
The Arc 3 and Collaborate.

A briefing for data protection officers.

REALWEAR · DATA PROTECTION BRIEF

The Arc 3 is RealWear's lightweight (175 g) assisted-reality smart glasses with a see-through monocular display. It runs Ari OS 2.0, which is based on Android 13 (AOSP), on a Qualcomm Snapdragon 662 platform. Technically and from a data protection perspective the device behaves much like a smartphone, with two important differences: the display sits in the user's line of sight, and the cameras are worn at eye level. A head-worn camera is less visible than a hand-held smartphone; for the recording of third parties (customers, colleagues), this imposes an additional duty of care. That duty sits not with the device, but with the customer organisation's internal usage policy.

01 What happens on the Arc 3

Data is captured on the Arc 3 only when an application actively requests it: photo and video via the dual forward-facing cameras (8 MP wide-angle, 48 MP main), audio via the four digital microphones, location via Wi-Fi positioning. Application permissions are visible at all times in the device settings and can be revoked. Like all RealWear devices, the Arc 3 runs on AOSP without Google services: no Google Play Store, no Google Analytics, no Google account requirement, and no automatic connection to Google servers.

Two sensors deserve explicit mention in a data protection review: the awareness sensor is a low-resolution (2 MP) black-and-white sensor with a 160° field of view used by the system for environmental awareness, and a wear detection sensor registers whether the device is being worn. Neither replaces the main cameras, and application access remains governed by Android permissions.

Hardware security

The Arc 3 features a Qualcomm Trusted Execution Environment, a hardware crypto engine, and verified secure boot. Per the RealWear Security Overview, RealWear devices are encrypted out of the box with AES-256 file-based encryption. Sign-in options are the RealWear Companion app, a voice keyboard with secure mode, and Everykey. Source: official Arc 3 specifications.

Updates

Operating system updates are delivered as Ari OS releases and can be rolled out centrally. The official RealWear firmware update and support policy applies; customers should verify the current commitment window for the Arc 3 against that policy.

ARI, the on-device AI assistant

The Arc 3 ships with ARI (Augmented Reality Intelligence), RealWear's AI assistant, alongside Collaborate. The data protection assessment of ARI (processing locations, model providers,

retention) is documented separately; request the current Ari OS security documentation from RealWear before enabling ARI in production.

02 Collaborate

Collaborate is RealWear's Microsoft Teams integration, optimised for head-mounted devices. It enables voice, video, and screen-sharing connections between Arc 3 wearers and standard Microsoft Teams users.

What Collaborate processes

RealWear does not collect personal data on its servers via Collaborate. Anonymised telemetry and crash logs are transmitted for troubleshooting purposes. On the headset itself, Collaborate stores contact names, Azure Entra ID identifiers, and call start times in a local database. This data is used exclusively locally (call history, address book search) and is not transmitted to RealWear. From a data protection perspective this is personal data which remains within the responsibility of the customer organisation. The RealWear Microsoft Teams app itself does not collect data about conversations, calls, or similar activities.

Authentication

Collaborate authenticates exclusively via Microsoft Single Sign-On (device code login). Sign-in credentials are at no point stored or processed by RealWear.

Microsoft Graph permissions

For the full functional scope of Collaborate (current version 2.5), delegated Microsoft Graph permissions are required. Delegated means that the application acts exclusively in the name of the signed-in user, within that user's existing rights. In detail: User.Read, User.ReadBasic.All, Calendars.ReadWrite, Group.Read.All, OnlineMeetings.ReadWrite, Presence.ReadWrite, Teams.ManageCalls, Teams.ManageChat, openid, profile, offline_access, access_as_user. Group.Read.All stands out because it grants access to all groups in the tenant; this is required for the address book functionality and must be released by the tenant administrator.

Microsoft Teams as data processor

Audio, video, and chat content of the Teams connection traverse the Microsoft infrastructure (Azure), exactly as for any other Teams endpoint. The Microsoft data protection terms and the customer organisation's existing Data Processing Agreement with Microsoft apply. The Arc 3 does not retain Teams calls or media persistently unless a manual recording is started.

03 Ari Cloud, optional

Arc 3 devices are managed through Ari Cloud, RealWear's cloud platform for centralised deployment and management of devices. Its use is optional; the device can also be operated standalone. Where Ari Cloud is used, data is transmitted via HTTPS and hosting runs on Microsoft Azure. Certifications: the SOC 2 Type II and ISO 27001 certifications referenced in the RealWear Data Processing Addendum apply to the underlying cloud infrastructure

providers (Microsoft Azure), not to RealWear as a company. This distinction is relevant where a RealWear-issued certification is required for the data protection assessment.

04 The biggest risk remains the human

As with any endpoint, the largest data protection risk lies not in the technology but in user behaviour. Unintentional recording of confidential content, forwarding of recordings through unsanctioned channels, the use of unauthorised applications. Before a productive rollout, a user training is recommended that clearly answers four questions: what may be recorded, where is the data stored, who has access, and how is it deleted. Central application and permission management via MDM complements this, but does not replace it.

05 Sources and further documentation

All statements in this brief are based on the following official RealWear documentation:

- Arc 3 Specifications (hardware security, sensors, sign-in) – support.realwear.com/knowledge/arc3/specifications
- Firmware Update and Support Policy – support.realwear.com/knowledge/realwear-firmware-update-and-support-policy
- Collaborate Technical Info – support.realwear.com/knowledge/collaborate-technical-info
- Collaborate Privacy Policy – realwear.com/legal/collaborate-privacy-policy
- Data Processing Addendum (DPA) – realwear.com/legal/data-processing-addendum

For IT-level follow-up questions

Provided separately as a PDF: Security Overview for Collaborate. This document, prepared by RealWear Software Engineering, describes in detail the architecture (client-side, Azure platform, Microsoft 365 ecosystem), the authentication and authorisation flow, all Microsoft Graph permissions with justification, the firewall configuration including all external endpoints, and the compliance inheritance from Microsoft Azure and Azure Communication Services.

This brief does not replace a Data Protection Impact Assessment.

RealWear Switzerland AG · Manuel Kesselring · July 2026