PICO business

COMPLIANT WITH GLOBAL POLICIES AND LAWS

PICO Business has strong focus on world-class data security and data protection, we are fully compliant with global and local practices, guidelines & laws.

DATA PROTECTION BY DESIGN:

- All enterprise headsets can be operated offline without any requirement for account registration.
- The Pico Business store is browsable without any account.
- Register your business account as an admin or invite users to join your company to download apps.
- We have a simple business account registration process: Name, Company Name, Email, Industry and Billing Address.
- Pico is committed to its own compliance with GDPR.

TRANSPARENCY YOU CAN TRUST:

Why do we collect data, what do we do with it, where do we store it?

DEVICE-RELATED DATA

WHY?	WHAT?	WHERE?
The headset data will be collected for device management support and system software use.	Serial Number, Mac Address, Model, Version, Region, Language, Charging, Network Information.	The data is stored on our secured cloud servers in Singapore and USA. The data will not be shared and made accessible across Bytedance companies.

FEATURE-RELATED DATA

WHY?	WHAT?	WHERE?
Position tracking, hand tracking, face tracking and eye tracking requires data from the embedded sensors and cameras.	Raw data: Images of hands, eyes, parts of the face and surrounding environments.	Accessible on the headset, but will be discarded immediately after being processed and will be neither retained on the device nor uploaded to our cloud servers.

PICO business

XR PLATFORM WITH SECURITY AND TRUST

PICO is committed to providing enterprise customers with safe, reliable products and services. We integrate security design into our hardware, systems and software to help provide comprehensive data security.

Enterprise Content you can trust

Dedicated Business Store featuring content

Hardware and System security

SoC supports ARM Trustzone technology with trusted execution environment (TEE) and enhanced kernel security. WPA3 & VPN encryption are supported.

Online Service and Data Security

Pico has established a complete cloud security protection architecture and adopts advanced technologies to ensure data security (for example - advanced network traffic analysis (NTA), web application firewall (WAF), DDoS protection system).

Updates and Management

Clear policies, procedures and requirements are set up to manage all upgrades, patches and incident responses. Full control of updates.

User driven data protection

PICO OS allows users to manage permissions of applications and apply lock screen.

Security Governance and Program

PICO is committed to providing customers with safe and secure product experiences. Dedicated cross-functional departments can support you with specific technical and legal enquiries.

Device-side data security

PICO OS supports encryption based on Android KeyStore and KeyChain as well as Android file-based encryption (FBE), providing computing and algorithm security via kernel-level application sandboxes.

Business software and services security

Optional choices of different business software and platforms under the whole system security.

ETSI/EN 303645 Certification

Product safety certification issued by TÜV SÜD, which proves that the products have met the requirements of ETSI/EN 303645, and can protect users' information security and privacy.

For more information, please reach out to your PICO representative