Operational Compliance

Data Storage, Logging & Internal Controls

1. Data Storage Documentation

1.1 Cloud Infrastructure

Component	Provider	Service	Region
Primary Database	AWS/GCP	RDS/Cloud SQL	us-east-1 / us-central1
User Photos	AWS/GCP	S3/Cloud Storage	us-east-1 / us-central1
Session Cache	AWS/GCP	ElastiCache/Memorystore	us-east-1 / us-central1
CDN	AWS/Cloudflare	CloudFront/CDN	Global
Compute	AWS/GCP	EC2/Compute Engine	us-east-1 / us-central1

1.2 Region Selection Criteria

Factor	Consideration
User base	Primary user location
Latency	< 100ms to majority users
Compliance	GDPR requires EU option for EU users
Cost	Region pricing differences
Availability	Multi-AZ deployment

1.3 Data Residency Requirements

User Region	Data Storage	Requirement
US	US regions	Default
EU	EU regions	GDPR compliance
California	US (with CCPA compliance)	CCPA/CPRA

---

2. Backup & Recovery Plan

2.1 Backup Strategy

Data Type	Backup Method	Frequency	Retention
Database	Automated snapshots	Daily	30 days
Database	Point-in-time recovery	Continuous	7 days
User photos	Cross-region replication	Real-time	Indefinite
Configuration	Version control (Git)	Per change	Indefinite
Logs	Archive to cold storage	Daily	2 years

2.2 Recovery Time Objectives

Scenario	RTO	RPO	Recovery Method
Database failure	1 hour	5 minutes	Promote replica
Region outage	4 hours	1 hour	Failover to DR region
Data corruption	2 hours	24 hours	Restore from snapshot
Accidental deletion	1 hour	Point-in-time	Point-in-time recovery

2.3 Recovery Testing Schedule

Test Type	Frequency	Last Tested	Next Due
Database restore	Quarterly	-	TBD
Full DR failover	Annually	-	TBD
Backup integrity	Monthly	-	TBD
Data export	Quarterly	-	TBD

2.4 Recovery Procedures

Database Recovery:
1. Identify failure type (corruption, deletion, outage)
2. Select appropriate backup/snapshot
3. Restore to new instance
4. Verify data integrity
5. Update connection strings
6. Validate application functionality

Full DR Failover:
1. Declare disaster
2. Activate DR environment
3. Update DNS/load balancer
4. Verify service restoration
5. Communicate status to users
6. Document incident

---

3. Logging & Monitoring

3.1 Required Log Types

Log Type	Events Captured	Retention	Storage
Authentication	Login success/failure, logout, password changes	1 year	CloudWatch
Match Events	Swipes, matches, unmatches	90 days	Database + Logs

Messages	Send/receive events (not content for privacy)	90 days	Database
Payments	Subscription events, transactions	7 years	Financial system
Admin Actions	All admin panel activity	2 years	Immutable logs
Content Moderation	Flags, reviews, actions taken	2 years	Moderation system

3.2 Authentication Logging

Events to capture:
- ■ Login attempts (success/failure)
- ■ Login location (IP, approximate geo)
- ■ Device information
- ■ Logout events
- ■ Password change/reset
- ■ MFA enrollment/use
- ■ Session invalidation

Log format example:

```
{"timestamp": "2024-12-08T10:30:00Z", "event": "login_success", "user_id": "user_abc123", "ip_address": "192.168.1.1", "device": "iOS 17.0 / iPhone", "session_id": "sess_xyz789", "mfa_used": false}
```

3.3 Match & Engagement Logging

Events to capture:
- ■ Profile view
- ■ Swipe left/right
- ■ Match created
- ■ Match conversation started
- ■ Unmatch

3.4 Payment Logging

Events to capture:
- ■ Subscription started
- ■ Subscription renewed
- ■ Subscription cancelled
- ■ Payment failed

- ■ Refund processed
- ■ Plan changed

3.5 Admin Action Logging

Events to capture:
- ■ Admin login
- ■ User account modification
- ■ User suspension/ban
- ■ Content removal
- ■ Configuration changes
- ■ Data access/export

3.6 Monitoring & Alerting

Metric	Threshold	Alert
Failed logins (per user)	> 5 in 10 min	Security alert
Failed logins (global)	> 100 in 10 min	Attack alert
API error rate	> 5%	On-call page
Database connections	> 80% capacity	Warning
Response time P95	> 2 seconds	Warning
Disk usage	> 80%	Warning

---

4. Internal Controls

4.1 Separation of Duties

Even with a small team, implement these controls:

Action	Required Approvals	Who Can Perform
Production deployment	Code review + approval	Any developer
Database migration	Both founders	Tech lead

User data export	Both founders	Limited access
Financial transactions	Both founders	Finance role
Access grant (production)	Both founders	Admin
Security incident response	One founder	Security lead

4.2 Repository Access Controls

Repository	Access Level	Who
Application code	Read/Write	Development team
Infrastructure code	Read/Write	Ops/DevOps
Secrets/Config	Read only (prod)	Limited
Financial data	No direct access	Via approved tools only

GitHub/GitLab Security:

- ■ 2FA required for all team members
- ■ Branch protection on main/production
- ■ Required reviews before merge
- ■ No force push to protected branches
- ■ Signed commits encouraged

4.3 Code Review Process

Minimum requirements:

- ■ All production changes require PR
- ■ At least one approval required
- ■ CI/CD checks must pass
- ■ No self-approval of PRs
- ■ Security-sensitive changes require senior review

Code Review Checklist:

- ■ Code follows style guide
- ■ No hardcoded secrets
- ■ Input validation present
- ■ Error handling appropriate
- ■ Tests included (where applicable)
- ■ No unnecessary data exposure

- ■ Performance considered

4.4 Access Control List

Document and maintain:

Person	Role	Production Access	Admin Access	Financial Access
[Name]	Co-founder	✓ Full	✓ Full	✓ Full
[Name]	Co-founder	✓ Full	✓ Full	✓ Full
[Name]	Developer	■ Read only	■ None	■ None

Access Review Schedule:
- ■ Monthly access review
- ■ Immediate revocation on departure
- ■ Quarterly unused access cleanup

---

5. Compliance Audit Preparation

5.1 Documentation Requirements

Maintain current versions of:
- ■ System architecture diagram
- ■ Data flow diagram
- ■ Network diagram
- ■ Access control matrix
- ■ Vendor list with DPAs
- ■ Incident log
- ■ Change log

5.2 Evidence Collection

For audits, be prepared to show:
- ■ Log samples demonstrating monitoring
- ■ Backup restoration proof
- ■ Access review records
- ■ Code review history
- ■ Security training records
- ■ Incident response records

5.3 Operational Compliance Checklist

Weekly:
- ■ Review security alerts
- ■ Check backup status
- ■ Review error logs

Monthly:
- ■ Access review
- ■ Security update review
- ■ Backup test (integrity check)

Quarterly:
- ■ Full access audit
- ■ Backup restoration test
- ■ Security training update
- ■ Vendor review

Annually:
- ■ Full compliance review
- ■ Penetration test
- ■ DR test
- ■ Policy updates

Last Updated: December 2024
Review Due: March 2025