MY
LEGAL
PARTNERS

www.mylegalpartners.com

Mandatory Privacy Policy

Every entity engaged in business or professional activity or otherwise processing personal information or sensitive personal information through its website in India is bound to have in place a privacy policy for handling or dealing in personal or sensitive personal information or data.

As envisaged under **Rule 4 of the IT Rules, 2011,** every entity must notify its privacy policy to the provider of information at the time of collecting information. In addition, law makes it mandatory for every entity to publish the privacy policy on its website.

Privacy policy is a legal document that discloses all the ways an entity gathers, uses, discloses, stores and manages information or data. It must mention whether the collected information is kept confidential, shared with partners or sold to others.

Privacy policy is a crucial document and should be drafted while keeping in mind the peculiarities of an entity. It must make mandatory disclosure and has to be in conformity with the Information Technology Act & Rules, other applicable laws and judgments passed by Courts in India.

Privacy Policy of every entity shall clearly provide for following information:

i. Clear and easily accessible statement of its Practice and policies
ii. Type of data or information collected
iii. Purpose of collection and usage of such information
iv. Disclosure of such information
v. Reasonable security practices and procedures

While drafting a privacy policy, the following nine principles of privacy should be kept in mind:

1. **Notice:** A data controller to notify all individuals of its information practices before collecting information from them.

2. **Choice and Consent:** Individuals divulging information must have a choice (opt-in/opt-out) with regard to providing personal information. No collection or processing of personal data should take place without consent. To be valid under privacy law, consent must be meaningful: voluntary, specific, informed, current and given by a person with capacity. It must be as easy to withdraw consent as to give it.

3. **Collection Limitation:** A data controller should collect only as much information as is directly necessary for the purposes identified for such collection.

4. **Purpose Limitation:** It requires that the collection or processing of information be restricted to only as much information as is adequate and relevant. It further states that the collection, procession, disclosure, usage of personal information by a data controller should be limited to the purpose notified and consented to and that any change in this purpose must be notified to the individual. After use of the information for the identified purpose it should be destroyed.

5. **Access and Correction:** This principle requires that data subjects have access to the data held about them, the ability to seek corrections, amendment, or deletion of such data in case of inaccuracy and the ability to confirm if a data controller is holding any information about them.

6. **Disclosure of Information:** According to this principle, the data subject (person whose information is taken) has the right to privacy. Data controller shall not publish or make public the personal information. Data controller is bound to adhere to the applicable laws.

7. **Security:** This principle requires that a data controller ensure the security of the collected personal information by implementing 'reasonable security standards' to protect from the risk of loss, unauthorized access, destruction, use, processing, storage, modification, de-anonymization (a strategy in which anonymous data is cross-referenced to identify the source) and unauthorized disclosure (either accidental or incidental).

8. **Openness:** This principle requires a data controller to make public all the information it can about the practices, procedures, policies and systems that it implements in order to comply with the National Privacy principles.

9. **Accountability:** The data controller shall be accountable to comply with measures that fulfil the other eight principles. It states that such measures should include mechanisms to implement privacy policies such as training and education, external and internal audits, etc.

You've been drafting your Privacy Policy all wrong if it ignores the above broad points. The Privacy Policy on your website is not magic and authorization to do anything that against the aforementioned broad points and applicable laws.

***