

RECOMMENDATIONS FOR DEVELOPERS OF MERCHANTS

1. PRIORITIZE USER PRIVACY IN DESIGN

Make user privacy a central consideration in the design and development process of VR shopping apps. Implement privacy-enhancing features and controls, such as clear explicit consent mechanisms before collecting any personal data and granular user permissions, to empower users to manage their data effectively.



2. THIRD-PARTY PARTNERSHIPS AND INTEGRATIONS

Exercise caution when partnering with third-party VR/VTO providers or integrating third-party services into VR shopping apps. Conduct thorough privacy assessments of third-party vendors to ensure alignment with the platform's privacy principles and standards. Ensure that user images and other biometrics are not sent to analytics services, either intentionally or unintentionally, unless explicit permission is obtained from users.



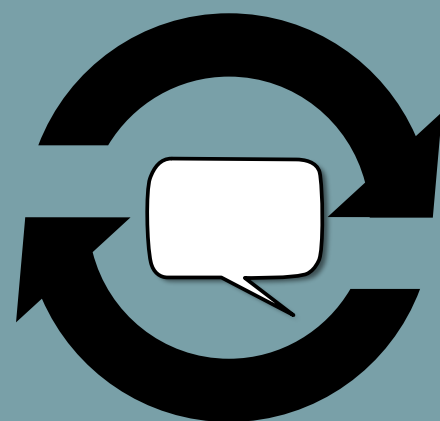
3. HONOR PRIVACY POLICIES AND DISCLAIMERS

Be transparent about your app data collection, handling, and retention practices. Display explicit disclaimers to users in case sensitive information such as user images and biometrics are being collected as part of the AR/VR experience. Ensure that the platform's privacy policies and disclaimers accurately reflect its data handling practices, and the details of the different types of data being handled. Avoid misleading users with contradictory disclaimers or privacy policies that do not align with actual data practices.



4. RESPONSIVE TO USER FEEDBACK

Respond promptly to user inquiries and complaints related to privacy issues, demonstrating a commitment to addressing user privacy needs.



5. MINIMIZE DATA COLLECTION AND RETENTION

Limit the collection and retention of user data to what is strictly necessary for the functionality of the VR shopping app. Minimize the storage of sensitive information, such as biometric data, and adopt data anonymization techniques to mitigate privacy risks.

