

Effective Date: August 22, 2025

Introduction

Orchard Match ("we," "us," or "our") values your privacy. This policy outlines how we handle information collected through our games, ensuring transparency about your data rights.

Key Principles

- When you engage with our games, certain personal data is processed to deliver gameplay functionality.
- Optional data requests (e.g., email for password recovery) are clearly indicated. Providing such data is voluntary, and we will not repurpose it without explicit consent.
- Personalized advertisements may appear in our services. Device-level ad identifier controls allow opting out of personalization while retaining non-targeted ads.
- Deleting a game from your device does not automatically remove stored personal data. Contact us for data deletion requests.

Data Collection & Use

We process personal and non-personal data as follows:

Data Type-Purpose(s)

Google AID: Analytics, fraud prevention, security, functionality, marketing

Android ID: Analytics, fraud prevention, security, functionality, marketing

IDFA / IDFV: Analytics, fraud prevention, security, functionality, marketing

MAC Address: Analytics, fraud prevention, security, functionality, marketing

IP Address: Analytics, fraud prevention, security, functionality, marketing

CPU / Screen / Memory Metrics: Game performance optimization

Device Manufacturer/Model: Marketing, performance optimization

OS / Network Status: Performance optimization

Region/Language/Timezone: Marketing, localization

Excluded Data: We never collect sensitive categories (race, religion, health, etc.).

Technologies Employed

Cookies, SDKs, and similar tools support:

- Service delivery and enhancement
- User behavior analytics
- In-app advertising operations
- Fraud prevention and security

Integrated SDKs:

1. Max SDK

- Purpose: Ad monetization
- Data: Approximate location (IP-based), ad interactions, device identifiers
- Security: Encrypted transit; data deletion via Max GDPR Portal

2. AppsFlyer SDK

- Purpose: Attribution analytics

- Data: Regional location, app events, crash reports, device identifiers
- Security: Encrypted transit; deletion via AppsFlyer GDPR Form

Scope & Legal Basis

Applicability:

- Covers game users and communication channels (email, phone).

Legal Grounds for Processing:

1. Legitimate Interests: Game improvements, ad personalization, fraud prevention (users may object via Section 7).
2. Legal Obligations: Financial record retention.
3. Consent: Optional data uses (revocable at any time).

Your Rights

1. Objection: Challenge processing based on legitimate interests.
 2. Restriction: Limit data use during accuracy disputes.
 3. Access/Correction: Request data details or amend inaccuracies.
 4. Erasure: Demand deletion under applicable laws.
 5. Consent Withdrawal: Revoke previously granted permissions.
 6. Data Portability: Obtain machine-readable copies of consent- or contract-based data.
- Repeat requests may incur administrative fees.

Advertising Practices


- Ad formats: Banners, interstitials, rewarded videos.
- Opting Out: Disable device-level ad identifiers to depersonalize ads.
- Data Recipients: Ad partners receive pseudonymized identifiers/IPs.
- Full partner list: Marketing & Advertising Partners

Data Sharing

1. Infrastructure Providers: AWS (global hosting).
2. Support Teams: Global Step (case management).
3. Advertising/Marketing Partners: See Marketing & Advertising Partners.
4. Authorities: Disclosed only under legal compulsion.

International Transfers:

Data routed globally under EU-approved safeguards (e.g., Standard Contractual Clauses).

 EU Transfer Mechanisms

Security & Age Controls

Protections:

- AWS-secured storage with SSL-encrypted transmissions.

- Restricted data access to trained personnel.

Age Restrictions:

Minimum gameplay ages:

- 16: FR, DE, HU, LT, LU, NL, SK
- 15: FI
- 14: AT
- 13: All other regions

We neither solicit data from nor target ads to underage users.

California (CCPA) Rights

California residents may:

1. Know: Request disclosure of collected data categories.
2. Delete: Demand erasure under CCPA exceptions.
3. Opt-Out: Refuse "sale/sharing" of personal info (email request).
4. Limit Sensitive Data Use: Restrict non-essential processing.

Verification required for requests.

Shine the Light: Annual disclosure rights for marketing third parties.

Minors may request public content removal.

Complaints & Contact

Questions/complaints? You can do so by sending an e-mail to us at the email address shown in the app.