educage.

SCOPE EU • UK • India

FORMAT Practical checklist, 3 pages

GDPR vs DPDPA

Practical Compliance Checklist

EU GDPR • UK GDPR • India's DPDPA

A practical comparison for organisations operating across multiple jurisdictions - built for CEOs, compliance managers, DPOs and legal teams who need the essentials without reading two acts and a set of rules.

EU GDPR | UK GDPR | VS | DPDPA (INDIA)

WHY THIS MATTERS

Similar principles. Very different obligations.

The GDPR and India's DPDPA pursue the same goal - protecting personal data -but differ in scope, consent design, individual rights, transfer rules and penalties. This checklist distils the practical differences your organisation needs to act on, jurisdiction by jurisdiction.

PRACTICAL CHECKLIST

Where GDPR and DPDPA pull apart

While the GDPR and India's DPDPA share many common privacy principles, they introduce different legal obligations and compliance requirements. Use this checklist as a quick reference when working across both jurisdictions - 25 practical differences, grouped into five areas.

A · SCOPE & DEFINITIONS

1 Scope

- [ ] Are we processing digital data only, or also structured paper records?

KD: DPDPA covers digital (or digitised) data only; GDPR covers digital and paper filing systems.

2 Territorial scope

- [ ] Do we offer goods/services to, or monitor, individuals in the EU/UK or India?

KD: Both reach outside their borders - GDPR via targeting/ monitoring, DPDPA via offering goods or services in India.

3 Publicly available data

- [ ] Have we mapped which "public" data qualifies for an exemption?

KD: DPDPA broadly exempts publicly available data; GDPR keeps such data fully in scope.

4 Key terminology

- [ ] Do our policies use the right defined terms for each law?

KD: Data Subject/Controller (GDPR) = Data Principal/Data Fiduciary (DPDPA) - "fiduciary" signals a stronger duty of care.

B · LEGAL BASIS & CONSENT

5 Legal bases

- [ ] Is every processing activity mapped to a valid basis under both laws?

KD: GDPR has six legal bases; DPDPA relies mainly on consent plus a closed "certain legitimate uses" list.

6 Legitimate interest

- [ ] Are we currently relying on legitimate interests anywhere?

KD: GDPR allows a standalone, balancing-test basis; DPDPA has no general legitimate-interest equivalent.

7 Consent

- [ ] Is consent free, specific, informed and given by clear affirmative action?

KD: Both require affirmative, specific consent; DPDPA also requires it be "unconditional" and use-limited.

8 Consent withdrawal

- [ ] Can individuals withdraw consent as easily as they gave it?

KD: Same principle in both - easy withdrawal, no effect on prior lawful processing.

9 Consent Managers

- [ ] Are we ready to interact with India's registered Consent Managers?

KD: DPDPA creates a regulated Consent Manager role; GDPR has no equivalent.

10 Children's data

- [ ] What age threshold applies in each jurisdiction we operate in?

KD: DPDPA sets 18, uniform. EU GDPR ranges 13–16 by Member State; UK GDPR generally uses 13.

11 Sensitive personal data

- [ ] Have we flagged all GDPR special-category data (Art. 9)?

KD: GDPR has a separate, stricter regime; DPDPA treats all personal data uniformly.

12 Privacy notices

- [ ] Do our notices meet each law's information requirements?

KD: GDPR requires detailed itemised notices (Arts. 13–14); DPDPA uses a simpler, purpose-focused notice.

C · RIGHTS & COMPLAINTS

13 Individual rights

- [ ] Do we support portability, restriction, objection and automated-decision rights?

KD: GDPR grants these as standalone rights; DPDPA does not name them separately.

14 Complaints

- [ ] Is our complaints process mapped to the right regulator?

KD: Both allow complaints to the authority, but DPDPA requires exhausting internal grievance first.

D · OBLIGATIONS OF THE CONTROLLER / FIDUCIARY

15 Accountability

- [ ] Can we demonstrate compliance on request, not just claim it?

KD: GDPR names accountability as an explicit principle; DPDPA achieves similar aims via general duties.

16 Privacy by Design

- [ ] Is privacy embedded by default when we build new systems?

KD: GDPR makes this an explicit obligation (Art. 25); DPDPA requires only "appropriate" measures.

17 Processor contracts

- [ ] Do our processor contracts meet GDPR's detailed content rules?

KD: GDPR prescribes detailed contract content (Art. 28); DPDPA requires a valid contract, less detail.

18 Records of processing

- [ ] Do we maintain a Records of Processing Activities (RoPA)?

KD: GDPR generally requires a RoPA; DPDPA has no comparable general obligation.

19 DPIA

- [ ] Have we assessed our Data Protection Impact Assessment duties?

KD: GDPR requires DPIAs broadly for high-risk processing; DPDPA only for Significant Data Fiduciaries.

20 Data Protection Officer

- [ ] Is our DPO appointed and correctly based?

KD: GDPR requires a DPO in defined cases; DPDPA only for Significant Data Fiduciaries, based in India.

21 Personal data breaches

- [ ] Can we meet each law's breach notification timeline?

KD: GDPR: 72 hours, risk-based threshold. DPDPA: broader duty, no comparable materiality threshold.

22 Data retention

- [ ] Do we erase data automatically once its purpose ends?

KD: Both apply storage limitation; DPDPA adds an express erasure duty on withdrawal or inactivity.

E · TRANSFERS & ENFORCEMENT

23 International transfers

- [ ] Do we rely on adequacy decisions, SCCs or a listed derogation?

KD: GDPR is prohibition-based; DPDPA is permissive by default unless India restricts a destination.

24 Supervisory authority

- [ ] Do we know who regulates us in each jurisdiction?

KD: EU: national DPAs + EDPB. UK: the ICO. India: the Data Protection Board of India.

25 Penalties

- [ ] Have we modelled our worst-case exposure under each law?

KD: GDPR fines scale with turnover (up to €20m/4%); DPDPA sets fixed statutory penalties per violation.

SAVE THIS PAGE

Summary at a glance

The full picture in one table. Keep this page open in a meeting, or pin it to your compliance wiki.

TOPIC	EU GDPR	UK GDPR	INDIA'S DPDPA
Scope	Digital + structured paper records	Digital + structured paper records	Digital / digitised data only
Territorial reach	Extraterritorial - targets/monitors EU individuals	Extraterritorial - targets/monitors UK individuals	Extraterritorial - offers goods/services in India
Key terms	Data Subject, Controller, Processor	Data Subject, Controller, Processor	Data Principal, Data Fiduciary, Data Processor
Legal bases	Six bases incl. legitimate interests	Six bases incl. legitimate interests	Consent + closed "legitimate uses" list
Consent Managers	No equivalent role	No equivalent role	Registered, licensed Consent Managers
Children's age	13–16, set by Member State	13 (online services)	18, uniform
Sensitive data	Separate special-category regime (Art. 9)	Separate special-category regime (Art. 9)	No separate category - treated uniformly
Individual rights	Access, rectification, erasure, portability, restriction, objection, automated-decision protection	Same as EU GDPR	Access, rectification, erasure - no standalone portability, restriction or objection rights
Records of processing	Generally required (Art. 30)	Generally required (Art. 30)	No comparable general obligation
DPIA	Required for high-risk processing	Required for high-risk processing	Required only for Significant Data Fiduciaries
DPO	Required for public bodies, large-scale monitoring or special-category processing	Same as EU GDPR	Required for Significant Data Fiduciaries; must be based in India
Breach notice	Authority within 72h, risk-based threshold	Authority within 72h, risk-based threshold	Broader notice duty; no comparable threshold
Retention	Storage-limitation principle	Storage-limitation principle	Express erasure duty on withdrawal / inactivity
International transfers	Prohibition-based: adequacy, SCCs or derogation	Prohibition-based: UK adequacy or safeguards	Permissive by default; government restricted-list
Supervisory authority	National DPAs + EDPB	Information Commissioner's Office (ICO)	Data Protection Board of India
Maximum penalty	Up to €20m or 4% global turnover	Up to £17.5m or 4% global turnover	Fixed statutory penalties per violation, up to ~₹250 crore

Source: GDPR (EU) 2016/679 · UK GDPR / Data Protection Act 2018 · DPDPA 2023 + DPDP Rules 2025

💡 Practical Tip

Run every cross-border data flow through both columns before you rely on a single global privacy policy.

⚠ Key Difference

DPDPA has no legitimate-interest basis - consent-first design is not optional in India.

✓ Good Practice

Maintain one master RoPA, then tag each entry with its DPDPA "Significant Data Fiduciary" status.

educage.training · info@educage.training