SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

GDPR

EU General Data Protection Regulation (EU) 2016/679 · with an India lens

Requirements, Implementation Guidance & Audit Testing Procedures

DOCUMENT ID	VERSION	STATUS
SRIDA-GDPR-RTP-001	1.0	Final — Approved for Publication

Rajendra Bodda
Chief Information Security Officer (CISO)
Srida IT · 2026

Independent professional guidance.
Not legal advice.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT



EU General Data Protection Regulation (GDPR) — with an India Lens

Requirements, Implementation Guidance & Audit Testing Procedures

SAMPLE

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

Published by Srida IT

SRIDA-GDPR-RTP-001 · Version 1.0 · November 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not an official publication of the European Union, the European Data Protection Board or any supervisory authority, is not legal advice, and does not confer any certification. Only the GDPR as published in the Official Journal of the European Union is authentic.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

Document Information and Control

Field	Value
Document title	EU General Data Protection Regulation (GDPR) — with an India Lens
Subtitle	Requirements, Implementation Guidance & Audit Testing Procedures
Document identifier	SRIDA-GDPR-RTP-001
Version	1.0
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	November 2026
Reference document	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88
Related documents	Digital Personal Data Protection Act, 2023 (India); DPDP Rules, 2025; Commission Implementing Decision (EU) 2021/914 (standard contractual clauses); ISO/IEC 27701:2025; ISO/IEC 27001:2022
Companion publications	SRIDA-DPDP-RTP-001; SRIDA-PIMS-27701-RTP-001; SRIDA-ISMS-27001-RTP-001; SRIDA-AIMS-42001-RTP-001
Next review	On significant EDPB guidance, case law or amendment, and at least annually

SAMPLE

Version history

Version	Date	Author	Description of change
1.0	November 2026	Rajendra Bodda	First published edition, approved for publication.

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	10 November 2026

Distribution

Released for publication by Srida IT. Distribution and use are subject to the permitted-use terms in the Copyright, Legal and Usage Notices.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

Table of Contents

Part I Foundations 14

Chapter 1 Introduction to the GDPR 15
Chapter 2 Structure, Recitals, Guidance and Enforcement 19
Chapter 3 Material and Territorial Scope 23
Chapter 4 Key Concepts 28
Chapter 5 The GDPR, the DPDP Act and Related Standards 33
Chapter 6 Terminology and Abbreviations 37
Chapter 7 How to Use This Manual and the Audit Method 41

Part II GDPR Requirements 45

Chapter 8 Scope and Principles (Chapters I–II) 46
Art. 3 Territorial scope 47
Art. 5 Principles relating to processing of personal data 53
Art. 6 Lawfulness of processing 59
Art. 7 Conditions for consent 66
Art. 8 Conditions applicable to child's consent in relation to information society services 72
Art. 9 Processing of special categories of personal data 77
Art. 10 Processing of personal data relating to criminal convictions and offences 84
Art. 11 Processing which does not require identification 89
Chapter 9 Transparency and Access (Chapter III, Sections 1–2) 94
Art. 12 Transparent information, communication and modalities for the exercise of the rights of the data subject 95
Art. 13 Information to be provided where personal data are collected from the data subject 102
Art. 14 Information to be provided where personal data have not been obtained from the data subject 108
Art. 15 Right of access by the data subject 114
Chapter 10 Rectification, Erasure, Objection and Automated Decisions (Chapter III, Sections 3–5) 121
Art. 16 Right to rectification 122
Art. 17 Right to erasure ('right to be forgotten') 127
Art. 18 Right to restriction of processing 134
Art. 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing 139
Art. 20 Right to data portability 143
Art. 21 Right to object 148
Art. 22 Automated individual decision-making, including profiling 154
Art. 23 Restrictions 161
Chapter 11 Controller and Processor Obligations (Chapter IV, Section 1) 167
Art. 24 Responsibility of the controller 168
Art. 25 Data protection by design and by default 174
Art. 26 Joint controllers 181
Art. 27 Representatives of controllers or processors not established in the Union 186
Art. 28 Processor 192
Art. 29 Processing under the authority of the controller or processor 201
Art. 30 Records of processing activities 206
Art. 31 Cooperation with the supervisory authority 213
Chapter 12 Security of Personal Data and Breach Notification (Chapter IV, Section 2) 218
Art. 32 Security of processing 219
Art. 33 Notification of a personal data breach to the supervisory authority 226
Art. 34 Communication of a personal data breach to the data subject 233
Chapter 13 DPIA, Prior Consultation and the Data Protection Officer (Chapter IV, Sections 3–4) 239
Art. 35 Data protection impact assessment 240

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

Art. 36 Prior consultation 247
Art. 37 Designation of the data protection officer 252
Art. 38 Position of the data protection officer 258
Art. 39 Tasks of the data protection officer 263

Chapter 14 **Codes of Conduct and Certification (Chapter IV, Section 5)** 268
Art. 40 Codes of conduct 269
Art. 41 Monitoring of approved codes of conduct 276
Art. 42 Certification 281
Art. 43 Certification bodies 287

Chapter 15 **International Transfers (Chapter V)** 292
Art. 44 General principle for transfers 293
Art. 45 Transfers on the basis of an adequacy decision 299
Art. 46 Transfers subject to appropriate safeguards 305
Art. 47 Binding corporate rules 312
Art. 48 Transfers or disclosures not authorised by Union law 318
Art. 49 Derogations for specific situations 323

Chapter 16 **Specific Processing Situations (Chapter IX)** 329
Art. 88 Processing in the context of employment 330
Art. 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes 336

Part III Implementation 342

Chapter 17 **Programme Roadmap for Indian Organisations** 343
Chapter 18 **Data Mapping and Records of Processing** 348
Chapter 19 **Lawful Basis, Consent and Legitimate-Interests Assessments** 352
Chapter 20 **Data Subject Rights Operations** 356
Chapter 21 **DPIA in Practice** 360
Chapter 22 **Processors, Sub-processors and Article 28 Contracts** 364
Chapter 23 **International Transfers to India: SCCs, TIAs and Supplementary Measures** 368
Chapter 24 **Breach Management and the 72-Hour Clock** 373
Chapter 25 **Security of Processing with ISO/IEC 27001 and 27701** 377
Chapter 26 **Supervisory Authorities, Remedies and Fines** 381

Part IV Audit and Assurance 385

Chapter 27 **Internal GDPR Audit Programme** 386
Chapter 28 **Audit Techniques and Evidence** 391
Chapter 29 **Findings and Corrective Action** 396
Chapter 30 **Certification, Codes of Conduct and Assurance** 400

Part V Appendices and Templates 404

Appendix A **Article Applicability Matrix** 405
Appendix B **Entry Summary Matrix** 423
Appendix C **RoPA Templates** 427
Appendix D **DPIA Template** 431
Appendix E **Data Subject Request Log and Procedure** 435
Appendix F **Breach Register and Notification Templates** 439
Appendix G **Article 28 DPA Checklist** 444
Appendix H **Transfer Impact Assessment Template** 449
Appendix I **Lawful Basis Register and LIA Template** 454

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

CHAPTER 1

Introduction to the GDPR

The General Data Protection Regulation, formally “Regulation (EU) 2016/679 of the European Parliament and of the Council”, is the European Union's principal law on the processing of personal data about living individuals. It sets the rules that organisations must follow when they collect, use, store, share or delete information about people, and it gives those people enforceable rights over that information. It is published in the Official Journal of the European Union, L 119, of 4 May 2016, and it is cited throughout this manual simply as "the GDPR".

This chapter explains what the GDPR is, where it came from, why it matters to organisations in India, and what this manual adds to the official text. It is an orientation chapter. The detailed requirements, interpretation and testing procedures are in Part II, and the practical implementation guidance is in Part III.

1.1 What the GDPR is

Article 1 sets out two objectives that sit side by side. The first is the protection of natural persons when their personal data is processed, which the Regulation frames as a fundamental right. The second is the free movement of personal data within the Union: Article 1(3) states that the free flow of data between Member States must not be restricted or prohibited on data protection grounds. The GDPR is therefore both a rights instrument and an internal-market instrument. An auditor who forgets either half will misread the text.

The rights dimension is anchored in EU primary law. Recital 1 refers to Article 8(1) of the EU Charter of Fundamental Rights and Article 16(1) TFEU, both of which recognise a right to the protection of personal data. This anchoring explains why the GDPR uses the language of rights, risks to “rights and freedoms of natural persons”, proportionality and accountability, rather than the language of a narrow technical or sectoral rulebook.

The GDPR is a **regulation**, not a directive. Under EU law a regulation is binding in its entirety and directly applicable in every Member State without national transposition; the closing formula of the GDPR says exactly that. A directive, by contrast, sets objectives that each Member State implements through its own legislation. The practical consequence is a single text that applies across the Union, although, as Chapter 2 explains, the GDPR leaves a number of matters to Member State law and the national picture is not entirely uniform.

SAMPLE

The GDPR is also technology-neutral. Recital 15 indicates that protection should not depend on the techniques used, and Article 2(1) applies the Regulation to automated processing and to manual records that form part of, or are intended to form part of, a filing system. A paper HR file in a structured cabinet can be within scope just as much as a cloud database.

1.2 History and timeline

The GDPR replaced Directive 95/46/EC, the Data Protection Directive of 24 October 1995. The Directive harmonised data protection rules to a degree, but each Member State implemented it differently, and Recital 9 records that this fragmentation produced legal uncertainty and uneven protection. The Directive also predated cloud computing, social media, smartphones and large-scale online tracking. Recitals 6 and 7 describe the pressure that rapid technological change and globalisation placed on the old framework and the need for a stronger, more coherent one.

The legislative milestones that can be read from the Regulation itself are set out in the table below. Earlier milestones (the Commission's proposal and the political agreement) are well documented elsewhere but are not reproduced here.

Table 1-1. GDPR milestones as stated in the Official Journal text

Date	Event	Source in the text
12 March 2014	European Parliament first-reading position	Footnote 3 to the citations
8 April 2016	Council position at first reading	Footnote 3
14 April 2016	European Parliament position (second reading)	Footnote 3
27 April 2016	Regulation adopted and signed at Brussels	Title and signature block
4 May 2016	Published in the Official Journal, L 119	OJ header
24 May 2016	Entry into force: the twentieth day after publication	Art. 99(1)
25 May 2018	Date of application; Directive 95/46/EC repealed from the same date	Arts. 94(1), 99(2)

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

Date	Event	Source in the text
25 May 2020, then every four years	Commission evaluation reports	Art. 97(1)

The two-year gap between entry into force and application was a transition period. Recital 171 indicates that processing already under way had to be brought into line within that period, and that consent obtained under the Directive did not need to be collected again if it already met the GDPR's conditions. Commission decisions and supervisory authority authorisations adopted under the Directive remain in force until amended, replaced or repealed, which matters for older adequacy decisions (Chapter 15).

Article 94(2) also provides that references to the Article 29 Working Party, the advisory group of national authorities under the Directive, are to be read as references to the European Data Protection Board (EDPB). Some Working Party guidance was later endorsed by the EDPB; which documents were endorsed is a detail to check at the point of use.

A corrigendum to the GDPR was published in 2018. It corrects language errors but is not part of the source text used for this edition; readers who rely on precise wording should check the corrected consolidated text on EUR-Lex.

1.3 What the GDPR changed

Compared with the Directive, the GDPR introduced or strengthened several features that shape every chapter of this manual:

- **Accountability.** Article 5(2) makes the controller responsible for compliance with the principles and able to demonstrate it. Compliance is not presumed; it must be evidenced. This is the reason an audit method is meaningful at all.
- **Extraterritorial reach.** Article 3(2) applies the Regulation to controllers and processors outside the Union that offer goods or services to people in the Union or monitor their behaviour there. This is the main route by which Indian organisations without an EU presence are drawn in (Chapter 3).
- **Direct processor obligations.** Processors now carry their own duties, including records of processing (Art. 30(2)), security (Art. 32), breach notification to the controller (Art. 33(2)) and transfer rules (Chapter V), and they can be fined directly.
- **Risk-based tools.** Data protection by design and by default (Art. 25), data protection impact assessments (Art. 35) and the designation of data protection officers (Art. 37) require organisations to anticipate risk rather than react to it.
- **Breach notification.** A general obligation to notify the supervisory authority, where feasible within 72 hours of becoming aware of a personal data breach, unless it is unlikely to result in a risk (Art. 33), and to inform data subjects where the risk is high (Art. 34).
- **Stronger rights.** New or expanded rights to erasure, portability and objection, and safeguards around solely automated decision-making (Arts. 17, 20, 21, 22).
- **Consistency and cooperation.** A one-stop-shop mechanism for cross-border processing and the EDPB as a Union body to secure consistent application (Chapters VI and VII).
- **Significant fines.** Two tiers of administrative fines in Article 83, up to EUR 10 million or 2% of total worldwide annual turnover, and up to EUR 20 million or 4%, whichever is higher in each case for undertakings.

1.4 Why the GDPR matters to Indian organisations

India has its own data protection law, the Digital Personal Data Protection Act, 2023 (the DPDP Act), with the Digital Personal Data Protection Rules, 2025. The DPDP Act does not displace the GDPR for activities that fall within the GDPR's scope, and the GDPR does not displace the DPDP Act for activities within India's. Many Indian organisations will need to satisfy both. The GDPR can reach an Indian organisation in four common ways, each examined in Chapter 3 against the factual tests of Articles 2 and 3:

1. **Serving people in the EU directly.** An Indian SaaS company, e-commerce brand, travel platform, education provider or mobile app that targets customers or users in the Union, for example through EU-language storefronts, euro pricing or EU delivery, may fall within Article 3(2)(a). An organisation that tracks or profiles the online behaviour of people in the Union, for example through behavioural advertising or analytics, may fall within Article 3(2)(b).
2. **Processing on behalf of EU clients.** India's IT services, BPO, KPO, payroll, software engineering and global capability centre sectors process very large volumes of EU personal data as processors or sub-processors. The EU controller remains subject to the GDPR and must flow down Article 28 terms and Chapter V transfer safeguards. Whether the Indian processor is itself directly subject to the GDPR depends on the facts; in practice its contracts will impose GDPR-derived obligations either way.
3. **Being part of an EU group.** An Indian subsidiary, branch or captive centre of a group with EU establishments may process data in the context of the activities of an EU establishment (Art. 3(1)), may act as a processor or joint controller for EU group companies, and will usually be bound by intra-group transfer arrangements such as standard contractual clauses or binding corporate rules.
4. **Receiving data transferred from the EU.** India does not, at the date of this edition, hold an EU adequacy decision under Article 45. Every transfer of personal data from the EU or EEA into India therefore needs another Chapter V route, typically standard

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

GDPR ARTICLE 28 · CHAPTER IV · SECTION 1

Processor

GDPR requirement · Controller, Controller and processor, Processor | WP-Art28

A Requirement Reference

Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016, Article 28 — Processor

Controller and processor · General obligations

Summaries are in Srida IT's own words; short quotations are marked. Only the Official Journal text is authentic.

Paragraph	Applies to	What it requires (Srida IT summary)
28(1)	CONTROLLER	A controller may hand processing to a processor only if that processor gives **sufficient guarantees** that it will apply technical and organisational measures good enough for the processing to meet the GDPR and protect data subjects' rights. The duty is one of selection and continuing reliance: the controller must be able to show why it trusted the processor.
28(2)	PROCESSOR	A processor may not bring in another processor (a sub-processor) without the controller's prior written authorisation, which may be **specific** (named sub-processor) or **general**. Under a general authorisation the processor must tell the controller in advance about any planned addition or replacement so that the controller has a real chance to object.
28(3)	CONTROLLER AND PROCESSOR	Processing by a processor must rest on a contract or other legal act under EU or Member State law that binds the processor to the controller and describes the processing: subject-matter, duration, nature, purpose, types of personal data, categories of data subjects, and the controller's rights and obligations. The contract must contain at least the eight terms in points (a) to (h).
28(3)(a)	PROCESSOR	The processor acts only on the controller's **documented instructions**, including on transfers to third countries or international organisations. The sole exception is a requirement of EU or Member State law binding the processor; the processor must then tell the controller before processing, unless that law forbids it on important public-interest grounds.

© 2026 Srida IT · Version 1.0 · Independent guidance, not legal advice

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

Paragraph	Applies to	What it requires (Srida IT summary)
28(3)(b)	**PROCESSOR**	Everyone the processor authorises to handle the data must be bound to confidentiality, either by a signed commitment or by a suitable statutory duty.
28(3)(c)	**PROCESSOR**	The processor takes every security measure that Art. 32 requires. The contract usually does this by attaching a schedule of technical and organisational measures (TOMs).
28(3)(d)	**PROCESSOR**	The processor respects the conditions in 28(2) and 28(4) for engaging sub-processors (authorisation, notice of change, flow-down and continuing liability).
28(3)(e)	**PROCESSOR**	Allowing for the nature of the processing and so far as possible, the processor helps the controller, through appropriate technical and organisational measures, to answer data subject requests under Chapter III (Arts. 12–22).
28(3)(f)	**PROCESSOR**	Allowing for the nature of the processing and the information it holds, the processor helps the controller meet Arts. 32–36: security, breach notification to the authority and to individuals, DPIAs and prior consultation.
28(3)(g)	**PROCESSOR**	When the services end, the processor deletes or returns all personal data, as the controller chooses, and deletes remaining copies, unless EU or Member State law requires the data to be kept.
28(3)(h)	**PROCESSOR**	The processor gives the controller all information needed to show compliance with Art. 28, and allows and contributes to audits, **including inspections**, by the controller or an auditor the controller mandates.
28(3) second subparagraph	**PROCESSOR**	The processor must tell the controller straight away if it believes an instruction breaches the GDPR or other EU or Member State data protection law. The text attaches this duty to point (h).

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

Paragraph	Applies to	What it requires (Srida IT summary)
28(4)	PROCESSOR	A processor that engages a sub-processor must impose on it, by contract or other legal act, the same data protection obligations as those in its own contract with the controller, in particular sufficient guarantees on technical and organisational measures. If the sub-processor fails, the initial processor stays **fully liable** to the controller.
28(5)	PROCESSOR	Adherence to an approved code of conduct (Art. 40) or approved certification mechanism (Art. 42) can be used as one element to show sufficient guarantees under 28(1) and 28(4).
28(6)	CONTROLLER AND PROCESSOR	The contract may be built wholly or partly on standard contractual clauses adopted under 28(7) or 28(8), including where those clauses form part of a certification under Arts. 42–43; parties remain free to use an individual contract.
28(7)	CONTROLLER AND PROCESSOR	The Commission may adopt standard contractual clauses covering the matters in 28(3) and 28(4) (examination procedure, Art. 93(2)).
28(8)	CONTROLLER AND PROCESSOR	A supervisory authority may adopt such clauses through the consistency mechanism (Art. 63).
28(9)	CONTROLLER AND PROCESSOR	The contract or legal act under 28(3) and 28(4) must be in writing; electronic form is acceptable.
28(10)	PROCESSOR	A processor that breaches the GDPR by deciding the purposes and means of processing is treated as a **controller** for that processing, without prejudice to liability, fines and penalties under Arts. 82, 83 and 84.

B Recitals and Guidance

Key recitals

Recital 79, Recital 81, Recital 74, Recital 82

Guidance and case law

- EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Part II, Art. 28 contract content, sub-processors and the processor-to-controller shift)
- Commission Implementing Decision (EU) 2021/915 on standard contractual clauses between controllers and processors under Art. 28(7)
- Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for transfers to third countries (Modules Two and Three for controller-to-processor and processor-to-processor transfers)
- EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), on when a non-EU processor is itself subject to the Regulation

© 2026 Srida IT · Version 1.0 · Independent guidance, not legal advice

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

C Administrative Fine Tier (Art. 83)

83(4)(a) — up to €10m or 2% of worldwide annual turnover, whichever is higher. Art. 83(4)(a) names the obligations of the controller **and the processor** under Arts. 25 to 39, so both parties are directly exposed. Under 28(10) a processor that becomes a controller can additionally face the 83(5) tier for infringements of, for example, Arts. 5, 6 or 44–49 in relation to that processing.

D Objective

To keep the controller in charge of processing it outsources. Art. 28 does this through three levers: careful selection of processors that can prove sufficient guarantees, a written contract that fixes the scope of processing and imports a minimum set of GDPR protections, and a chain of authorisation and flow-down so that the protections survive every hop down the supply chain. It also stops a processor from quietly turning client data to its own ends by reclassifying it as a controller when it does.

E Interpretation

Two-sided duties. Art. 28 is often read as a controller's procurement rule, but several obligations sit squarely on the processor: no sub-processing without authorisation (28(2)), flow-down and continuing liability (28(4)), written form (28(9)) and the controller reclassification in 28(10). Art. 83(4)(a) makes the processor's own Art. 28 failures fineable. The contract must be “binding on the processor with regard to the controller”, so the GDPR requirement is a mutually executed instrument, not a policy the processor publishes. EDPB guidance expects both parties to share responsibility for ensuring that a compliant contract exists. Srida IT practice treats an unsigned or expired DPA as a failure by both the controller and the processor.

Specific content, not a copy of the article. Art. 28(3) requires the contract to describe the actual processing: subject-matter, duration, nature and purpose, data types and data subject categories. A DPA that merely repeats points (a) to (h) with no processing annex does not let anyone tell what the processor is permitted to do. EDPB guidance indicates that restating the Regulation is not enough and that the contract should say how each obligation will be met, for example through a TOMs schedule and a defined assistance procedure. Srida IT recommends one processing annex per service line or statement of work, kept under change control.

Documented instructions and the foreign-law trap. Under 28(3)(a) the processor may deviate from instructions only where **EU or Member State** law requires it. Indian law is neither. A demand from an Indian authority, court or regulator (for example a production order or a direction under the Information Technology Act, 2000 and the CERT-In Directions of April 2022) is therefore not a legal-requirement exception under Art. 28; it is a conflict to be managed under the transfer instrument (the government-access clauses of the 2021 SCCs) and Art. 48. Instructions include the transfer decision: an Indian processor that moves EU client data to a US tool or a Singapore data centre without a documented instruction breaches 28(3)(a) even if the security is excellent. Instructions may be documented in the master agreement, statements of work, configuration baselines and authorised tickets; what matters is that they are traceable and that the processor can show processing stayed inside them.

SAMPLE

Sub-processors and flow-down. 28(2) offers a choice between specific and general written authorisation. General authorisation is common in IT services because tooling changes often, but it only works if the processor gives advance notice of each addition or replacement and the controller can genuinely object; a notice published on a web page that no one at the controller monitors is weak evidence. The text does not fix a notice period or say what happens if the controller objects; contracts must fill that gap (Srida IT suggests 30 days' notice and a termination or alternative-provider right). 28(4) requires the **same** data protection obligations to be imposed on the sub-processor; EDPB guidance reads this as the same level of protection rather than identical wording. The chain is recursive: a sub-processor's own sub-processors need the same treatment. Intra-group entities, such as the Indian delivery centre of a European IT group, are sub-processors like any other and need authorisation and a flow-down contract.

Audits and inspections. 28(3)(h) gives the controller a right to information and to audits, explicitly including inspections, by itself or a mandated auditor. Processors commonly offer ISO/IEC 27001 certificates or independent assurance reports instead of on-site audits. Srida IT's view is that such reports can satisfy most information requests and reasonable conditions on audits (notice, frequency, confidentiality, cost) are acceptable, but a clause that removes the inspection right altogether, or makes it conditional on the processor's consent, is not consistent with the text. The duty to flag infringing instructions sits, oddly, after point (h); practitioners treat it as a free-standing processor obligation.

Processor turned controller. 28(10) bites when a processor decides why and how data are processed for its own ends: an Indian contact centre that uses an EU client's call recordings to train its own speech-analytics model, a SaaS vendor that pools tenant data to benchmark or sell insight, or an analytics firm that reuses client data to build marketing segments. For that processing the processor becomes a controller and needs its own lawful basis, transparency and rights handling, which it almost never has. EDPB guidance distinguishes decisions on **essential** means (which data, how long, who gets access) reserved to the controller from **non-essential** technical means (hardware, software choices) that a processor may make without becoming a controller.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT

F India Lens

Art. 28 is the single most important GDPR article for Indian IT, ITeS and BPO firms, because their typical role for EU clients is that of processor or sub-processor. Whether the GDPR applies to the Indian firm **directly** depends on the factual test in Art. 3: an EU establishment (Art. 3(1)), or processing related to offering goods or services to, or monitoring, people in the EU (Art. 3(2)). EDPB guidance on territorial scope suggests that a non-EU processor is not brought within the GDPR merely because it serves an EU controller; even so, Art. 28 reaches it **contractually**, because the EU controller must impose the 28(3) terms and, since India has no EU adequacy decision, must also put a Chapter V transfer tool in place, usually the 2021 SCCs Module Two (controller to processor) or Module Three (processor to processor) with a transfer impact assessment. Indian subsidiaries of EU groups acting as captive delivery centres are sub-processors of the group entities and need intra-group DPAs and authorisation. In practice an Indian processor should: keep a client-by-client register of DPAs and instructions; publish and maintain an accurate sub-processor list with a change-notification workflow; flow down obligations to every Indian and overseas vendor that touches client data; map Indian-law obligations (CERT-In incident reporting and log retention, DPDP Rules log retention, court orders) that could conflict with instructions and disclose them to clients before signing; and police secondary use of client data to stay out of 28(10).

G DPDP Act Crosswalk

- DPDP Act s.8(2) — a Data Fiduciary may engage a Data Processor only under a **valid contract**, which parallels 28(3). Difference: the Act does not list mandatory contract terms like 28(3)(a)–(h), does not regulate sub-processing and has no equivalent of the 28(10) reclassification; the content is left to the parties and to the Rules.
- DPDP Act s.8(1) and s.8(5) with DPDP Rules r.6(1)(f) — the Data Fiduciary remains responsible for processing done on its behalf, must take reasonable security safeguards covering its Data Processor, and r.6(1)(f) requires the fiduciary–processor contract to provide for such safeguards. Difference: under the GDPR the processor carries its own fineable duties (Art. 83(4)(a)); the DPDP Act places obligations chiefly on the Data Fiduciary. Most Rules obligations, including r.6, apply from 13 May 2027.
- DPDP Act s.8(7)(b) and Rules r.8(3) — the fiduciary must cause its processor to erase data when the purpose ends, but r.8(3) also requires personal data, traffic data and processing logs to be retained for at least one year, including for processing by a processor. Difference: 28(3)(g) lets the controller choose deletion or return at the end of service and only Union or Member State law can override; an Indian processor serving both regimes must segregate DPDP-scope and GDPR-scope data and settle retention in the contract.
- DPDP Act s.17(1)(d) — processing in India of personal data of Data Principals outside India, under a contract with a person outside India, is exempt from most of Chapter II (except s.8(1) and s.8(5)), Chapter III and s.16. Difference: this exemption does nothing to relieve an Indian processor of its Art. 28 contractual obligations to EU clients; mapping is not compliance, and the GDPR terms continue to apply through the contract and SCCs.

Indicative comparison only; complying with one law does not by itself establish compliance with the other.

SAMPLE

H Applicability

Applies whenever a controller subject to the GDPR has personal data processed on its behalf by another person, and to every subsequent link in the processing chain. There is no size threshold and no exemption for intra-group processing, free services or cloud services offered on standard terms. Art. 28 does not apply where the service provider is itself a controller (for example a statutory auditor, a bank processing payments for its own purposes, or a recruitment agency acting for itself) or where two parties jointly decide purposes and means (Art. 26). Characterisation is factual: a contract labelling a party as a processor does not settle the matter if it in fact decides purposes. For non-EU processors, direct application depends on Art. 3; contractual application through the controller's 28(3) terms and Chapter V transfer tools is near universal.

I Implementation Guidance

1. **Characterise every relationship.** For each vendor or client, record whether the party is a controller, joint controller, processor or sub-processor, and the facts supporting the call (who sets purposes, who decides essential means). Re-test when services change.
2. **Due diligence before onboarding (28(1), 28(5)).** Use a risk-tiered questionnaire covering security (Art. 32), sub-processors, locations and transfers, breach handling, rights assistance, staff vetting, certifications and codes. Record the decision and residual risk; refresh annually for high-risk processors.
3. **Standard DPA with a processing annex (28(3), 28(9)).** Adopt a template that covers (a)–(h) and the infringing-instruction duty, with annexes for processing details, TOMs, approved sub-processors and transfer mechanism. The 2021/915 clauses may be used as a base. Execute before any data flows; store signed copies centrally.
4. **Instruction management (28(3)(a)).** Define authorised instruction channels and approvers on both sides. Processors keep an instruction register linked to change tickets, and a procedure to escalate instructions believed to infringe data protection law.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gdpr · © 2026 Srida IT