SmartSuite

Framework / Privacy / Global Privacy Regulations

India IT (RSPP & SPDI) Rules, 2011

The IT (RSPP & SPDI) Rules, 2011 (G.S.R. 313(E)) set consent, disclosure, transfer and reasonable security duties for companies holding sensitive personal data in India.



What it is

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (G.S.R. 313(E)) require a body corporate that holds sensitive personal data or information to publish a privacy policy, obtain written consent before collecting the data, limit its disclosure and transfer, and keep reasonable security practices. The Central Government made them on April 11, 2011 under section 87(2)(ob) read with section 43A of the Information Technology Act, 2000, and they came into force on publication in the Gazette (Rule 1).

The Rules apply to a body corporate, and a person acting on its behalf, that collects, receives, possesses, stores, deals with or handles information (Rule 4(1)). “Body corporate” has its section 43A meaning: any company, including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities (Rule 2(1)(c)).

At a glance

PUBLISHER
Government of India, Department of Information Technology (Ministry of Communications and Information Technology)

TYPE
Regulation

VERSION
Rules, 2011 (G.S.R. 313(E))

EFFECTIVE
April 11, 2011 (on publication in the Gazette of India)

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
India

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: wipo.int/wipolex/en/text/494931

Why it matters

- **A named security standard** Rule 8(2) names IS/ISO/IEC 27001 as one standard that meets the reasonable security requirement.
- **A deemed compliance route** A body corporate that has implemented IS/ISO/IEC 27001, or codes of practice approved and notified by the Central Government, is deemed compliant if the standard or codes are certified or audited regularly by an independent auditor approved by the Central Government (Rule 8(4)).
- **Written consent tied to purpose** Consent in writing about the purpose of use is required before collection, and the information may be used only for that purpose (Rule 5(1) and (5)).
- **A grievance clock** A Grievance Officer's name and contact details are published on the website, and grievances are redressed within one month (Rule 5(9)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports IT (RSPP & SPDI) Rules 2011

Sensitive Data Inventory

Record which Rule 3 categories each system, vendor and process holds, and the lawful purpose for each.

Privacy Policy Register

Check the published policy against the five Rule 4 content items and keep version history and the website publication date.

Written Consent and Purpose Records

Store consent received by letter, fax or email, the stated purpose, retention limit, correction requests and written withdrawals (Rule 5).

Grievance Officer Log

Track each grievance to its one-month deadline and keep the published Officer name and contact details current (Rule 5(9)).

Disclosure and Transfer Register

Record each third-party recipient, the permission or contract basis, government agency requests and the protection level of each transfer destination (Rules 6 and 7).

Information Security Program and Audit

Hold the documented program and policies, the ISO/IEC 27001 mapping, annual audit results and the evidence to show after a breach (Rule 8).

Common framework mappings

GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27018 | ISO 27701 | NIST Privacy Framework v1.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

India IT Rules, 2011

Defines reasonable security practices and procedures for sensitive personal data protection.

indiacode.gov.in/handle/123456789/510187

Frequently asked questions

Who must comply with the India IT (SPDI) Rules, 2011?

A body corporate, and any person acting on its behalf, that collects, receives, possesses, stores, deals with or handles personal information or sensitive personal data or information (Rule 4(1)). “Body corporate” means any company, including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities (section 43A, Explanation).

What counts as sensitive personal data or information?

Rule 3 lists passwords, financial information such as bank account, card or payment instrument details, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information, and details of those categories provided to or received by the body corporate. Information freely available in the public domain or furnished under the Right to Information Act, 2005 is excluded.

Is ISO/IEC 27001 mandatory under the Rules?

No. Rule 8(2) says IS/ISO/IEC 27001 is one standard for reasonable security practices. A body corporate may instead follow an industry code approved and notified by the Central Government (Rule 8(3)). Either route gives deemed compliance only if it is certified or audited regularly by an independent auditor approved by the Central Government, at least once a year (Rule 8(4)).

How must consent and grievances be handled?

Consent is obtained in writing by letter, fax or email on the purpose of use before sensitive personal data or information is collected (Rule 5(1)). Providers can withdraw consent in writing (Rule 5(7)). The body corporate designates a Grievance Officer, publishes the name and contact details on its website, and redresses grievances within one month of receipt (Rule 5(9)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Are the SPDI Rules still in force after the DPDP Act?

Section 44(2)(a) of the Digital Personal Data Protection Act, 2023 omits section 43A of the IT Act, and clause (c) omits section 87(2)(ob), under which these Rules were made. G.S.R. 843(E) brings Section 44(2) into force eighteen months after publication, in May 2027. The Act and the DPDP Rules, 2025 do not say what happens to the text of the 2011 Rules.

License included / downloadable: Yes The Rules are Indian subordinate legislation published in the Gazette of India. The text is free to read; the linked copy is hosted by WIPO Lex.

Full framework page and mappings: smartsuite.com/frameworks/india-it-rspp-spdi-rules-2011

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.