INDUCTUS

GDPR *meets* DPDP

The Compliance Convergence That Changes
EU–India GCC Economics

EXECUTIVE Summary

As reflected in the latest November 2025 regulatory and government communications, the operationalization of **India's Digital Personal Data Protection (DPDP) Act** marks a significant inflection point in global data governance and cross-border compliance frameworks. With **179 of 240 jurisdictions now possessing enforceable data protection frameworks**, organizations operating across EU-India corridors face dual compliance obligations that are increasingly aligned in principle yet divergent in execution. This convergence fundamentally restructures the business case for Global Capability Centers (GCCs) while introducing material compliance risk without coordinated implementation.

Regulatory Landscape

Dimension	GDPR	DPDP Act & Rules 2025
Effective Date	May 2018 (enforced)	May 2027 (phased implementation from Nov 2025)
Jurisdictional Reach	Extraterritorial (targeting criterion)	India-focused with cross-border provisions
Enforcement Fines	€7.1B+ cumulative (60% issued since 2023)	Up to ₹250 Crore (~USD 29M) per contravention
Key Mechanism	SCCs, adequacy decisions, BCRs	Consent-led, fiduciary accountability

Key Convergence Points

Both frameworks mandate privacy-by-design architecture, accountability-first governance structures, and rights-centric processing. Organizations can design a unified compliance infrastructure leveraging the following:

Shared privacy architecture

GDPR Article 25 and DPDP design requirements achieve functional equivalence through granular consent, data minimization, and purpose-linked retention.

Accountability structures

DPO (GDPR) and Grievance Redressal Officer (DPDP) roles align organizational responsibility within identifiable functions.

Processor safeguards

Article 28 (GDPR) and Rule 6 (DPDP) establish similar controller-processor contractual frameworks.

CRITICAL COMPLIANCE GAPS

Government access provisions

DPDP Section 17(2) permits broad exemptions without proportionality review, failing the **Schrems II standard** for adequacy determination.

Supervisory independence

The Data Protection Board lacks structural independence; members are government-appointed without security of tenure.

Special-category data

GDPR extends heightened protections to **health, genetic, and biometric data**; DPDP treats all personal data uniformly.

Transfer mechanisms

GDPR requires Chapter V safeguards (SCCs/adequacy); DPDP permits unrestricted transfers absent specific government notification.

Legitimate interests basis

GDPR permits processing on legitimate interests; DPDP mandates consent in most scenarios.

The regulatory convergence creates unprecedented GCC opportunities while introducing corresponding complexity. Organizations that implement integrated dual-compliance architectures will gain a competitive advantage; those treating the regimes as separate will face unacceptable compliance risk and operational cost. The India–EU adequacy pathway remains uncertain; organizations must design for SCC dependency through at least 2028.

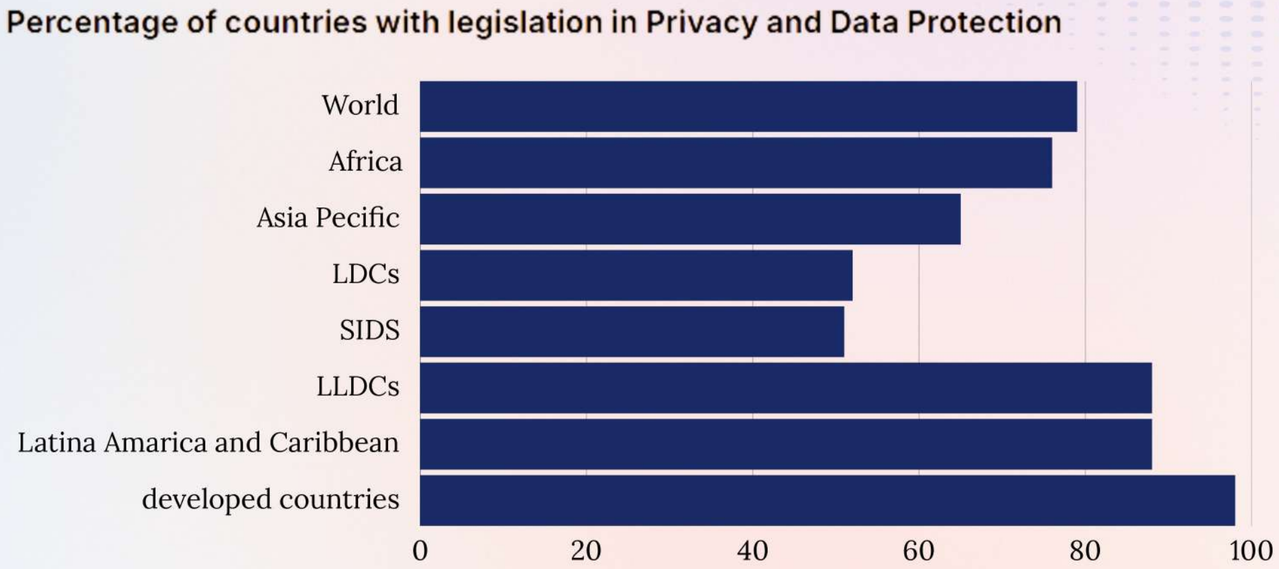
TABLE OF CONTENTS

The Global Data Privacy Inflection Point

Global data governance has shifted from fragmented, sector-specific regulation to comprehensive, rights-based privacy regimes. As of 2026, 179 of the 240 analyzed jurisdictions have data protection frameworks in place, while another eight are considering draft laws. This means approximately 3 out of every 4 countries are covered by data protection laws, with **UNCTAD estimating that over 75% of the global population is now covered under modern data protection frameworks** grounded in individual rights, accountability, and cross-border transfer controls. (

The year 2025 marks a structural shift in global data governance. India's notification of the Digital Personal Data Protection Rules on 13 November 2025 operationalizes the **Digital Personal Data Protection Act 2023 (DPDPA)** and establishes a complete, enforceable framework for personal data processing. With this step, India joins the **European Union's General Data Protection Regulation (GDPR)** and **China's Personal Information Protection Law (PIPL)** as a jurisdiction whose data protection requirements carry direct implications for multinational operating models.

The rules convert statutory provisions into defined obligations, including consent management, notice requirements, breach reporting, and the designation of significant data fiduciaries. This expansion reflects a structural convergence in regulatory design rather than formal global harmonization. Despite jurisdictional differences, **core compliance expectations, lawful basis, purpose limitation, data minimization, security safeguards, and enforceable data subject rights** are increasingly consistent across major economies.



1.1 The Rise of Rights-Based Data Legislation Worldwide

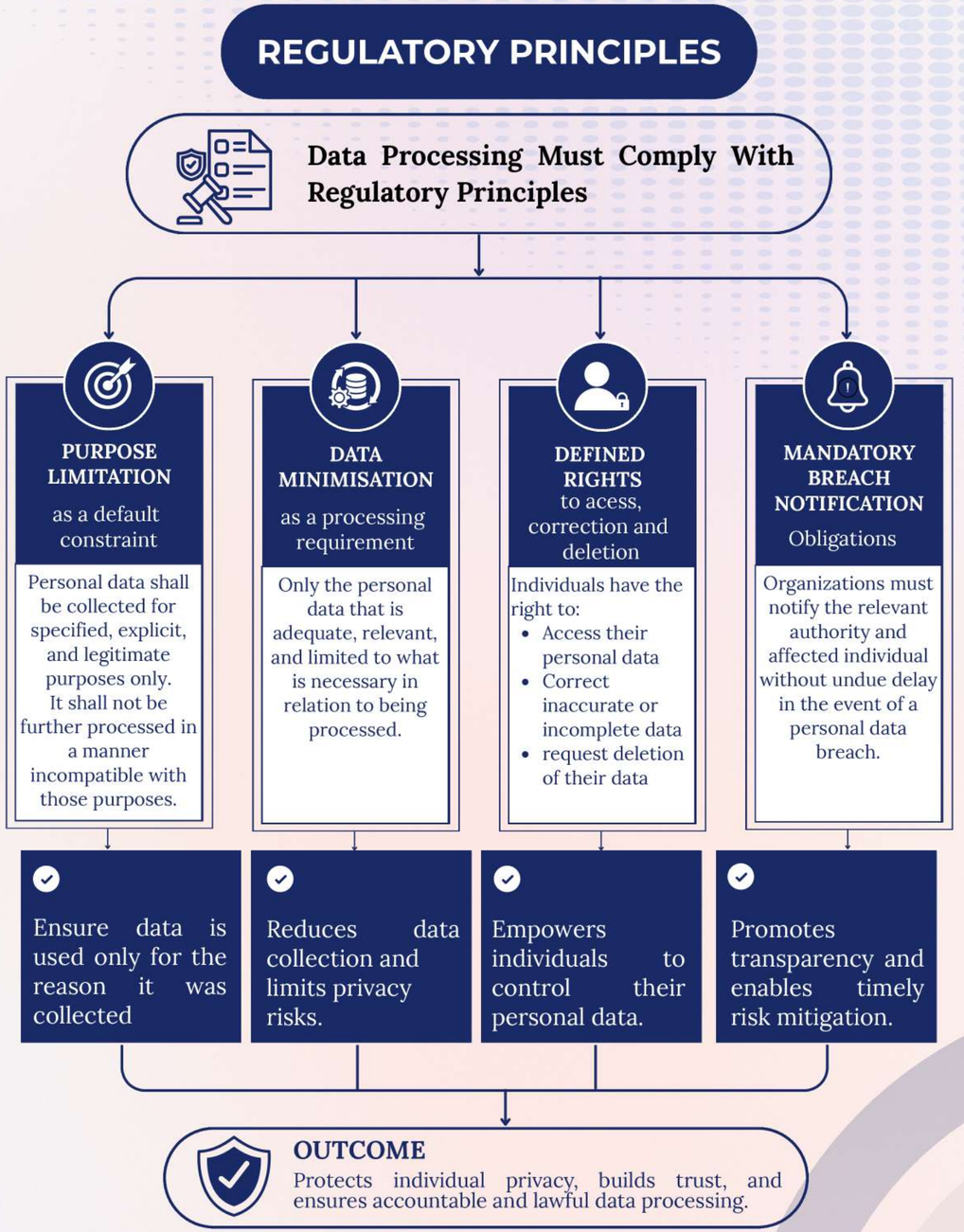
Rights-based data protection frameworks have become the dominant global regulatory model, replacing earlier notice-and-consent or sector-specific approaches.

Key structural indicators:

- Countries are increasingly framing data laws around individual rights over personal data rather than just corporate compliance.
- The core idea behind this is that people should control how their data is collected, used, shared, and deleted.
- Rapid regulatory development is concentrated in Asia-Pacific, Latin America, and North America, driven by digital economy expansion and cross-border data flows.

The General Data Protection Regulation (GDPR) continues to function as the reference architecture for modern privacy regimes due to its **enforcement maturity and extraterritorial reach.** At the same time, newer frameworks, including India's Digital Personal Data Protection (DPDP) Act, 2023, and multiple U.S. state-level privacy laws (e.g., California, Virginia, and Colorado), reflect functional convergence in regulatory principles.

This has resulted in the **de facto alignment of compliance obligations** across jurisdictions without formal treaty-based harmonization.



1.2 Why Do GDPR and DPDP Sit at the Center of Multinational Strategy?

The EU's GDPR and India's DPDP Act represent two structurally influential regulatory models shaping global enterprise data architecture.

GDPR	DPDP
Enforced since 2018 across 27 EU member states and EEA (European Economic Area) jurisdictions	Enacted in 2023, with a phased implementation framework, it will finally come into effect on 12 May 2027.
Covers both domestic and extraterritorial processing where EU data subjects are involved	Designed for digital-scale compliance with simplified obligations relative to GDPR
Total administrative fines issued since 2018 exceed €4 billion cumulatively	Introduces consent-centric processing architecture, supported by notice, purpose limitation, and data principal rights
Established a mature enforcement ecosystem via national Data Protection Authorities and the European Data Protection Board (EDPB)	Emphasises operational scalability for high-volume digital systems (cloud, platforms, AI ecosystems)

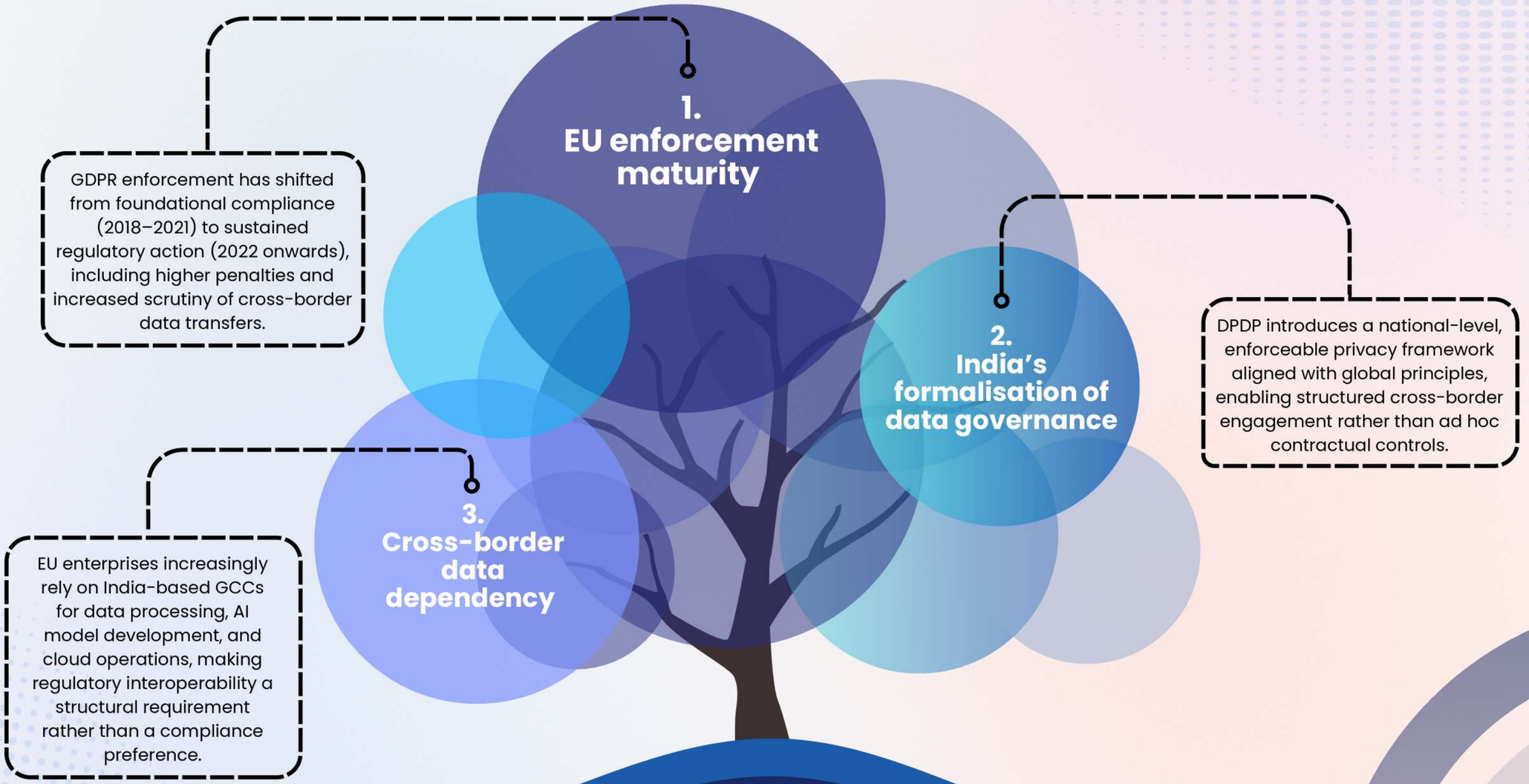
For multinational enterprises and Global Capability Centers (GCCs) or Offshore Development Centers (ODCs), GDPR and DPDP now form dual baseline compliance layers:

- **GDPR defines governance depth, auditability, and cross-border transfer discipline.**
- **DPDP enables scalable deployment within high-growth digital markets and centralized processing hubs.**

As a result, enterprise data architectures are increasingly designed for "dual compliance compatibility," particularly in shared services, analytics, and AI training environments operating across EU–India corridors.

1.3 The India–EU Regulatory Moment

Three structural factors define the India–EU regulatory alignment moment:



GDPR - Architecture, Enforcement & Global Reach

2.1 Origins, Legal Basis & Jurisdictional Scope

The **General Data Protection Regulation (Regulation (EU) 2016/679)** was adopted by the European Parliament and the Council of the European Union on **14 April 2016** and became enforceable across **all EU Member States on 25 May 2018**. Unlike its predecessor, which required national transposition, the GDPR is directly applicable across all EU Member States, creating a uniform legal framework for personal data protection. Its structure is built on directly applicable provisions, eliminating the need for national transposition while allowing limited member-state derogations in defined areas such as employment data and public interest processing.

Jurisdictional scope is defined in Article 3 and extends beyond territorial boundaries:

Criterion	Applicability	Key Explanation
Establishment Criterion	EU-based controllers and processors	Applies where an entity is established within the European Union, irrespective of whether the actual data processing takes place within or outside the EU.
Targeting Criterion	Non-EU entities	This applies to organizations outside the EU that offer goods or services to individuals located in the EU, or that monitor their behavior within the Union.
Public International Law	Special jurisdictional locations	Applies to processing activities carried out in locations where Member State law applies by virtue of public international law, such as embassies and diplomatic missions.

This extraterritorial reach has resulted in non-EU companies aligning internal data governance structures with EU standards, particularly in sectors involving digital services, financial systems, and cross-border data processing.

2.2 Core Principles: Lawfulness, Purpose Limitation & Data Minimisation

GDPR establishes principles under Article 5; three form the operational core for compliance design:

1. Lawfulness, Fairness, and Transparency:

Processing must rely on one of six lawful bases (Article 6), including consent, contract, legal obligation, vital interests, public task, or legitimate interests.

- Consent must be freely given, specific, informed, and unambiguous.
- Transparency obligations require clear disclosures on processing purposes, retention, and rights.

2. Purpose Limitation:

Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

- Secondary processing requires a compatibility assessment or renewed legal basis.
- Derogations exist for archiving, research, and statistical purposes under safeguards

3. Data Minimization:

Processing must be adequate, relevant, and limited to what is necessary for the intended purpose.

- Drives architectural decisions such as data field reduction, anonymization, and retention controls.
- Increasingly enforced through audits of system design and data lifecycle management.

These principles are operationalized through accountability requirements (Article 24), mandating demonstrable compliance via documentation, policies, and technical controls.

2.3 Cross-Border Transfer Mechanisms: Adequacy, SCCs & BCRs

Cross-border data transfers under GDPR (Chapter V, Articles 44–49) are a distinct compliance obligation. Any transfer outside the EEA must preserve the level of protection guaranteed within the EU, with full accountability placed on the data exporter.

Adequacy Decisions (Article 45)

Article 45 allows transfers to jurisdictions deemed "adequate" by the European Commission, meaning their legal frameworks provide sufficient protection. An adequacy decision is the most operationally straightforward transfer mechanism: it eliminates the need for additional contractual or technical safeguards, and data flows to the adequate country proceed on the same basis as intra-EEA transfers. (Source: Cybersecurity attorney)

- Enables data flows without additional safeguards; operationally closest to intra-EEA transfers.
- As of 2025, adequacy covers jurisdictions including Japan, South Korea, the UK, Switzerland, and the EU–US Data Privacy Framework (DPF, 2023).
- The DPF operates via self-certification and redress mechanisms under U.S. Executive Order 14086; legal challenges remain ongoing.

Standard Contractual Clauses (SCCs) (Article 46)

SCCs are the primary transfer mechanism for non-adequate jurisdictions. Updated in June 2021, the new SCCs include four modules covering different controller-processor and controller-controller combinations, and all four modules impose obligations on both the data exporter and the data importer.

Post-Schrems II (2020) requirements:

- **Mandatory Transfer Impact Assessments (TIAs)** evaluating the enforceability of SCCs in the recipient country
- Implementation of supplementary measures where required:
  - Technical: encryption, pseudonymization
  - Contractual obligations on government access transparency
  - Organisational: access controls, policy enforcement

Binding Corporate Rules (BCRs) (Article 47)

Binding Corporate Rules (BCRs) are data protection policies approved by a lead EU supervisory authority that govern intra-group transfers of personal data across borders for multinational organizations. Unlike SCCs, which are bilateral contractual arrangements, BCRs establish a group-wide legal framework that all entities in the corporate group are bound by, and they are directly enforceable against the group's EU entity.

- Legally binding across all group entities; enforceable by EU data subjects
- Approval timelines are typically 18–36 months, with high documentation thresholds
- Suitable for large multinational groups with stable, high-volume internal data flows

Trade-off:

- Higher upfront cost and regulatory engagement
- Lower marginal compliance burden once operational

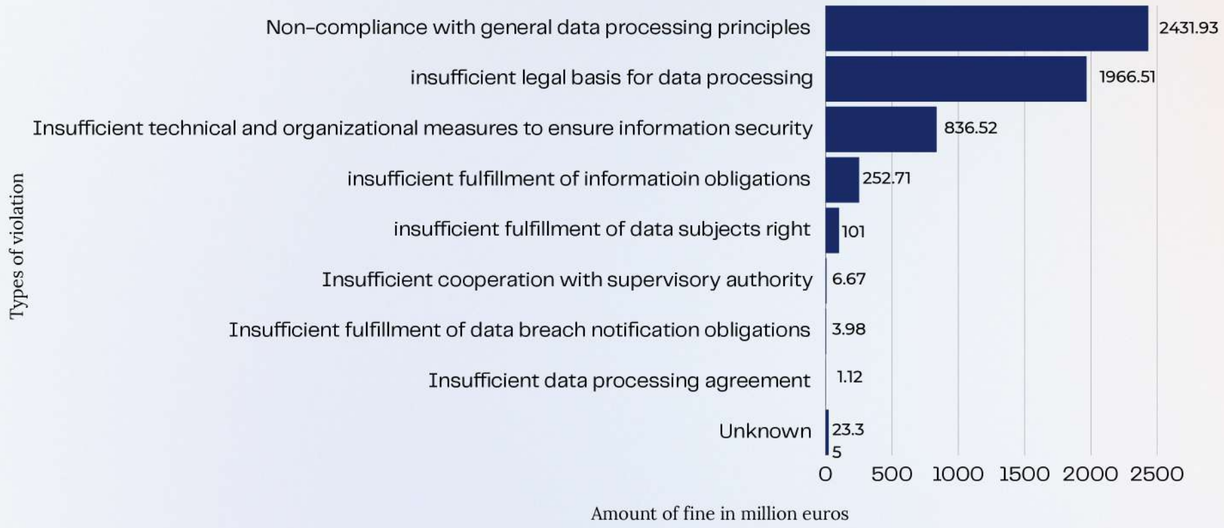
Operational Positioning

- SCCs remain the default mechanism for EU-India data flows
- Adequacy provides the lowest-friction model, but is unavailable for India
- BCRs offer structural certainty for scaled GCC operations with sustained EU data exposure

2.4 GDPR Enforcement Record: Key Fines & Precedents (2018–2025)

As of 1 March 2025, 2,245 GDPR enforcement actions had been recorded, with cumulative fines of approximately €5.65 billion. **By January 2026, total penalties exceeded €7.1 billion,** including €1.2 billion imposed during 2025, with over 60% of aggregate fines issued since January 2023, indicating a concentration of enforcement in recent years.

Largest fines issued for General Data Protection Regulation (GDPR) violations as of February 2025, by type of violation (in million euros)



Landmark enforcement decisions: The table below summarizes the most consequential enforcement actions from 2018 to 2025, selected on the basis of financial magnitude, doctrinal significance, or sectoral precedent.

Entity	DPA	Year	Fine	Primary Violation
Meta Platforms Ireland	Irish DPC	2023	€1.2 billion	Article 46(1): Transfer of EU user data to the U.S. without adequate safeguards
Amazon Europe	Luxembourg CNPD	2021	€746 million	Article 5: Non-compliance with general data processing principles
TikTok	Irish DPC	2025	€530 million	Article 46(1): Transfer of EEA user data to China; Article 13(1) (f); Transparency failures
Meta / Instagram	Irish DPC	2023	€405 million	Articles 5, 6, 12, 13: Processing of children's data, legal basis deficiencies
LinkedIn Ireland	Irish DPC	2024	€310 million	Articles 5, 6, 13, 14: Unlawful processing for behavioural targeting, invalid legal bases
Uber	Dutch AP	2024	€290 million	Article 46(1): Transfer of EU driver data to the U.S. without adequate safeguards
Meta	Irish DPC	2022	€265 million	Article 25, 32: Data breach exposing 533 million Facebook users
WhatsApp	Irish DPC	2021	€225 million	Articles 12, 13, 14: Transparency failures regarding inter-company data sharing
Google LLC	French CNIL	2022	€150 million	ePrivacy / GDPR: Cookie consent mechanism violations
Meta	Irish DPC	2024	€251 million	Articles 25, 32: Security breach affecting 29 million users globally

India's DPDP Act 2023 & DPDP Rules 2025 - A Complete Anatomy

India's Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a **consent-led, fiduciary-based framework governing the processing of digital personal data.** The Digital Personal Data Protection Rules, 2025 (notified on 13 November 2025) operationalize the Act through **detailed prescriptions on consent architecture, breach notification, grievance handling, and obligations of Significant Data Fiduciaries.** Together, the Act and rules define the legal and operational baseline for all entities processing digital personal data in India or in connection with offering goods or services to individuals in India.

3.1 DPDP Rules 2025 - Notified 13 November 2025: What Changed

The Digital Personal Data Protection Rules, 2025, provide full effect to the DPDP Act, 2023, by setting out a defined framework for the processing of personal data. They establish requirements for lawful processing, consent management, notice, data security, breach reporting, and grievance redressal.

The Rules specify **obligations for data fiduciaries and processors, including conditions for cross-border data transfers and additional requirements for entities designated as significant data fiduciaries.** They also set out the operational structure for enforcement, including the role of the Data Protection Board.

Phased Implementation Framework

- The rules provide for phased implementation over eighteen months. During this period, organizations are required to align internal systems and processes with statutory requirements.
- Each Data Fiduciary must issue a standalone consent notice in clear and plain language, specifying the purpose of data collection and use. Consent Managers are required to be entities incorporated in India.

Breach Notification Procedures

- The rules prescribe a defined process for personal data breach notification. Upon becoming aware of a breach, the data fiduciary must notify affected individuals without undue delay.
- The notification must describe the nature of the breach, its potential impact, and remedial actions taken, and provide contact details for further assistance.

Transparency and Accountability Requirements

- Entities designated as significant data fiduciaries are subject to additional obligations, including independent audits, data protection impact assessments, and specific due diligence requirements when deploying certain technologies.
- The Rules also provide for compliance with government directions in respect of notified categories of data, including conditions relating to storage.

Enhancement of Data Principal Rights

- The Rules restate and operationalize the rights of data principals. Individuals may seek access to their personal data, request correction or updating, and require erasure in specified circumstances.
- They may nominate another individual to exercise these rights. Data fiduciaries are required to respond to such requests within a period of ninety days.

Digital-First Data Protection Board

- The rules establish a Digital Data Protection Board of India comprising four members. Complaints may be filed and tracked through an online portal and mobile application.
- Orders of the Board are appealable to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

3.2 DPDP 2025 - Operational Flow

PHASED IMPLEMENTATION
(18 MONTHS)
The organization aligned systems and processes with the rules

CONSENT FRAMEWORK

- Separate, clear consent notice
- Purpose - Specific data use
- Consent manager must be India-based entities

DATA PROCESSING BEGINS

IF DATA BREACH OCCURS

Organizing alignment systems and processes with the rules

- Identify breach → Notify affected individuals without delay → Include the follwing in the notifications:
  - Nature of breach
  - Potential Impact
  - Remedial action
  - Contact deatils

ONGOING COMPLIANCE REQUIREMENTS

TRANSPARENCY MEASURES

- Public contact details for data-related queries and grievances

IF SIGNIFICANT DATA FIDUCIARY

- Conduct independent audits
- Perform impact assessments
- Apply enhanced due diligence for certain technologies
- follow goverment direction on restricted categories of data, including local storage requirements

ENHANCEMENT OF DATA PRINCIPAL RIGHTS

- Access personal data
- Correct / update data
- Request erasure
- Nominate representative

REPONSE TIME
Data Fiduciary to respond within 90 days

GRIEVANCE REDRESSAL FRAMEWORK

File complaint (Online portal/ mobile app) → Reviewed by data protection Board of india → Decision issued by the Board → If an appeal is required → Escalation to TDSAT (Appellate Tribunal)

The DPDP Rules, 2025, establish clear obligations for individual rights and ensure accountability through a transparent and technology-enabled framework.

3.3 Phased Implementation Timeline: November 2025 → May 2027

DPDP Acts & Rules - Phased Implementation Roadmap

A calibrated, time-bound approach to oprationalise data protection across india's digital ecosystem

PHASES AND TIME	KEY ACTIVITIES	REGULATORY FOCUS	EXPECTED OUTCOME
PHASE I November 2025 (Notification Stage)	• Rules notified on 13 November 2025 • Initiation of institutional setup, including the data protection Board • Publication of compliance requirements for fiduciaries and processors	Establish an institutional framework and set the foundation for compliance readiness	A foundation for regulatory framework and institutional infrastructure was established.
PHASE II 2026 (Core Compliance Activation)	• Enforcement of consent, notice, and grievance mechanisms • Activation of breach notification obligations • Initial compliance requirements for data fiduciaries	Operationalise core data protection obligations for all data fiduciaries	Core compliance obligations become operational for all data fiduciaries
PHASE III 2026-2027 (Enhanced Obligations)	• Designation and compliance requirements for significant data fiduciaries • Enforcement of DPIA and audit requirements • Scaling of enforcement activity by the Data Protection Board	Strengthen oversight for higher-risk entities and embed accountability through audits and assessments.	Enchanced obligations enforced for higher-risk entities, regulatory oversight scaled.
PHASE IV May 2027 (Full Operationalisation)	• Full enforcement across all provisions • Stabilisation of regulatory processes • Consistent application of penalties and adjudication mechanisms	Ensure full operation of the act and consistency.	End to end oprationalisation of the DPDP act & Rules with consistent enforcement

This phased approach reflects the scale of transition required across India's digital ecosystem, which includes over 850 million interest users (IAMAI 2024) .

3.4 Penalty Regime: Up to ₹250 Crore (~USD 29 Million)

The DPDP Act establishes a civil penalty regime administered by the Data Protection Board of India under Section 33, read with the Schedule, with monetary penalties linked to specified contraventions and subject to statutory caps. The DPDP Rules, 2025, prescribe procedures for breach notification and complaint handling, which may be considered by the Board during adjudication.

Contravention	Statutory Provision	Maximum Penalty
Failure to implement reasonable security safeguards resulting in a personal data breach	Section 8(5)	Up to ₹250 crore
Failure to notify the Board and affected Data Principals of a personal data breach	Section 8(6)	Up to ₹200 crore
Non-fulfilment of obligations relating to children's data (including age-gating and parental consent where applicable)	Section 9	Up to ₹200 crore
Failure to comply with additional obligations of Significant Data Fiduciaries (including DPIA and audits)	Section 10	Up to ₹150 crore
Failure to comply with duties relating to accuracy, retention, and purpose limitation	Section 8	Up to ₹50–₹100 crore (depending on the nature of contravention)
Failure to provide information or comply with directions issued by the Data Protection Board	Section 33	Up to ₹50 crore

Determination Criteria for Penalty Quantum

Section 33 requires the Board to determine penalties based on defined statutory factors. These include:

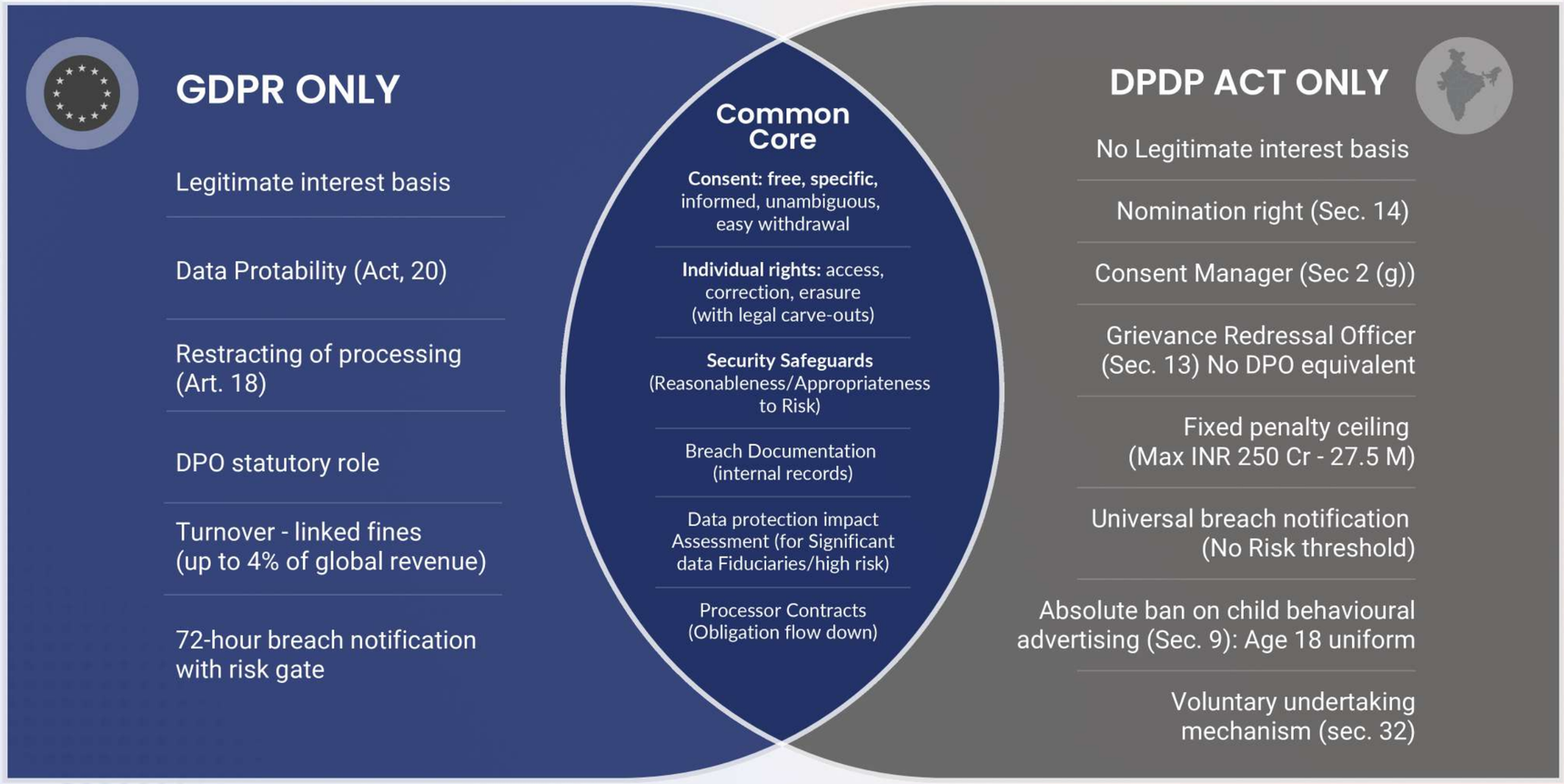
- **Nature, gravity, and duration of the breach:** The scale of impact, duration of exposure, and continuity of non-compliance are considered. Persistent or systemic failures attract higher penalties.
- **Type and volume of personal data affected:** Incidents involving sensitive categories of data or large-scale datasets are treated with higher severity.
- **Repetitive nature of contraventions:** Prior instances of non-compliance, including warnings or directions issued by the board, are considered in escalation.
- **Mitigation measures undertaken:** Timeliness and adequacy of remedial actions, including breach containment and notification, influence penalty outcomes.
- **Gain or avoidance of loss:** Any demonstrable economic benefit derived from non-compliance may be factored into the penalty determination.

This structured approach aligns penalty assessment with observable compliance behavior rather than abstract thresholds.

GDPR vs. DPDP - A Comparative Compliance Matrix

The GDPR and India's Digital Personal Data Protection Act, 2023 (DPDP Act) share a common normative origin, the treatment of personal data protection as an individual right rather than a regulatory permission. Beyond that shared foundation, the two regimes diverge substantially in legal architecture, enforcement design, and operational obligations.

For organizations operating across both jurisdictions, the differences are not academic. They determine what compliance infrastructure must be built, where duplication is possible, and where two distinct systems are unavoidable.



The Convergence Thesis: Where GDPR and DPDP Align Strategically

India's Digital Personal Data Protection Act, 2023 (DPDP Act), notified in August 2023 and operationalized by the Digital Personal Data Protection Rules, 2025 (notified 13 November 2025) on a phased implementation basis, draws from the same normative tradition as the GDPR; both regimes treat personal data protection as an individual right.

The shared rights basis defines the structural direction of both regimes: data protection obligations flow from the right of the individual, and organizations are accountable stewards rather than proprietors of the data they process.

5.1 Privacy-by-Design as a Shared Mandate

Article 25 of the GDPR imposes a binding obligation on data controllers to integrate data protection into processing activities. It requires appropriate technical and organizational measures to be applied both at the stage of determining processing methods and during processing. By default, only data necessary for a defined purpose may be collected, used, retained, or accessed, without requiring user intervention.

The **European Data Protection Board's Guidelines 4/2019 define seven implementation elements: proactive design, default privacy settings, integration within system architecture, preservation of functionality, end-to-end security, transparency, and user-centric safeguards.** These are design-stage requirements, not retrospective controls. Non-compliance is independently enforceable under **Article 83(4), with penalties of up to €10 million or 2% of global annual turnover.**

India's DPDP Act and the Digital Personal Data Protection Rules, 2025, establish an equivalent framework. **Data fiduciaries, particularly significant data fiduciaries, are required to implement technical and organizational controls from the point of data collection.** Consent requests must be clear and unbundled. Data retention must be limited to defined purposes. Security safeguards are mandatory. In combination with data minimization requirements, these provisions establish a functional equivalent to privacy-by-design under GDPR.

For GCC operators, this alignment is operationally relevant. Systems designed to meet Article 25 standards featuring granular consent capture, default data minimization, and purpose-linked retention can meet DPDP requirements without structural changes. A unified architecture reduces duplication across audit, documentation, and governance while maintaining compliance across both regimes.

5.2 Accountability- First Architecture: DPO vs. Grievance Redressal Officer

Both the GDPR and the DPDP Act operationalize their accountability mandates through designated individuals charged with oversight of the organization's data protection function. While the roles are structurally distinct, they share the same institutional purpose: to place responsibility for data protection compliance within an identifiable, accountable person or function within the organization.

Dimension	GDPR - Data Protection Officer (DPO)	DPDP - Accountability Roles
Legal Basis	Articles 37–39	Sections 10 & 13 + DPDP Rules, 2025
Applicability Trigger	Mandatory for public authorities, large-scale monitoring, or sensitive data processing	Mandatory role structure for Significant Data Fiduciaries; grievance mechanism required for all Data Fiduciaries
Primary Role Type	Internal oversight authority	Split structure: compliance contact + grievance interface
Core Function	End-to-end data protection oversight	Regulatory interface + complaint resolution
Regulatory Interface	Direct contact point for supervisory authority	Designated contact person for the board and Government (SDFs only)
Data Subject Interface	Contact point for data subjects	The Grievance Redressal Officer handles complaints
Monitoring Responsibility	Monitors compliance and internal controls	Data audits and DPIAs are required for SDFs
Scope of Responsibility	Organisation-wide compliance function	Functionally segmented responsibilities

5.3 Vendor & Processor Due Diligence: Article 28 GDPR ↔ Rule 6 DPDP

The **controller–processor (or, in DPDP terminology, data fiduciary–data processor)** relationship is governed by mandatory contractual requirements under both regimes. The structural logic of both frameworks is identical: the organization that determines the purpose and means of processing (the controller/fiduciary) is ultimately **accountable for compliance but must exercise that accountability through the selection, instruction, and ongoing oversight of the processors it engages.**

Dimension	GDPR - Article 28	DPDP Act & Rules, 2025
Processor selection	Verifiable compliance capability required; the controller must assess and evidence	The processor acts under a fiduciary mandate; no formal pre-engagement verification standard is defined
Instruction control	Binding deviation constitutes a breach of GDPR	Binding, aligned with fiduciary direction under the Act
Breach reporting	Immediate notification to the controller; supports a 72-hour regulatory timeline	Prompt notification to fiduciary; fiduciary manages regulatory disclosure
Data exit controls	Mandatory deletion/return at contract end; auditable requirement	Not explicitly prescribed; inferred via the purpose limitation principle
Sub-processor approval	Prior written authorization is required in all cases	No explicit approval requirement defined
Downstream obligations	Full contractual replication across sub-processors	No explicit flow-down mandate; indirect control via fiduciary
Liability chain	The processor is fully liable for sub-processors; this is enforceable through contract	The fiduciary retains end-to-end accountability across the processing chain
Role reclassification risk	Independent decision-making triggers controller status (CJEU, 2025)	No explicit statutory equivalent, but the fiduciary role remains primary
Cross-border processing	Permitted with transfer safeguards (Chapter V GDPR)	Permitted unless restricted by government notification

5.4 The India–EU Data Adequacy Pathway: Status, Hurdles & Horizon

An adequacy decision by the European Commission under Article 45 of the GDPR in respect of India would constitute the most consequential development in EU–India digital trade since the GDPR's inception. It would **eliminate the requirement for SCCs, Transfer Impact Assessments (TIAs), and the attendant legal uncertainty that currently characterizes cross-border data flows from EU entities to India-based GCCs and service providers.**

Current Mechanisms and Their Limitations

- In February 2024, the European Data Protection Supervisor declined the European Investment Bank's proposed data transfer to India. A later clarification in May 2025 confirmed that this was procedural, not a direct assessment of India's data protection law. However, the decision highlighted a **key issue for TIAs: whether individuals have adequate protection against government access to their data, particularly in the absence of independent oversight.**

- **Two aspects of India's DPDP framework are central to this assessment:**
  - **First, Section 17(2) allows the central government to exempt government bodies from the Act on grounds such as national security, public order, or sovereignty.** This provision does not require proportionality review, independent oversight, or prior judicial approval. The Court of Justice of the European Union, in the Schrems II judgment, held that SCCs cannot ensure effective protection where domestic laws permit state access to personal data without comparable safeguards. Section 17(2), in its current form, does not clearly meet this standard.
  - **Second, the Data Protection Board of India, established under Section 19, does not have structural independence from the central government.** Its members are appointed by the government, and their terms of service are also determined by it. This differs from the requirement under GDPR Article 52, which mandates independent supervisory authorities.

These elements remain central to evaluating the effectiveness of SCC-based transfer mechanisms for India-bound data flows.

What an Adequacy Assessment would examine?

Under Article 45(2), the European Commission determines whether a third country ensures a level of data protection essentially equivalent to that of the European Union. Prior adequacy decisions for Japan (2019), the Republic of Korea (2021), and the United Kingdom (renewed in December 2025) indicate a consistent evaluation framework across seven areas:

- **Rule of law and protection of fundamental rights**
- **Existence and independence of a supervisory authority**
- **International data protection commitments**
- **Presence of legally binding data protection instruments**
- **Availability of administrative and judicial redress**
- **Rights afforded to individuals**
- **Obligations imposed on organisations processing personal data**

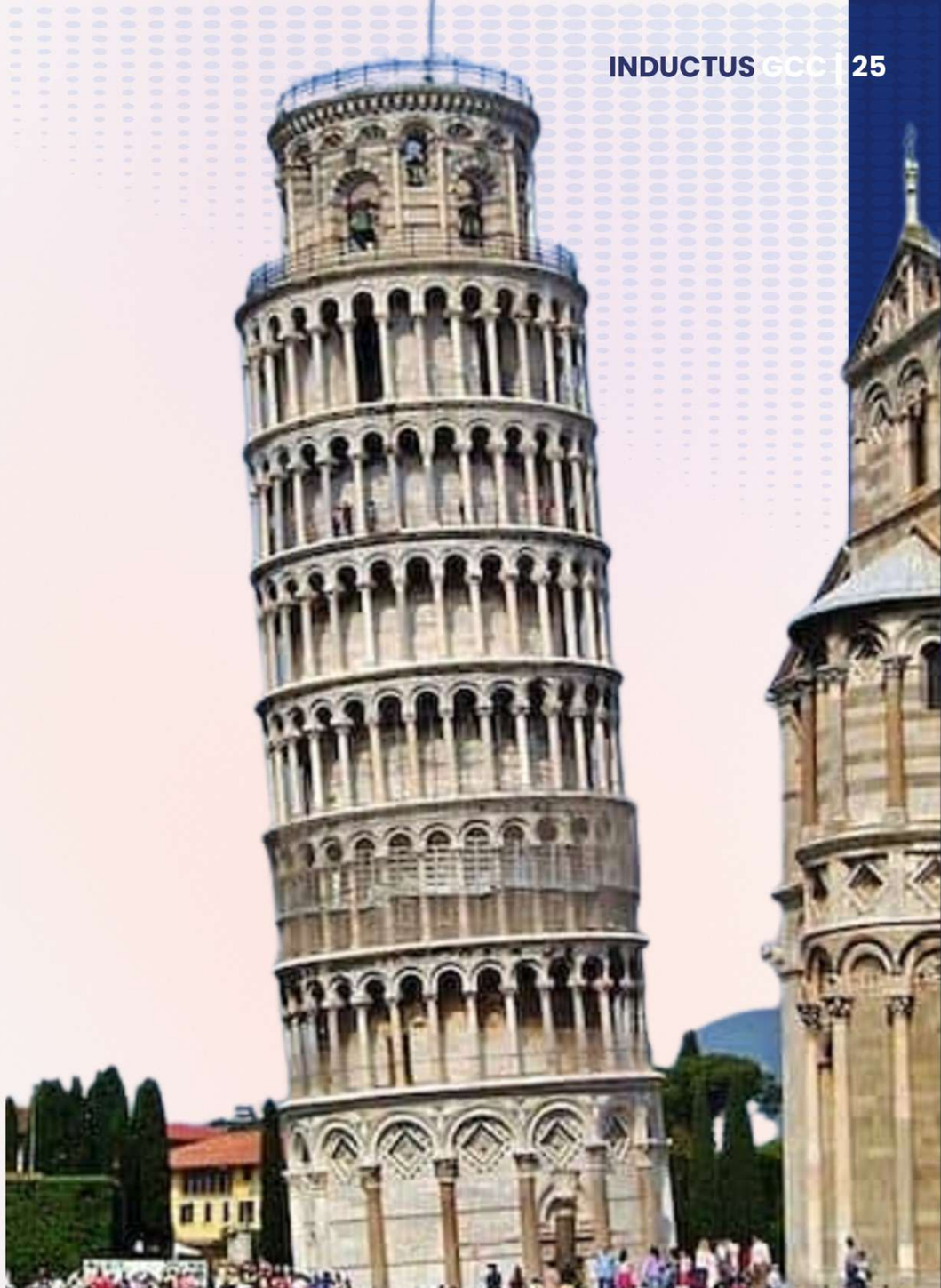
India's Digital Personal Data Protection Act (DPDPA) aligns with several elements of this framework:

- Establishes a rights-based structure grounded in constitutional principles
- Positions consent as the primary basis for processing
- Provides defined rights to Data Principals, including access, correction, erasure, and nomination
- Imposes obligations on Data Fiduciaries, including security safeguards and breach notification
- Introduces financial penalties for non-compliance, up to INR 250 crore (approximately €27.5 million)
- Incorporates principles such as purpose limitation, data minimisation, and accuracy, consistent with GDPR standards

Identified Gaps Relative to Adequacy Benchmarks: Certain structural elements differ from those observed in prior adequacy determinations.

- Government access provisions do not incorporate an explicit proportionality-based review standard
- The independence of the supervisory authority is not fully established
- Judicial redress mechanisms remain limited in scope
- The Act applies only to digital personal data, excluding non-digitised records

The European Data Protection Supervisor has not initiated a formal assessment of the DPDP Act, and the Digital Personal Data Protection Rules, 2025, are in phased implementation, meaning key operational provisions are not yet in force.



The Adequacy Horizon

The **India–EU Trade and Technology Council (TTC),** established in 2023, provides a formal channel for engagement on data governance. The EU has previously used such bilateral forums when working with countries pursuing adequacy status.

In the near term, adequacy status for India is unlikely within the next three to five years. Key issues remain unresolved, particularly around the independence of the supervisory authority and provisions relating to government access to data. The DPDP Rules, 2025, implement the existing Act but do not address these structural concerns. Progress toward adequacy would therefore require legislative amendments or a more limited arrangement focused on specific sectors, similar in structure to the EU–US Data Privacy Framework.

India-EU Adequacy Assessment Gap Analysis

Adequacy Criterion (Article 45(2))	DPDP Act Status	Assessment
Rights-based framework/rule of law	Present	Constitutional grounding in Article 21 (Puttaswamy, 2017). Data principal rights are codified in Sections 11–13 of the DPDP Act.
Independent supervisory authority	Partial / At Risk	Data Protection Board members are appointed, and service conditions are set by the central government. Structural independence from executive influence not established (cf. GDPR Article 52).
Government access - proportionality and judicial oversight	Gap	Section 17(2) permits broad government exemptions without proportionality review or independent oversight. Schrems II standard is not demonstrably met.
Effective judicial and administrative redress	Developing	The Data Protection Board is quasi-judicial; appeals lie with the High Court. Direct judicial review mechanisms are limited under the current text. Rules (2025) provide complaint procedures.
Data subject rights—practical enforceability	Partially in force	Rights under Sections 11–13 are qualified by 'as may be prescribed,' dependent on notified rules. DPDP Rules (2025) are in phased implementation; practical enforceability is to be established.
Cross-border transfer framework	Divergent	The DPDP Act permits transfers to all countries by default unless restricted by a government notification. No adequacy equivalence requirement for outbound transfers. Contrasts with GDPR's Chapter V structure.
Enforcement and penalties	Present but limited	Maximum penalty of INR 250 crore (≈ €27.5M) for certain violations. Lower penalty ceiling than GDPR (€20M / 4% of global turnover). Board enforcement is operational from Phase I implementation.

The India–EU digital relationship shows measurable regulatory gaps, a consistent direction of alignment, and strong economic incentives to converge. Adequacy will depend not only on the DPDP Act but also on future legislative choices and the priority given to India–EU engagement.

Sector-Specific Compliance Implications

Sector-specific compliance obligations under GDPR and the DPDP framework differ by data classification, transfer architecture, and processor positioning, requiring calibrated implementation across industries.

6.1 BFSI: Cross-Border Data in Financial Services & Fintech

BFSI GCCs in India process payment data, credit data, KYC records, and trading data for EU-based parent entities and clients. Every data category involved carries either sectoral regulatory obligations under RBI, SEBI, or IRDAI, or special-category status under the GDPR, or both. No other sector operates under as dense a regulatory stack.

~340
Largest GDPR fine - BFSI

€746M
Amazon
(Luxembourg, 2021)

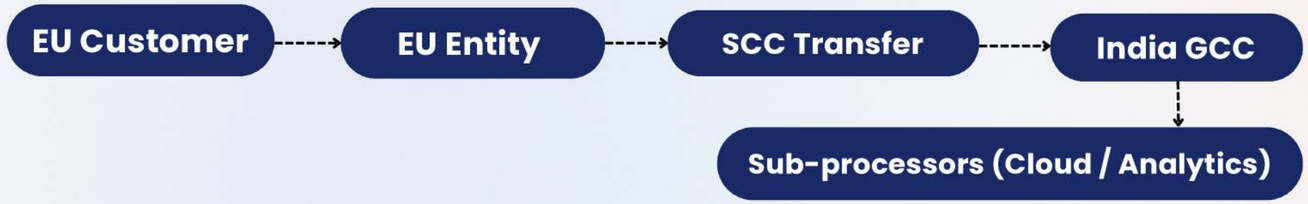
RBI payment data rule
India-only
Storage mandate, 2021

GDPR financial data classification
Art. 9+
Where health and financial data overlap

Regulatory Exposure Map

Data Category	GDPR Classification	DPDP Classification	Primary Risk
Credit/loan records	Personal data (Art. 4)	Personal data (Sec. 2(t))	Dual-regime consent obligation
Transaction history	Personal data	Personal data	Cross-border transfer - SCC + TIA required
Biometrics (eKYC)	Special category - Art. 9	Not separately categorised*	GDPR explicit consent; DPDP lacks equivalent special-category tier
AML/fraud analytics	Personal data; profiling under Art. 22	Personal data	DPDP lacks a legitimate interest basis; consent is required
Employee payroll data	Personal data	Legitimate use - Sec. 7(f)	Aligned employment processing basis available in both

Data Flow Structure (Financial Services)



6.2 Healthcare & Life Sciences: Clinical Data, Trials & Patient Privacy

Clinical trial data processed in India
40%+
of global trials use India-based CROs / GCCs

GDPR health-data fines (2018–2025)
€380M+
CMS Enforcement Tracker, March 2025

DPDP health data
No special tier
Treated as personal data under Sec. 2(t)

The Asymmetry Problem: GDPR Special Category vs. DPDP Standard Personal Data

Parameter	GDPR	DPDP Act
Health data classification	Special category - Art. 9. Processing generally prohibited unless explicit consent, vital interests, health care purposes, or public health (Art. 9(2))	Personal data, Sec. 2(t). Standard consent rules apply. No elevated processing prohibition.
Genetic/biometric data	Special category - explicit consent or Art. 9(2) derogation required	Not separately categorized. Standard consent suffices.
Research processing basis	Art. 9(2)(j) scientific research with appropriate safeguards and pseudonymization	No equivalent research derogation. Consent or legitimate use (Sec. 7) required.
Pseudonymization requirement	Recommended by Art. 89 for research; reduces risk under Art. 25	Not prescribed. Organizations may apply voluntarily.
Cross-border transfer of patient data	Chapter V mechanism required (SCC + TIA for India)	No restriction unless a central government notification is issued under Sec. 16.

Clinical Data Lifecycle (Simplified)

Patient Data → **Trial Collection** → **Processing (EU/India)** → **Analysis → Retention / Deletion**

6.3 IT/ITeS & BPO: Processor Liability & Client Data Instructions

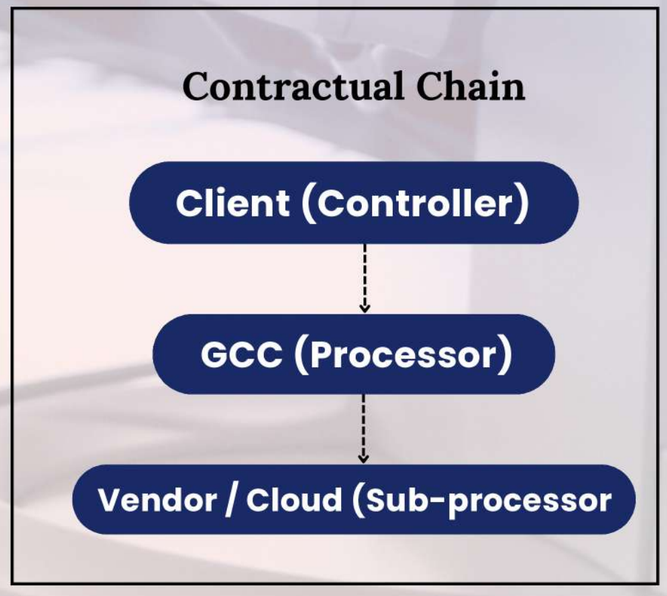
India GCC IT/ITeS share
47%
of the total GCC workforce, 2024

CJEU - processor reclassification
Dec 2025
Russmedia ruling: processors acting beyond instructions become controllers

GDPR processor fines (2018–2025)
€210M+
For Art. 28 / security failures

Processor Liability Architecture: Where IT/ITeS GCCs Are Exposed

Scenario	GDPR Position	DPDP Position	Risk Level
GCC processes strictly per EU client instructions	Processor. Liable for Art. 28 obligations only.	Data Processor. Rule 6 safeguards apply.	Manageable
GCC makes discretionary decisions on processing methods	Reclassified as joint controller (Russmedia, Dec 2025). Full GDPR liability.	May qualify as a data fiduciary. Full DPDP obligations apply.	High
GCC subcontracts to an Indian vendor without client approval	Breach of Art. 28(2). The controller may terminate and seek damages. GCC retains full liability for sub-processors.	The DPDP Act is silent on sub-processor pre-approval; fiduciary accountability persists.	High, GDPR
GCC processes Indian employee data for EU parent HR systems	The EU parent is the controller; the GCC is the processor. Art. 28 DPA required.	GCC is a data fiduciary for Indian employee data under Sec. 7(f) legitimate use.	Dual-regime: separate obligations
GCC uses client data for internal AI model training	Likely exceeds processing instructions - controller reclassification risk (Art. 28(3)(a)).	Processing outside the fiduciary's instructions. Unlawful under Sec. 8.	Critical



- **GDPR: Full contractual replication**
- **DPDP: Accountability retained at fiduciary level**

6.4 Retail, E-Commerce & Consumer Data

India's digital consumer base 820M+
Internet users, TRAI 2024

GDPR fines - consumer data €1.9B+
Consent & profiling violations, 2018–2025

DPDP children's data age gate 18 yrs
vs. 13–16 yrs under GDPR. (member-state variable)

Consumer Data Processing: Compliance Parameters by Activity

Processing Activity	GDPR Basis	DPDP Basis	Compliance Gap
Loyalty programme enrolment	Consent (Art. 6(1)(a)) or Contract (Art. 6(1)(b))	Consent (Sec. 6) or Contract legitimate use (Sec. 7(b))	Aligned contract basis available in both
Behavioral/retargeting ads	Consent required for ePrivacy; legitimate interests permitted with a balancing test	Consent required. No legitimate interests basis.	DPDP requires consent, whereas GDPR may not
Cross-border purchase data to the EU parent	SCC + TIA required (EU → India direction)	No restriction (India → EU direction) unless Sec. 16 notification issued	One-directional EU-origin data requires SCC
Targeting users aged 13–17	Permitted with parental consent in some member states	Prohibited - tracking and behavioural ads to under-18s are absolutely prohibited (Sec. 9(3))	DPDP is more restrictive, with a separate age-gate required
AI-driven personalisation	Profiling / automated decisions: Art. 22 safeguards if significant effects	No equivalent Art. 22. Standard consent covers personalization.	GDPR imposes additional safeguards for significant automated decisions

Consumer Data Flow

User ----→ **Platform** ----→ **Consent Capture** ----→ **Processing** ----→ **Personalisation / Marketing**

6.5 Manufacturing, Engineering & Industrial R&D GCCs

Engineering GCCs in India
580+
NASSCOM, 2024: fastest-growing segment

Industrial R&D data processed in India
$8.3B
Offshore engineering services market, 2024

Primary GDPR risk category
Employee data
Workforce records of EU-based staff processed in India

Data Categories in Manufacturing / Engineering GCCs - Regulatory Mapping

Data Type	GDPR Relevance	DPDP Relevance	Compliance Requirement
EU employee records (processed in India GCC)	Personal data. Controller = EU parent. GCC = processor. Art. 28 DPA + SCC + TIA required.	If Indian employees are in scope: Sec. 7(f) legitimate use. If EU data only: GDPR governs.	SCC mandatory; DPDP applies to Indian employee records separately
Industrial IoT / sensor telemetry	Personal data only if identifiable to individuals. Aggregated machine data: outside GDPR scope.	Same analysis. Non-identifiable data outside the DPDP scope.	The identifiability test determines the scope under both regimes
R&D/IP documentation	Outside the GDPR scope unless it contains personal data of researchers or subjects.	Outside the DPDP scope unless it contains personal data.	Not a data protection issue unless personal data is embedded
Supplier/vendor individual contacts	B2B contact data is personal data under Art. 4. The legitimate interests basis is generally available.	Personal data under Sec. 2(t). Consent or legitimate use is required—no LI basis.	DPDP requires consent for supplier contact processing; GDPR does not
EHS/safety incident records (employee-linked)	May include health data (special category - Art. 9). Explicit consent or a vital interests basis is required.	Personal data (standard). Standard consent or Sec. 7 legitimate uses (medical emergency) may apply.	GDPR imposes special-category restrictions absent from DPDP

R&D Data Flow Model

EU Design Centre ----→ **Data Transfer** ----→ **India GCC** ----→ **Engineering / Analytics** ----→ **Output**

How Does GDPR–DPDP Compliance Convergence Redefine the GCC Business Case?

Before November 2025, India-based GCCs operated under a regulatory arbitrage: they managed EU data under the constraints of the General Data Protection Regulation (GDPR) while India itself maintained no comprehensive personal data protection framework at the federal level. This asymmetry reduced operational efficiency, increased compliance costs through redundant infrastructure, and created jurisdictional friction in cross-border processing.

The DPDP framework aligns core elements with GDPR across processing principles, accountability, data subject rights, and enforcement. This convergence standardizes compliance expectations and affects GCC operating models, including location strategy, workforce requirements, and technical capabilities.

How regulatory convergence restructures compliance economics, workforce strategy, and technology architecture for India-based Global Capability Centers?

Cost Reduction
30–40%
In systems duplication

Annual Savings
USD 90–150K
Per mid-size GCC,

Workforce Gap
6,500–8,500
Professionals needed by 2027

Capacity Shortage
4–10x
Demand vs. supply

7.1 Regulatory Compatibility as Location Factor

Before DPDP operationalization, India's GCCs maintained parallel compliance architectures: one for GDPR and one for India's sectoral regulations. This duplication created operational inefficiency and location friction.

Cost Structure Comparison: Pre-DPDP vs. Post-DPDP

Cost Category	Pre-DPDP	Post-DPDP
Systems Infrastructure	USD 350–950K/yr	USD 100–250K/yr
Governance & Oversight	USD 120–240K/yr	USD 60–120K/yr
Transfer Compliance (TIA)	EUR 30–120K/yr	EUR 15–35K/yr
Total Annual Burden	USD 600–1,300K	USD 300–550K

Location Factor Ranking (2025)

Rank	Location Factor	2023 Position	2025 Position	Driver
1	**Labor Cost**	1st	1st	Primary differentiator
2	**Talent Availability**	2nd	2nd	Skill depth in tech hubs
3	**Regulatory Compatibility**	6th	3rd ↑	DPDP operationalization
4	**Infrastructure Quality**	3rd	4th	Data centers, connectivity
5	**Tax Incentives**	4th	5th	SEZ benefits, state schemes

7.2 Unified Compliance Architecture

GDPR Article 25 and DPDP Section 8 establish functionally equivalent privacy-by-design requirements. Organizations can now implement single compliance systems serving both frameworks.

Architecture Unification Scope

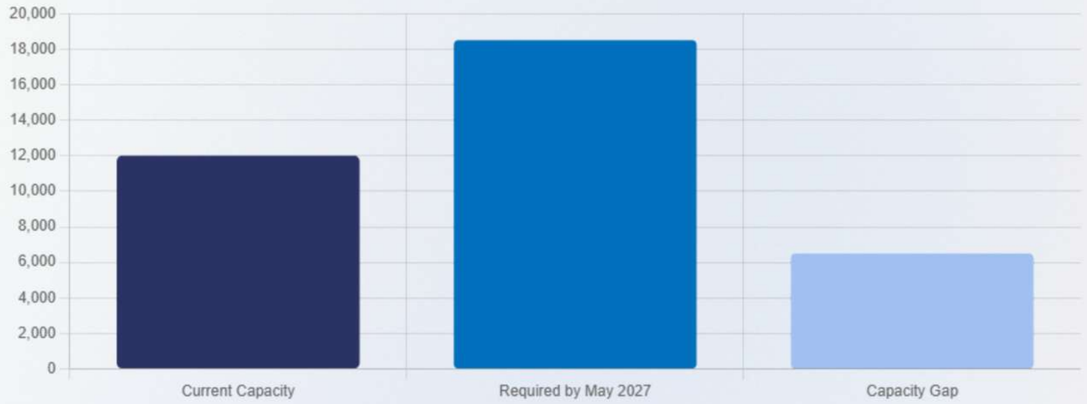
Domain	Unification Approach	Implementation Cost	Timeline
Consent Management	Single platform, dual-format consent capture (GDPR + DPDP parametric)	USD 180–280K	6-9 months
Data Retention	Unified retention framework with purpose-linked purge schedules	USD 120–200K	4-6 months
Security & Access Control	Single SOC managing both frameworks (ISO 27001 baseline)	USD 80–150K	Ongoing
Audit & Governance	Consolidated DPIA process serving both regimes	Internal resource reallocation	6 months
Processor Contracts	Unified DPA satisfying GDPR Article 28 + DPDP Rule 6	Legal review 30–40% reduction	Faster onboarding

Resource Efficiency Gains

GCCs maintaining separate GDPR and DPDP DPIAs require 3-4 FTE annually. Post-unification: 2–2.5 FTE (25–30% reduction). For a representative 500-person GCC, this translates to approximately USD 90,000–150,000 annual savings in labor allocation.

7.3 DPDP-Ready Workforce: Upskilling & Talent Pipeline

Current Capacity vs. Requirement



Certification Landscape (2025)

Credential	India-based Professionals	Growth Rate	Status
IAPP CIPP/E	2,100	+35–40% annually	Established
DPIA Specialist	300–400	+22% annually	Growing
DPDP-Specific	None	-	Launching Q4 2026
Privacy Engineering	350–450	+45–55% annually	High demand

Training Program Capacity by 2027

University Programs	400–550/yr
Corporate Training	2,000–3,500/yr
NASSCOM Programs	5,000–8,000 by 2027
Bootcamp/Specialized	300–500/yr

Capacity Gap: 5,300–7,700 professionals over an 18-month implementation period.

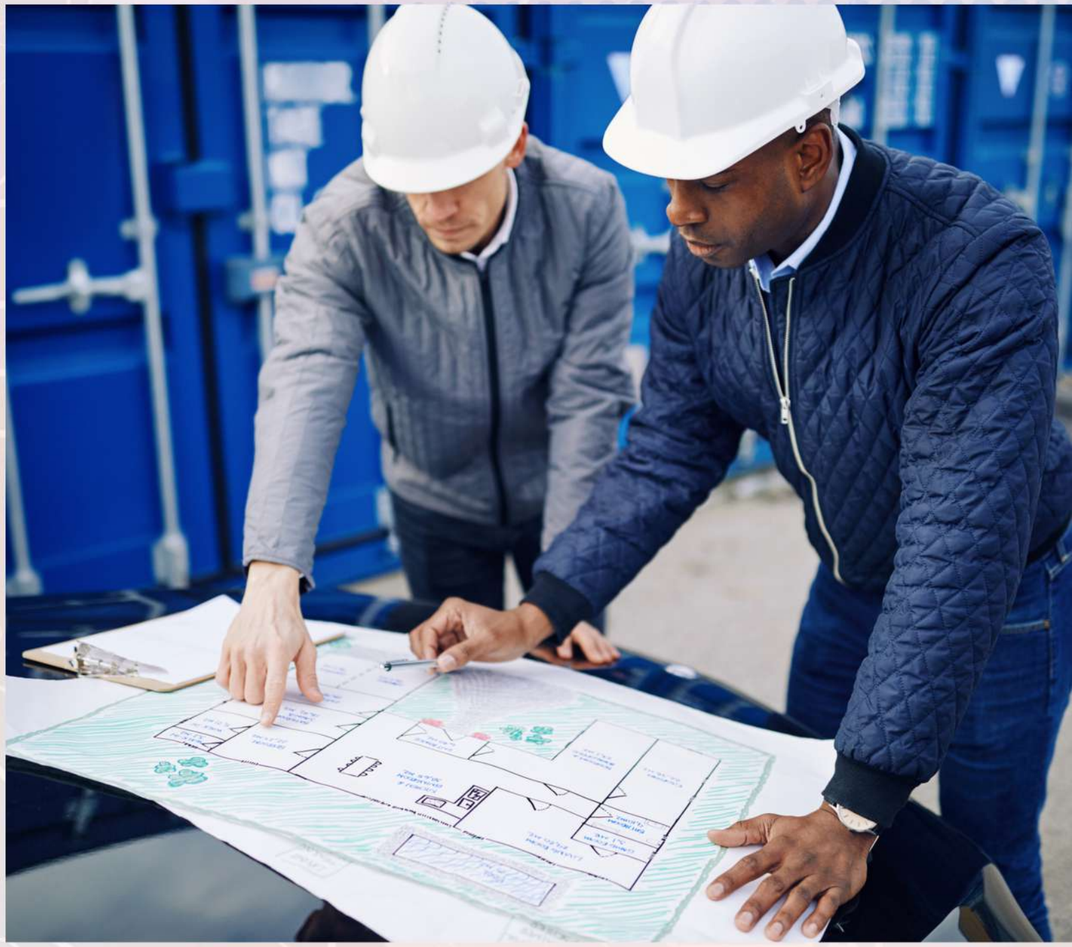
7.4 Privacy Engineering as Core Competency

Current Capability Distribution

Tier	GCC Count	Professionals	Characteristics
Advanced	50–70	150–200	Privacy integrated into the development lifecycle; DPIA automation
Intermediate	200–250	100–150	Privacy requirements documented; ad-hoc implementation
Foundational	900–1,100	80–100	Privacy secondary; policy-driven controls; no technical integration
Total Current	1,200–1,450	350–450	0.03% of the GCC workforce

Privacy Engineering Technology Stack (Annual Cost)

Component	Tool Examples	Cost Range
Privacy by Design / DPIA Tools	LINDDUN, TrustArc, OneTrust	USD 5–15K
Encryption & Cryptography	AES, TLS/SSL, and Tokenization platforms	USD 5–15K
Pseudonymization / Anonymization	Differential Privacy, K-Anonymity, Data Tagging	USD 20–50K
Access Control & Identity	RBAC, PAM, ABAC systems	USD 30–80K
Data Discovery & Monitoring	Data Catalogs, DLP, Compliance Monitoring	USD 50–150K
Total Stack (Mid-size GCC)		**USD 150–350K/yr**



Strategic Implications

Location Economics

Regulatory compatibility now ranks 3rd in GCC location decisions, elevating India's strategic value for data-intensive operations.

Unified Infrastructure

Organizations implementing single-architecture compliance systems realize 30–40% cost reductions and 25–30% workforce efficiency gains.

Talent Development

A capacity gap of 6,500–8,500 professionals presents retention and compensation risk; early upskilling investments improve competitive positioning.

Privacy Engineering

A 4–10x demand-supply imbalance creates outsourcing and partnership opportunities for technology-focused GCCs.

Adequacy Pathway

India–EU adequacy determination is unlikely before 2028; organizations must design for SCC-dependent transfers and supplementary measure requirements.

The India–EU Partnership Dividend: Why Now Is the Optimal Window?

Three developments between January 2025 and January 2026 changed the commercial and regulatory conditions for EU–India GCC operations in ways that have no precedent in the prior decade of the bilateral relationship. The conclusion of the India–EU Free Trade Agreement on 27 January 2026, after eighteen rounds of negotiations spanning nine years, eliminated a long-standing source of bilateral policy uncertainty. This section examines each of these developments and their direct implications for GCC operators and their EU parent entities.

8.1 India–EU Free Trade Agreement (27 January 2026): A Historic Milestone

Years of negotiation	EU–India bilateral trade (goods + services)	India's rank among EU trading partners
9 yrs	**€120B**	**#9**
18 rounds, suspended in 2007, resumed in 2022	2024 - European Commission	Goods: #8 services, 2024

The India–EU Free Trade Agreement, formally designated the **India–EU Broad-based Trade and Investment Agreement (BTIA),** was concluded at the India–EU Summit in New Delhi on 27 January 2026 and is subject to ratification by EU Member States and the European Parliament.

The concluded agreement covers goods tariffs, services market access, investment protection, government procurement, intellectual property, sustainability, and a standalone digital trade chapter.

FTA Chapter	Core Commitment	GCC Implication
Services (Mode 3)	Easier establishment of EU subsidiaries across key sectors	Simplifies GCC setup and expansion; reduces entry restrictions
Services (Mode 4)	Defined mobility frameworks for intra-company transfers	Improves the movement of EU and India-based professionals
Digital Trade	Framework for data flows, e-contracts, and source code protection	Supports cross-border data operations beyond GDPR mechanisms
Investment Protection	Safeguards against expropriation; dispute resolution mechanisms	Reduces investment risk for EU-backed GCCs
Intellectual Property	Stronger protection and enforcement standards	Enables transfer of IP-intensive work to India GCCs
Government Procurement	Access to public sector contracts on a reciprocal basis	Expands participation of GCCs in government projects

8.2 Digital Trade Chapter: E-Contracts, Privacy Sovereignty & Interoperability

The Digital Trade Chapter of the India–EU FTA is the first treaty-level instrument to directly address the legal framework for EU–India data flows, electronic commerce, and digital services.

India's digital economy (2025 est.)	EU digital single market GDP contribution	Cross-border data flows: India–EU volume
$1T	**€415B annually**	**#1**
Towards $1 trillion by 2025-DPIIT	2024 - European Commission	Fastest-growing bilateral data corridor in Asia, 2023–25

Digital Trade Chapter: Key Commitments

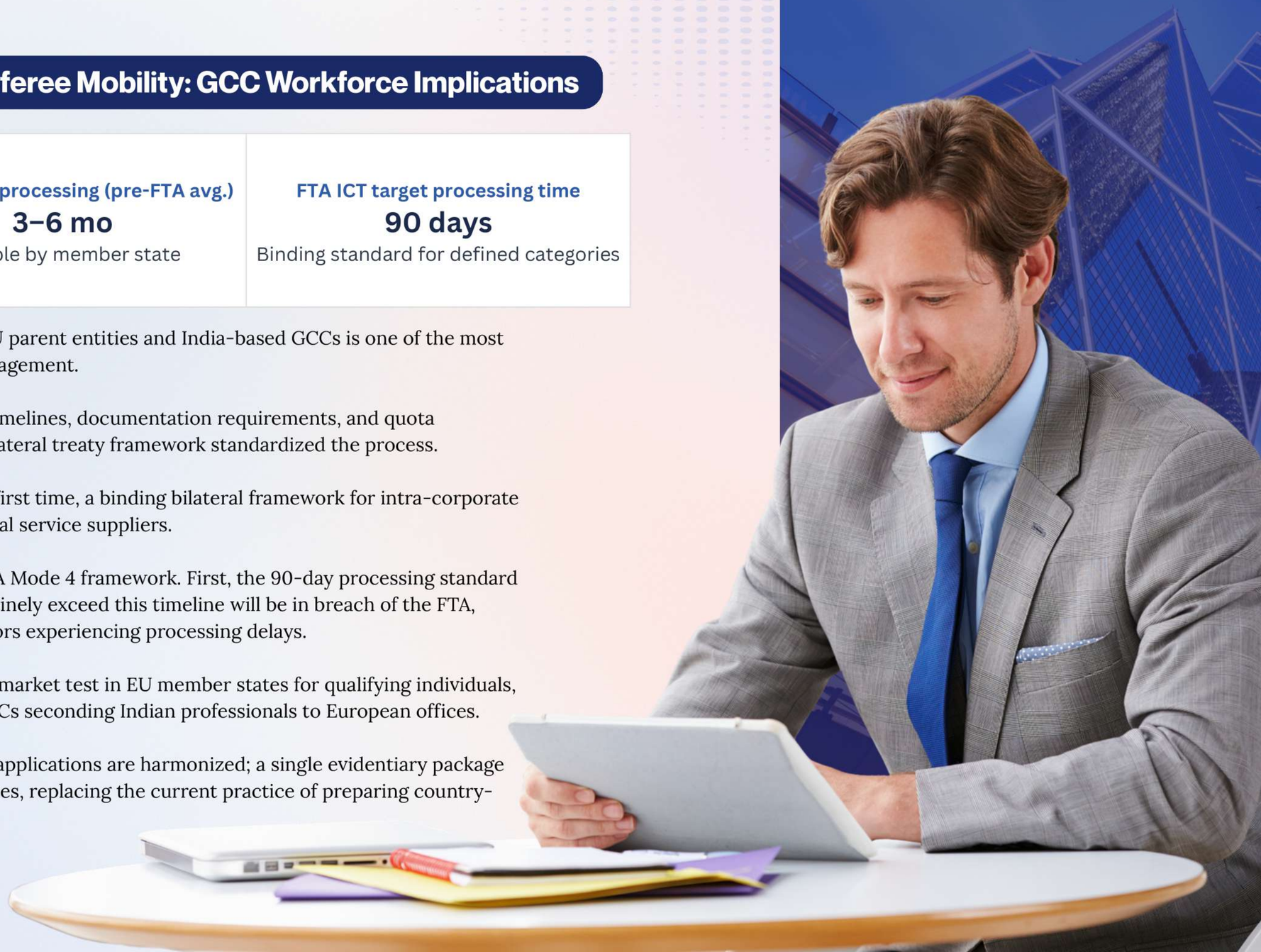
Commitment Area	Treaty Provision	Operational Effect
Electronic contracts	Legal validity of electronic contracts and e-signatures recognised	Cross-border agreements enforceable without physical signatures
Cross-border data flows	No unjustified restrictions on data transfers for commercial use	Supports EU–India data flows; GDPR transfer rules still apply
Privacy sovereignty	Each party retains its own data protection framework	GDPR and DPDP operate independently; no adequacy implied
Source code protection	No mandatory disclosure of source code for market access	Protects software handled by GCCs from forced access
Regulatory transparency	Obligation to publish and consult on new digital regulations	Advance visibility on regulatory changes
Interoperability	Cooperation on digital systems and standards	Enables future alignment of digital frameworks

> “The Digital Trade Chapter does not resolve the adequacy gap. It constrains both governments from creating arbitrary new barriers to data flows, which is a different and more durable form of protection for GCC operators than private contractual mechanisms alone.”

8.3 India–EU Intra-Corporate Transferee Mobility: GCC Workforce Implications

Indian IT professionals in the EU (est.)	EU ICT visa processing (pre-FTA avg.)	FTA ICT target processing time
320K+	**3–6 mo**	**90 days**
2024 - NASSCOM / Eurostat	Variable by member state	Binding standard for defined categories

- The movement of skilled professionals between EU parent entities and India-based GCCs is one of the most operationally constrained dimensions of GCC management.
- Before the FTA, visa and work permit processing timelines, documentation requirements, and quota restrictions varied by EU member state, and no bilateral treaty framework standardized the process.
- The FTA's Mode 4 commitments establish, for the first time, a binding bilateral framework for intra-corporate transferees (ICTs), business visitors, and contractual service suppliers.
- Three compliance implications follow from the FTA Mode 4 framework. First, the 90-day processing standard is a binding commitment. Member States that routinely exceed this timeline will be in breach of the FTA, creating an escalation mechanism for GCC operators experiencing processing delays.
- Second, the ICT category does not require a labor market test in EU member states for qualifying individuals, removing a significant operational obstacle for GCCs seconding Indian professionals to European offices.
- Third, the FTA's documentation standards for ICT applications are harmonized; a single evidentiary package will satisfy the requirements of all EU member states, replacing the current practice of preparing country-specific application bundles.



8.4 Profitability Analysis: Cost, Risk & Strategic Value for EU-Origin GCCs

Labour cost differential: India vs. EU	India GCC market size (2025)	GCC revenue CAGR (2019–2025)
~60–70% Comparable seniority; engineering / legal functions	**~$69.85B**	**11.4%** consistent across sectors

Cost Structure (Post-2025)

Component	Position
Labour cost	50–70% lower vs EU
One-time compliance cost	€150K – €500K*
Annual compliance cost	€50K – €175K*
Cost driver	DPDP implementation on GDPR baseline

*Industry estimates based on advisory benchmarks.

Risk vs Cost Position

Parameter	Regulatory Position
GDPR exposure	Up to €20M or 4% global turnover
DPDP exposure	Up to ₹250 crore (~€27–30M)
Compliance spend	Limited relative to enforcement thresholds

Compliance costs represent a small proportion of potential regulatory exposure, assuming standard GCC operating scales.

Operational Impact

- SCC-based transfers and transfer impact assessments remain standard for EU data flows.
- DPDP introduces incremental controls without altering the core architecture
- Dual-regime alignment reduces enforcement and transfer disruption risk
- Compliance status is increasingly referenced in EU client contracting

The labor cost differential remains the primary driver of GCC economics. Incremental compliance costs under the DPDP framework do not materially alter the cost structure and support continuity in EU–India data flows.

8.5 Government of India's GCC Policy Infrastructure: SEZs, State Incentives & DPIIT Schemes

Active SEZs in India (2025)	GCC-hosting states (major)	DPIIT Startup India GCC support
368	**6**	**2023**
Ministry of Commerce; 276 operational	KA, MH, TN, TS, NCT, AP - 80%+ of GCC base	Dedicated GCC policy framework notified

India's central and state governments have, since 2022, developed a formal policy infrastructure for attracting and retaining GCCs. This infrastructure operates at three levels: **the national SEZ framework under the Special Economic Zones Act, 2005; state-level GCC policies with direct incentive schedules; and central government schemes administered by the Department for Promotion of Industry and Internal Trade (DPIIT).**

Benefit Category	Applicable Provision
Income Tax	Section 10AA of the Income Tax Act, 1961: 100% tax exemption on export profits for the first 5 years; 50% for years 6–10; 50% of reinvested export profits for years 11–15. New units established in SEZs under the amended framework retain deduction eligibility subject to notified conditions.
Goods & Services Tax	Services exported from SEZ units are treated as zero-rated supplies under the IGST Act, 2017. No GST on services provided to clients outside India, including EU parent entities and EU-based clients.
Customs Duty	Duty-free import of goods required for operations (hardware, servers, specialist equipment). Applicable to technology and engineering GCCs importing specialized equipment not manufactured domestically.
Single-Window Clearance	SEZ units receive single-window regulatory approvals through the Development Commissioner's office, covering environmental clearances, building permits, and labor registrations.
FEMA / Forex	SEZ units may maintain foreign currency accounts; proceeds from the export of services may be credited directly without mandatory conversion within prescribed timelines.

State GCC Policies Comparative Incentive Matrix

Incentive	Karnataka	Maharashtra	Telangana	Tamil Nadu	NCT Delhi	Andhra Pradesh
GCC-specific policy	Yes (2022)	Yes (2023)	Yes (2022)	Yes (2023)	Partial	Yes (2024)
Stamp duty waiver	100%	Up to 100%	100%	Up to 100%	50%	100%
Land allotment (IT parks)	Yes	Yes	Yes	Yes	Limited	Yes
Power tariff subsidy	Yes	Yes	Yes	Yes	No	Yes
Talent pipeline/skilling support	Yes	Yes	Yes	Yes	Partial	Yes
Data centre/infra subsidy	Yes	Yes	Yes	Partial	No	Yes

DPIIT - Central Government GCC Schemes

Scheme	Provision	GCC Relevance
GCC Policy Framework (2023)	Formal classification of GCCs; single-window facilitation; streamlined FDI approvals	Improves establishment timelines and regulatory clarity
PLI-IT Hardware	Incentives for domestic production of servers and network equipment	Reduces infrastructure cost and import reliance
IndiaAI Mission	Public investment in AI compute capacity, datasets, and skilling	Enables access to shared AI infrastructure for R&D operations
National Data Governance Framework	Structured access to non-personal government datasets	Supports analytics and model development use cases
Startup India - GCC Connect	Institutional mechanism for GCC–startup collaboration	Facilitates external innovation and technology sourcing

FUTURE RECOMMENDATIONS

Transfer Mechanism Strategy

• Design for SCC dependency through 2028+, given India-EU adequacy likelihood remains low. India's government access exemptions (Section 17(2)) and supervisory authority independence gaps require resolution before adequacy status is achievable.
• Conduct Transfer Impact Assessments (TIAs) for all EU-origin data flows; document supplementary measures (encryption, access controls, transparency) to withstand Schrems II scrutiny.

Implement Unified Compliance Systems

• Consolidate GDPR and DPDP compliance infrastructure into single systems for consent management, data retention, audit workflows, and processor contracts. Estimated cost savings: USD 90–150K annually for mid-size GCCs.
• Leverage regulatory convergence as a competitive location advantage in GCC site selection and client RFPs.

Address Talent Gap

• Launch DPDP-specific upskilling programs immediately. Capacity shortage: 6,500–8,500 professionals needed by May 2027. Partner with NASSCOM, universities, and certification bodies (IAPP) to accelerate training pipelines.
• Build privacy engineering competency as a differentiator. Current supply covers only 0.03% of the GCC workforce; a 4–10x demand-supply imbalance creates retention and compensation risk.

Operationalize India–EU FTA Benefits

• Use Mode 4 commitments (90-day ICT processing, labor market test waiver) to accelerate EU professional mobility. Streamline visa documentation and secondment processes.
• Monitor Digital Trade Chapter provisions for advanced visibility on regulatory changes; engage the India–EU TTC on data governance alignment priorities.

Strengthen Risk Governance

• Establish dual-regime compliance KPIs: consent rates, breach response timelines, DPIA frequency, and regulatory health scorecards. Board-level reporting on GDPR/DPDP exposure (up to €20M/₹250Cr risk thresholds).
• Monitor DPDP Rules implementation phases (Nov 2025 → May 2027); conduct quarterly SDF compliance assessments for GCCs meeting significant data fiduciary thresholds.

Position for Mid-Term Opportunity

• Organizations executing integrated GDPR–DPDP compliance architectures will achieve cost efficiency, regulatory stability, and competitive advantage in EU-India data operations. Early movers gain reputational and contractual leverage with risk-averse EU clients.

Conclusion

India's operationalization of the Digital Personal Data Protection (DPDP) Act in November 2025 marks a structural inflection point in global data governance and EU–India economic relations. For the first time, multinational enterprises operating across the EU–India corridor face a regulatory environment where both jurisdictions impose comprehensive, rights-centric data protection requirements grounded in similar normative principles.

The convergence is neither complete nor automatic. Critical divergences persist—particularly around government access provisions, supervisory authority independence, and special-category data protections—that make an India–EU adequacy determination unlikely before 2028. Yet the functional alignment of privacy-by-design, accountability structures, and processor safeguards creates an unprecedented opportunity for organizations to deploy unified compliance architectures, reducing duplication costs by 30–40% while maintaining dual-regime compliance maturity.

Global Capability Centers (GCCs) in India are positioned at the center of this opportunity. As regulatory compatibility rises to the third-ranked location factor (from sixth in 2023), and with complementary provisions in the India–EU Free Trade Agreement easing workforce mobility and cross-border service delivery, organizations that implement integrated GDPR–DPDP compliance frameworks will gain measurable competitive advantages in cost efficiency, regulatory credibility, and client risk profile.

The immediate challenge is talent. A shortage of 6,500–8,500 qualified data protection professionals through May 2027 will constrain GCC scaling unless upskilling investments begin immediately. The strategic priority is therefore clear: organizations must synchronize three parallel workstreams—unified compliance infrastructure, workforce development, and regulatory monitoring—to capture the transient window of regulatory opportunity before adequacy determination reshapes the transfer landscape.

> *Organizations that act now will transition from managing regulatory complexity as a cost center to positioning data governance as a competitive advantage in EU–India digital trade. Those who delay will face accelerating compliance costs, talent retention pressure, and contractual friction with risk-averse clients.*

GLOSSARY

Term	Definition
Adequacy Decision	EU determination that a country's data protection framework is equivalent to GDPR standards.
Binding Corporate Rules (BCRs)	Group-wide data protection policies approved by an EU authority for intra-group transfers.
Data Controller	The entity that determines the purposes and means of personal data processing. Equivalent to Data Fiduciary under DPDP.
Data Fiduciary	Under DPDP, the entity is responsible for determining the purposes and means of data processing.
Data Minimization	Principle requiring only the necessary data to be collected and processed for specified purposes.
Data Principal	Under DPDP, an individual to whom personal data relates. Equivalent to a data subject under GDPR.
Data Protection Board (DPB)	An Indian quasi-judicial authority established to handle DPDP complaints and impose penalties.
Data Protection Officer (DPO)	Mandatory officer under GDPR for public authorities and large-scale data processing operations.
Data Subject Rights	Individual rights to access, correct, erase, and object to the processing of personal data.
Digital Personal Data Protection Act (DPDP)	India's comprehensive data protection law was enacted in 2023 and operationalized in May 2027.
EU Data Privacy Framework (DPF)	An adequacy arrangement between the EU and the U.S. was established in 2023 for data transfers.
General Data Protection Regulation (GDPR)	EU regulation has been enforceable since May 2018, governing personal data protection with extraterritorial reach.
Grievance Redressal Officer (GRO)	Under DPDP, a designated officer is responsible for receiving and resolving data-principal complaints.
Lawful Basis	Legal foundation required for personal data processing. GDPR has six bases; DPDP relies primarily on consent.
Personal Data	Information relating to an identified or identifiable individual.
Privacy by Design	Requirement to integrate data protection into processing activities from inception.
Processor	Entity processing personal data on behalf of a controller under instructions and contractual safeguards.
Purpose Limitation	Principle preventing further processing of data in ways incompatible with original collection purposes.
Schrems II	2020 CJEU judgment requiring stringent safeguards for data transfers outside the EU.
Significant Data Fiduciary (SDF)	Under DPDP, a data fiduciary processes large volumes or sensitive categories of personal data.
Special Category Data	Sensitive personal data (health, genetic, biometric, and religious) requires heightened GDPR protections.
Standard Contractual Clauses (SCCs)	Pre-approved contractual modules governing data transfers from the EU to non-adequate countries.
Sub-processor	Entity engaged by a processor to process personal data; requires controller authorization (GDPR).
Transfer Impact Assessment (TIA)	Analysis assessing whether SCCs ensure adequate protection given the recipient country's laws and practices.

References:

- CMS Law / GDPR Enforcement Tracker Report, 6th Edition (cut-off 1 March 2025)
- DLA Piper, GDPR Fines and Data Breach Survey: January 2025.
- DLA Piper, GDPR Fines and Data Breach Survey: January 2026
- Digital Personal Data Protection Act, 2023 - Sections 11–13, 17(2), 19, 33
- Digital Personal Data Protection Rules, 2025 - notified 13 November 2025
- Court of Justice of the European Union - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18
- Regulation (EU) 2016/679 (GDPR) - Articles 45, 52
- European Data Protection Supervisor - Annual Report 2024 (published April 2025)
- Observer Research Foundation - The Adequacy Dilemma: India's DPDPA and the GDPR (June 2025)
- Vidhi Centre for Legal Policy - A Curious Case of EDPS's Refusal (September 2025)
- DPDPA.com - India–EU Data Adequacy: Pathway Analysis (February 2026)
- European Commission, India–EU BTIA Fact Sheet, January 2026
- Ministry of Commerce & Industry, Government of India, FTA Summary, January 2026;
- Eurostat, EU–India Bilateral Trade Statistics, 2024.
- India–EU BTIA Digital Trade Chapter, Text as concluded 27 January 2026;
- DPIIT, India Digital Economy Report 2025;
- European Commission, Digital Single Market Economic Report 2024.
- European Commission, India–EU Broad-based Trade and Investment Agreement (BTIA) Fact Sheet, January 2026.
- Ministry of Commerce and Industry, India–EU FTA Summary Note, January 2026.
- Eurostat, EU–India Bilateral Trade Statistics, 2024.
- Department for Promotion of Industry and Internal Trade, India Digital Economy Estimates, 2025.
- *European Commission, Digital Single Market Economic Report, 2024.*
- *India–EU BTIA Digital Trade Chapter, Text as concluded, 27 January 2026.*
- NASSCOM, *Indian Tech Talent in Europe Report, 2024.*
- *Eurostat, EU Work Permit and Migration Statistics, 2024.*
- *India–EU BTIA Mode 4 Annex, Text as Concluded, 27 January 2026.*
- NASSCOM, *GCC Landscape Report, 2024.*
- *Mercer, Total Remuneration Survey India, 2024.*

- Korn Ferry, Global Salary Survey, 2024.
- Deloitte, India GCC Compliance Cost Benchmarking, 2025.
- KPMG, Data Protection Implementation Survey, 2025.
- CMS, GDPR Enforcement Tracker, 6th Edition, March 2025.
- Digital Personal Data Protection Act, 2023 (India).
- Regulation (EU) 2016/679 (GDPR).
- Ministry of Commerce and Industry, Special Economic Zones Policy Overview, 2025.
- Special Economic Zones Act, 2005 (India).
- Income Tax Act, 1961 - Section 10AA.
- Integrated Goods and Services Tax Act, 2017 (India).
- Government of Karnataka, GCC Policy, 2022.
- Government of Maharashtra, IT & ITES Policy, 2023.
- Government of Telangana, ICT Policy, 2022.
- Government of Tamil Nadu, GCC Policy, 2023.
- Government of Andhra Pradesh, Sunrise AP 2.0 Policy, 2024.
- Department for Promotion of Industry and Internal Trade, GCC Policy Framework, 2023.
- Ministry of Electronics and Information Technology, PLI Scheme for IT Hardware, 2021.
- Government of India, IndiaAI Mission - Cabinet Approval Note, March 2024.
- Department for Promotion of Industry and Internal Trade, National Data Governance Framework Policy, 2022.
- Startup India, GCC–Startup Connect Programme Overview, 2024.

Inductus GCC Service Models

India's Leading GCC Enabler

BOT (Build-Operate-Transfer)

A structured pathway to establishing your GCC with minimized risk and maximum efficiency. We **build** and **operationalize** your center, ensuring seamless performance before **transferring full ownership** to you—**equipping your business with a mature, self-sustaining capability.**

COPO (Company-Owned, Partner-Operated)

Maintain **full ownership** while leveraging Inductus' operational expertise. This model enables you to establish a GCC with **absolute control over intellectual assets (IP), agility**, **and scalability** while we manage day-to-day operations, **ensuring zero liability, compliance, and maximum efficiency**.
Additionally, a **Zero Capex Model** with **Digital Twin or a Mirror Like Operational Structure** with superior process excellence.

FLEXI (Adaptive & Custom GCC Solutions)

Beyond predefined structures, **Flexi is a bespoke model offering absolute customization and adaptability.**

It molds itself around your unique business prerequisites, evolving seamlessly with your vision. **This isn't just a service—it's an agile, high-impact partnership crafted to maximize your success.**

Proud recipient of **Times Power Icons Award** for being one of the **Leading GCC Enabler of India**

Presented by Bennett & Coleman THE TIMES OF INDIA

Inductus ensures that each model is executed with precision, innovation, and strategic foresight—helping you unlock the full potential of your GCC in India.

Our deep expertise in GCCs, coupled with a strong network of industry partnerships and policy-level advisory, positions us as a trusted partner for driving transformational outcomes.

Certificate of Excellence' for Consulting & Advisory Services by **Chicago Open University USA**

+91-92346-92346 gcc@inductusgroup.com www.indcutusgcc.com

COPO & Digital Twin Integrated Service Model

A study based proposition to build a global standard GCC mechanism for Large & Mid-sized Corporations

> *"In a world full of rapid tech & process disruptions, global corporations that invest in innovation-led R&D don't just survive—they lead. Innovation is the key to staying relevant, cost-competitive, and future-ready in an ever-evolving marketplace..."*
>
> **Alouk Kumar** - CEO, Inductus

Inductus GCC's Digital Twin and COPO (Company-Owned, Partner-Operated) Service Model creates a seamless, future-ready operational framework for global businesses setting up GCCs in India. The Digital Twin Process ensures real-time collaboration, decision-making, and operational efficiency by replicating physical systems in a virtual environment, enabling synchronized execution across multiple time zones. Meanwhile, the COPO Model allows MNCs to retain full ownership and strategic control while leveraging Inductus' expertise for execution, compliance, and scalability.

This hybrid approach optimizes costs, mitigates risks, and accelerates GCC growth, ensuring innovation-driven operations with minimal liabilities and maximum efficiency.

Designed to be Different.

www.inductusgcc.com