally?
- ☐ Does the vendor or its support staff ever have remote access?
- ☐ Who can administer the system, and how is that access limited?

Lifecycle (CRA)

- ☐ What is the security-update support period after purchase?
- ☐ Is there a coordinated vulnerability disclosure policy and a security contact?
- ☐ Is a software bill of materials available?
- ☐ Is there an EU declaration of conformity?

Contract

- ☐ Does the vendor see personal data, and if so, is a data processing agreement in place?
- ☐ Does the system keep working if the vendor stops trading?

Conclusion

Compliance is a shared job, and Tigermeeting's architecture keeps the vendor's share small and easy to evidence. Because meeting data never reaches the vendor and its cloud is optional, the data map is short and the supplier footprint is small, so the hardest questions fall on your calendar system and your network.

Four next steps: add Tigermeeting to your record of processing, place the screens on their own network segment, ask the vendor the lifecycle questions in the checklist, and decide whether a data protection impact assessment is needed.

References

- Regulation (EU) 2016/679, General Data Protection Regulation
- Directive (EU) 2022/2555 (NIS2), Article 21
- Regulation (EU) 2024/2847, Cyber Resilience Act. Dates per the European Commission's CRA page (https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)
- ISO/IEC 27001:2022, Annex A
- Tigermeeting Admin User manual – the latest version is at https://tigermeeting.app/downloads (https://tigermeeting.app/uploads/documents/20260922/Tigermeeting-user-manual-3.5.0-en.pdf)

- Tigermeeting Android Setup manual – the latest version is at https://tigermeeting.app/downloads (https://tigermeeting.app/uploads/documents/20260922/Tigermeeting-android-setup-3.5.0-en.pdf), version 3.5.1
- Tigermeeting GDPR compliance page (https://tigermeeting.app/en/features/gdpr-compliance) and cybersecurity compliance document (https://tigermeeting.app/compliance)
- Tigermeeting white papers: Beyond the Server (https://tigermeeting.app/en/why-tiger/white-paper-beyond-the-server), The Walled Garden (https://tigermeeting.app/en/why-tiger/white-paper-the-walled-garden) and The Sovereign Office (https://tigermeeting.app/en/why-tiger/white-paper-the-sovereign-office)
- Software Bill of Materials (SBOM) https://tigermeeting.app/open-source-licenses
- Tigermeeting supported calendars https://tigermeeting.app/calendars

This paper is a mapping aid, not legal advice. Have your own counsel confirm how these rules apply to your organisation.

Contact information

Email: info@tigermeeting.app

Web: https://tigermeeting.app/contact

Customer Support: support@tigermeeting.app

More information can be obtained under “About” menu in the Admin Application.



Social media

Follow us on social media to get event updates on product news and new releases.

LinkedIn https://www.linkedin.com/company/tigermeeting/

Facebook https://www.facebook.com/tigermeeting/

Instagram https://www.instagram.com/tigermeeting

Threads https://www.threads.net/@tigermeeting

Tik Tok https://www.tiktok.com/@tigermeeting

YouTube https://youtube.com/@tigermeeting

GitHub https://www.github.com/tigermeeting

X(Twitter) https://x.com/tigermeeting

Telegram https://t.me/tigermeeting

Pinterest https://www.pinterest.com/tigermeetingroom/

Bluesky https://bsky.app/profile/Tigermeeting.bsky.social

WhatsApp

https://www.whatsapp.com/channel/0029VanwIDn6LwHgKMtMF90S

Weixin / WeChat

Tigermeeting is trademark of Tigermeeting AB, all other mentioned trademarks are owned by their respective companies.