realwear

2512 E Evergreen Blvd,
PMB 3024 Vancouver, WA, 98661
United States

The Navigator Z1 and Collaborate.

A briefing for data protection officers.

REALWEAR · DATA PROTECTION BRIEF

The Navigator Z1 is a head-mounted, hands-free wearable built for hazardous industrial environments. It is certified intrinsically safe (ATEX and IECEx Zone 1, CSA C1/D1) and runs Android 12 (AOSP) on a Qualcomm QCS6490 platform. Technically and from a data protection perspective the device behaves much like a smartphone or rugged tablet, with two important differences: the display sits in the user's line of sight, and the camera is mounted on the head. The latter matters because a head-mounted 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 Navigator Z1

Data is captured on the Navigator Z1 only when an application actively requests it: photo and video via the 48 MP camera, audio via the microphones, location via GPS or Wi-Fi positioning. Application permissions are visible at all times in the device settings and can be revoked. Unlike standard Android devices, the Navigator Z1 runs Android 12 on AOSP without Google services. There is no Google Play Store, no Google Analytics, no requirement for a Google account, and no automatic connection to Google servers.

Hardware security

The Navigator Z1 is built on the Qualcomm QCS6490 chipset with an on-device AI engine; per the RealWear Security Overview, RealWear devices are encrypted out of the box with AES-256 file-based encryption. For the intrinsic safety certification, the battery pack is mounted with screws that prevent accidental removal in hazardous zones; it remains removable outside those zones. The housing is IP66-rated and 2-metre drop tested. Source: official Navigator Z1 documentation.

Updates

Firmware updates including AOSP security patches are delivered per the official RealWear firmware update and support policy; according to that policy, currently supported devices are committed through at least December 2030. Updates can be distributed centrally via RealWear Cloud or an MDM, so devices in the field do not depend on individual users installing patches.

02 Collaborate

Collaborate is RealWear's Microsoft Teams integration, optimised for head-mounted devices. It enables voice, video, and screen-sharing connections between Navigator Z1 wearers and standard Microsoft Teams users.

2512 E Evergreen Blvd,
PMB 3024 Vancouver, WA, 98661
United States

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 Navigator Z1 does not retain Teams calls or media persistently unless a manual recording is started.

03 RealWear Cloud, optional

RealWear Cloud is a web-based management platform for the centralised administration of devices. It is not mandatory for operating the Navigator Z1; alternatively, a standard MDM such as Microsoft Intune can be used.

Where RealWear Cloud is used: data is transmitted via HTTPS and stored encrypted at rest. Hosting runs on Microsoft Azure Kubernetes Service, protected by a Web Application Firewall. RealWear performs regular penetration tests and security audits. 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.

2512 E Evergreen Blvd,
PMB 3024 Vancouver, WA, 98661
United States

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:

- Navigator Z1 FAQs (features, OS, intrinsic safety) — support.realwear.com/knowledge/realwear-navigator-z1-faqs
- 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
- RealWear Cloud Security — support.realwear.com/knowledge/realwear-cloud-security
- 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