1) Was ist rechtlich erforderlich?

- **Verantwortlicher festlegen** (Impressum/Privacy): Name, Kontakt, ggf. **Datenschutzbeauftragte:r** (DPO) benennen, **wenn** Kernaktivität umfangreiche Verarbeitung besonderer Kategorien ist → bei Dating-/Matching-Funktionen praktisch **ja** (Art. 37 DSGVO).
- **Rechtsgrundlagen** (Art. 6 DSGVO):
    - **Vertrag** (Art. 6 (1)(b)): Account anlegen, Matchen, Nachrichten zustellen.
    - **Einwilligung** (Art. 6 (1)(a)) für optionale Features (z. B. Newsletter, Standortfreigabe).
    - **Berechtigtes Interesse** (Art. 6 (1)(f)) eng und dokumentiert für Missbrauchs-/Fraud-Prevention, Security-Logs (Interessenabwägung + Opt-out, wo passend).
- **Besondere Kategorien** (Art. 9 DSGVO – z. B. sexuelle Orientierung):
    - Feld „**Interessiert an Geschlecht**“ **offenbart** i.d.R. die sexuelle Orientierung (hetero/bi/homo) → **nur mit ausdrücklicher Einwilligung** nach Art. 9 (2)(a) (explizit, getrennt, protokolliert, jederzeit widerrufbar).
    - **Fotos** sind personenbezogen; **biometrisch** werden sie erst, wenn du sie **technisch zur eindeutigen Identifizierung** verarbeitest (Face-Recognition etc.) → dann ebenfalls Art. 9 (2)(a) + strenge TOM.
    - **Nachrichteninhalte** können sensible Angaben enthalten → wie besondere Kategorien behandeln.
- **Transparenz** (Art. 13/14): Datenschutz-Hinweise in klarer Sprache (Zwecke, Rechtsgrundlagen, Empfänger, Speicherfristen, Drittlandtransfers, Rechte, DPO-Kontakt).
- **Datenschutz-Folgenabschätzung (DPIA)** (Art. 35): Für eine Matching/„Dating“-Plattform mit Profiling, Messaging und besonderer Kategorie **in der Regel erforderlich**. Ergebnis + Risikomitigation dokumentieren.
- **Verzeichnis von Verarbeitungstätigkeiten** (Art. 30), **Auftragsverarbeitungsverträge** (Art. 28) mit Cloud/Hosting/Analytics, **TTDSG** für Cookies/Tracker.
- **Mindestalter/Elternzustimmung** (Art. 8): In DE i. d. R. **16 Jahre** für Online-Einwilligungen → Age-Gate.
- **Datenübermittlungen in Drittländer**: Nur mit gültiger Grundlage (z. B. EU-US Data Privacy Framework, **oder** SCC + TIA).

2) Welche Datenarten liegen vor & wie schützen?

Datenart	**Beispiele**	**Einstufung**	**Schutz/Fokus**
Identifikatoren	E-Mail, Name, User-ID	personenbezogen	TLS, Verschl. at rest, Zugriff strikt
Kontaktdaten	Telefon	personenbezogen	Verschl., Maskierung im UI/Logs
Adressdaten	Straße, Nr., PLZ, Ort	personenbezogen	Verschl., Need-to-know
Demografie	Geburtsdatum, Gender	personenbezogen (teilweise sensibel in Kontexten)	Minimisierung, Sichtbarkeits-Kontrollen
Sexuelle Orientierung	abgeleitet aus „Interessiert an Geschlecht“	**besondere Kategorie (Art. 9)**	**Explizite Einwilligung**, Pseudonymisierung, starke Zugriffskontrollen
Fotos	Profilfoto	personenbezogen (biometrisch **nur** bei Ident-Verarb.)	Kein Face-Matching ohne Art. 9-Einwilligung; Signierte URLs, CDN-Beschränkung
Kommunikationsdaten	Nachrichten-Text, Timestamps	personenbezogen (kann sensibel sein)	Transport-Verschl., starke Zugriffskontrollen; Lösch-/Export-Funktionen
Beziehungs-/Verhaltensdaten	Likes, Friends, Konversation-IDs	personenbezogen, **Profiling**	Zweckbindung, Minimisierung, Opt-out wo möglich
System-/Sicherheitsdaten	Logs, IP (falls erhoben)	personenbezogen	begrenzte Aufbewahrung, Hash/IP-Trunkierung

3) Technisch-organisatorische Maßnahmen (TOM) – kompakte To-do-Liste

Sicherheit

1. **Verschlüsselung**: TLS 1.2+ in Transit; Datenbanken/Backups **at rest** (AES-256).
2. **Passwörter**: Argon2id/bcrypt, per-User-Salt; MFA für Admins; Secrets in KMS/HSM.
3. **Zugriffssteuerung**: RBAC/ABAC, Least-Privilege, getrennte Prod/Stage, 4-Augen-Prinzip für Datenexports.
4. **Protokollierung & Monitoring**: Audit-Logs (unveränderbar), Anomalie-Erkennung; **kein** Logging sensibler Inhalte.
5. **Trennung & Pseudonymisierung**: sensible Attribute (Orientierung, Nachrichten) in separaten Schemas/Secrets, wo möglich Pseudonym-IDs.
6. **Backups**: verschlüsselt, getrennter Storage, Restore-Tests.

7. **Sichere Entwicklungspraktiken**: SAST/DAST, Dependency-Scanning, SBOM, Secrets-Scanning.

Produkt/UX
8. **Einwilligungs-Flows**: Layered Consent; **explizit** (Opt-in) für „Interessiert an Geschlecht“ und biometrische Verarbeitungen; Protokoll & Widerruf im Konto.
9. **Privacy by default**: Profile standardmäßig **nicht** öffentlich; Sichtbarkeit einzelner Felder steuerbar.
10. **Rechte der Betroffenen**: Self-Service für Auskunft, Berichtigung, **Löschung**, Portabilität; Lösch-Button für Nachrichten/Account.
11. **Aufbewahrung**: klare Retentions (z. B. „Likes pending“ 90 Tage; inaktive Accounts 24 Monate → Anonymisierung/Löschung; Logs 30–90 Tage, wo möglich).
12. **Altersprüfung**: 16+; unter 16 nur mit nachweisbarer Elternzustimmung.

Organisation/Vendor
13. **DPIA** durchführen (Risiken: Re-Identifikation, Datenabfluss aus Nachrichten/Fotos, Profiling) und Maßnahmen festlegen.
14. **AV-Verträge** mit allen Auftragsverarbeitern; Sub-Prozessor-Liste pflegen; Transfer-Folgenabschätzung (TIA) bei Drittländern.
15. **Incident-Response**: Data-Breach-Plan (72-Stunden-Meldung an Aufsicht, Benachrichtigung Betroffener bei hohem Risiko), Table-Top-Übungen.
16. **Awareness & Prozesse**: Schulungen, Berechtigungsaudits, Joiner-Mover-Leaver-Prozess.

4) Minimaler Lösch- & Aufbewahrungsplan (Beispiel)

- **Accountdaten**: bis Konto-Löschung + gesetzliche Fristen (Nachweise max. 3 Jahre).
- **Nachrichten**: nutzerseitig löschbar; serverseitig z. B. **Rolling 24 Monate**, danach anonymisieren/löschen.
- **Likes/Friendships (pending)**: z. B. 90 Tage → Auto-Expire.
- **Backups**: definierter Zyklus (z. B. 30/60/90 Tage), danach sichere Vernichtung.
- **Logs**: 30–90 Tage, stark minimiert.

5) Einwilligungstexte – worauf achten (Kurz)

- **Getrennt & granular**: „Profiling/Matching“ ≠ „Newsletter“ ≠ „bes. Kategorien“.
- **Explizit** (Art. 9): Checkbox + klare Formulierung für „Interessiert an Geschlecht“ als Offenbarung der sexuellen Orientierung; Protokollierung (Zeit, Inhalt, Nutzer-ID).
- **Widerruf** ohne Nachteile; UI-Schalter; dokumentierte Wirkung (Daten ggf. löschen/anonymisieren).

Wenn du willst, formuliere ich dir daraus direkt:

- eine **Privacy-Notice** (Art. 13) für deine App/Website,
- eine **DPIA-Gliederung** mit konkreten Risikoszenarien,
- und eine **TOM-Liste** passend zu deiner Architektur (Cloud/On-Prem).