

Personal data handling and processing in India

India | August 28 2020



Click here to compare the answers in this article to hundreds of others



Legitimate processing of PII

Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner’s legal obligations or if the individual has provided consent?

Yes, sensitive personal data and information (SPDI) cannot be collected unless the information is collected for a lawful purpose connected with a function or activity of the party collecting or using the information and the collection of the SPDI is considered necessary for that purpose. Apart from this, there are also notice and consent requirements.

Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Section 43A of the IT Act and the privacy rules relate to SPDI, which has a narrower meaning than personal information. Personal information is referred to in section 72A of the IT Act.

Data handling responsibilities of owners of PII

Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

While collecting sensitive personal data and information (SPDI), the provider must be made aware through reasonable steps of the following:

- the fact that the information is being collected;
- the purpose for which it is collected;
- the intended recipients of the information; and
- the name and address of the agency collecting or retaining the information.

Consent must be obtained from the provider of the SPDI regarding purpose of usage before collection of the information. Further, of the three grounds on the basis of which disclosure of SPDI is permitted to a third party, one relates to the provider of the information agreeing to the same and another relates to it being permitted under a contract with the provider.

Exemption from notification

When is notice not required?

There is no exemption to providing notice. It may be noted, however, that the privacy rules may not apply where the parties have agreed on their own terms of reasonable security practices and procedures (RSPP). The privacy rules also do not appear to apply to transfer of SPDI from one entity to another as opposed to from an individual provider of his or her own information to a data processor. It should also be noted that the privacy rules do not apply to the government.

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

No, the privacy rules do not offer individuals any degree of choice or control over the use of their information, although consent is required as to the purpose of the use so the individual may simply refuse to permit the use of his or her SPDI or withdraw his or her consent later. The collecting party then has the option not to provide the goods or services for which the information was sought.

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The privacy rules deal with this only indirectly. In regard to currency, the SPDI cannot be retained for longer than is required for the purpose for which the information can lawfully be used or is otherwise required under any other law for the time it is in force. As regards accuracy, the provider of the information has the right to review the information it provided and correct any inaccuracy. However, this appears to relate only to information provided by the individual and not information collected separately.

Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, the privacy rules specify that the SPDI cannot be retained for longer than is required for the purpose for which the information can lawfully be used or is otherwise required under any other law currently in force.

Finality principle

Are the purposes for which PII can be used by owners restricted? Has the ‘finality principle’ been adopted?

Yes. SPDI cannot be collected unless:

- the information is collected for a lawful purpose connected with a function or activity of the party collecting or using the information;
- the collection of the SPDI is considered necessary for that purpose; and
- the information collected is used for the purpose for which it has been collected.

There is no requirement however that the purpose of use must be specific in its description.

Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The privacy rules do not provide for any exceptions or exclusions. The purpose of collection or usage must be mentioned in the privacy policy. Further, consent is required as to the purpose of usage. Strictly speaking, if the new purpose is not covered by the purpose for which consent was given, the SPDI cannot be used for the new purpose. Since consent is required as to the purpose of use, change in the purpose, whether through the privacy policy or otherwise, would require the consent of the provider of the information. It must be noted that the privacy rules do not require that the purpose must be described in specific terms. It would appear, therefore, that if consent is obtained for a broad purpose, this would be sufficient.

Law stated date

Correct on

Give the date on which the information above is accurate.

4 May 2020