Data Privacy Law (India)

Rohas Nagpal
Asian School of Cyber Laws

The information in this book is provided for informational purposes only and does not constitute legal advice.

Established in 1999, Asian School of Cyber Laws is a global pioneer in cyber law and cyber crime investigation.

Rohas Nagpal is a lawyer by qualification, a cyber crime investigator by profession, a hacker at heart and a programmer by passion. He is the founder President of Asian School of Cyber Laws.

Rohas has assisted the Government of India in framing draft rules and regulations under the Information Technology Act.

He has authored several books in digital forensic investigation, technology law and financial law. One of his publications, the Cyber Crime Investigation Manual, has been referred to as a "bible for cyber crime investigators" by Times of India – the world's largest selling English newspaper.

He is also the author of the first ever Commentary on the Information Technology Act. He has also co-authored an Internet Draft titled Biometric based Digital Signature scheme, which proposes a method of using biometrics to generate keys for use in digital signature creation and verification.

Table of Contents

1. Introduction

The term *data protection laws* or *data privacy laws* applies to laws that regulate the collection, possession, dealing, handling, usage, transfer of information, relating to private individuals, held by body corporates[1].

The Indian law relating to data privacy is contained primarily in sections 43A and 72A of the *Information Technology Act* and the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* (referred to as Data Privacy Rules in this document).

The *Data Privacy Rules* apply to all those who collect, receive, possess, store, deal or handle information of individuals during the course of commercial or professional activities. These include companies, partnerships, associations, sole proprietorships etc. They also include professionals like doctors, lawyers, chartered accountants etc.

An indicative list of those covered by the *Data Privacy Rules* include:

1. Insurance companies in respect of information relating to their customers and employees.

2. Banks in respect of information relating to their customers and employees.

[1] Body corporate means "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

3. Hospitals in respect of information relating to their customers and employees.

4. All business organizations (manufacturing, trading etc) in respect of information relating to their employees.

5. Doctors, stock brokers and chartered accountants in respect of information relating to their clients.

6. Retails stores, restaurants, ecommerce companies that collect payment through debit cards, credit cards etc.

7. Call centers, BPOs, LPOs etc.

Personal Information[2] is a wider term and *sensitive personal data*[3] *or information* is a subset of personal information.

Personal information (PI) means any information that:

1. relates to a natural person, and
2. is capable of identifying such person.

Sensitive personal data or information (SPDI) of a person means personal information which consists of information relating to -

[2] Information includes data, message , text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.

[3] Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

1. password[4]
2. financial information such as Bank account or credit card or debit card or other payment instrument details
3. physical, physiological and mental health condition
4. sexual orientation
5. medical records and history
6. Biometric information[5]
7. any detail relating to the above as provided to body corporate for providing service
8. any of the information received by body corporate for processing, stored or processed under lawful contract or otherwise.

Information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 (or any other law) is not regarded as sensitive personal data or information.

[4] Password means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information.

[5] "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes.

2. Compensation for failure to protect data

Section 43A of the *Information Technology Act* penalizes body corporates, possessing, dealing or handling any sensitive personal data or information in a computer resource which they own, control or operate, if, they are:

1. negligent in implementing and maintaining reasonable security practices and procedures[6], and

2. wrongful loss or wrongful gain is caused because of this negligence to any person,

In such cases, the body corporate shall be liable to pay damages by way of compensation[7] to the person so affected. In case the claim for injury or damage does not exceed Rs 5 crore, the adjudicating officer exercises jurisdiction. The jurisdiction in respect of the claim for injury or damage exceeding Rs 5 crore vests with the competent court.

---

[6] Reasonable security practices and procedures are designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment. These may be specified either in (1) an agreement between the parties or (2) in any law. ISO 27001 (The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements") is one such approved standard.

[7] Simply put, compensation is the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim. Simply put, damages are the compensation for legal injury. Damages can be of various types: (1) Compensatory damages are allowed as a recompense for injury actually suffered (2) Consequential damages are consequential upon the act complained of (3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others (4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

3. Punishment for disclosure of information in breach of lawful contract

Section 72A of the *Information Technology Act* applies to any person (including an intermediary[8]) who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person. This person will be penalised if he discloses such material:

1. without the consent of the person concerned, or in breach of a lawful contract, and

2. with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

This section does not apply if the person reveals this information in compliance with any law.

> **Illustration:** Sameer works in a call-centre for a large bank. He has access to the financial records of all the customers of the bank. He comes to know that Pooja has fixed deposits worth Rs 2 crore. He passes on this information to his friend Siddharth, who starts threatening Pooja in order to extort money from her. Sameer would be liable under this section.

[8] Intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

Illustration: Sameer works in a call-centre for a large bank. He has access to the financial records of all the customers of the bank. One day, he is approached by the police who are seeking information about a suspected terrorist who happens to be a customer of the bank. Sameer hands over the banking records of this suspect to the police. He would not be liable under this section as he is acting in conformance with the law which requires everyone to assist the police.

SUMMARY OF 72A:

Acts penalized	(1) Disclosure of personal information about some other person (2) The disclosure must either be without consent or in breach of contract (3) There must be intention to cause wrongful loss or wrongful gain or knowledge that wrongful loss or wrongful gain may be caused
Punishment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation	(1) Police officer not below the rank of

authorities	Inspector (2) Controller (3) Officer authorised by Controller under section 28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused disclosed personal information about some other person (2) The accused made the disclosure either without consent or in breach of contract (3) The accused had the intention to cause wrongful loss or wrongful gain or knowledge that wrongful loss or wrongful gain may be caused
Points for defence	(1) The act was a result of a mistake or negligence and was not done with knowledge or intention (2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise (3) The accused had obtained consent for the disclosure (4) The accused was acting in the discharge of his duties under the law (5) The accused did not breach the terms of any contract

4. Policy for privacy and disclosure of information

Entities, covered by data privacy law, are required to provide a data privacy policy on their website. This policy should provide details relating to:

1. clear and easily accessible statements of its practices and policies

2. type of information collected,

3. purpose of collection and usage of such information,

4. disclosure of information

5. reasonable security practices and procedures

5. Collection of information

The body corporate (or any person on its behalf):

1. Must obtain consent from the provider of the SPDI regarding the purpose of usage before collection of such information. This consent can be in writing through letter or fax or email.

2. Must not collect sensitive personal data or information unless the information is collected for a lawful purpose connected with its function or activity and the collection is considered necessary for that purpose.

3. Must take reasonable steps to ensure that the person concerned is having the knowledge of:

    a. the fact that the information is being collected
    b. the purpose for which the information is being collected
    c. the intended recipients of the information
    d. the name and address of the agency that is collecting the information
    e. the name and address of the agency that will retain the information.

4. Must not retain that information for longer than is required.

5. Must use the information only for the purpose for which it has been collected.

6. Must permit the providers of information, on request, to review the information they had provided.

7. Must ensure that any PI or SPDI found to be inaccurate or deficient is corrected or amended as feasible.

8. Must, prior to the collection, provide an option to the person not to provide the data or information sought to be collected.

9. Must give an option to the provider to withdraw his earlier consent. The body corporate has the option not to provide goods or services for which the said information was sought.

10. Must keep the information secure.

11. Must address any discrepancies and grievances in a time bound manner.

12. Must designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer must redress the grievances within one month from the date of receipt of grievance.

6. Disclosure of information

Disclosure of SPDI, by body corporate to any third party, requires one of the following conditions[9]:

1. prior permission has been taken from the provider of the information, or

2. the disclosure has been agreed to in the contract between the body corporate and provider of information, or

3. the disclosure is necessary for compliance of a legal obligation, or

4. the information is being shared with Government agencies[10] mandated under the law to obtain SPDI for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents[11], prosecution, and punishment of offences.

5. SPDI is being disclosed to any third party by an order under the law for the time being in force.

---

[9] The third party receiving SPDI from body corporate, or any person on its behalf, is prohibited from disclosing it further.

[10] The Government agency is required to send a request in writing to the body corporate possessing the SPDI stating clearly the purpose of seeking such information. The Government agency must also state that the information so obtained will not be published or shared with any other person.

[11] Cyber incidents means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

The body corporate or any person on its behalf is prohibited from publishing the SPDI.

7. Transfer of information

A body corporate, or any person on its behalf, is permitted to transfer SPDI to any other body corporate or a person in India or abroad under the following conditions:

1. the transferee ensures the same level of data protection that is adhered to by the transferor under the Indian law,

2. the transfer is necessary for the performance of the lawful contract with the provider of information,

3. the provider of the information has consented to the transfer.

8. Reasonable Security Practices and Procedures

A body corporate or a person on its behalf is considered to have complied with reasonable security practices and procedures, if:

1. it has implemented security practices and standards that are commensurate with the information assets being protected[12], and

2. it has a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures,

3. in the event of an information security breach, it is able to demonstrate that they have implemented security control measures as per their documented programme and policies,

4. it gets certified or audited on a regular basis by Government approved independent auditors[13].

Industry associations can get their codes of best practices approved and notified by the Central Government.

---

[12] The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard.

[13] The audit must be carried out at least once a year or as and when it undertakes significant upgradation of its process and computer resource.

9. Sample Privacy Policy (Customers)

Privacy policy for handling of or dealing in personal information including sensitive personal data or information as mandated by Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Definitions

For the purposes of this and related documents, unless the context otherwise requires,

1. "Act" means the Information Technology Act, 2000 (21 of 2000);

1. "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

2. "Body corporate" means "_____"

3. "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

4. "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being

processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

5. "Information" includes data, message , text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

6. "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;

7. "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

8. "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

9. “Sensitive personal data or information of a person” means such personal information which consists of information relating to;

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information.

Declaration under Rule 5 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Body Corporate makes the following declaration under Rule 5 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

1. The sensitive personal data or information (see Annexure 1) is being collected for a lawful purpose (see Annexure 2) connected with a function or activity of Body Corporate or any person on its behalf.

2. The collection of the sensitive personal data or information is considered necessary for the purpose above.

3. Body Corporate shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

4. The information collected shall be used for the purpose for which it has been collected.

5. Body Corporate or any person on its behalf shall permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible: provided that Body Corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to Body Corporate or any other person acting on behalf of Body Corporate .

6. Body Corporate shall keep the information secure as per security practices and procedures provided in The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System -

Requirements. Any person on behalf of Body Corporate shall keep the information secure as per security practices and procedures provided either in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 or The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System - Requirements.

7. Body Corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose Body Corporate designates _____ as the Grievance Officer. His / her contact number is _____ and his / her email address is _____. The Grievance Officer shall redress the grievances of provider of information expeditiously but within one month from the date of receipt of grievance.

Declaration under Rule 6 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Body Corporate makes the following declaration under Rule 6 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

1. This sensitive personal data or information may be disclosed to any person, if such disclosure is required for a lawful purpose connected with a function or activity of Body Corporate or any person on its behalf.

2. This sensitive personal data or information may be disclosed where the disclosure is necessary for compliance of a legal obligation.

3. This sensitive personal data or information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.

4. Body Corporate or any person on its behalf shall not publish the sensitive personal data or information.

5. The third party receiving the sensitive personal data or information from Body Corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

6. This sensitive personal data or information shall be disclosed to any third party by an order under the law for the time being in force.

Declaration under Rule 7 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Body Corporate makes the following declaration under Rule 7 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

Body Corporate or any person on its behalf may transfer sensitive personal data or information including any

information, to any other body corporate or a person in India, or located in any other country, that follows the security practices and procedures provided either in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 or The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System – Requirements.

Annexure 1

Type of personal or sensitive personal data or information collected under rule 3 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Personal Information

Sensitive personal data or information

Annexure 2

Purpose of collection and usage of personal or sensitive personal data or information collected under rule 3 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Consent, in writing through letter or Fax or email, from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

1. I understand and I have the knowledge that my sensitive personal data or information is being collected by "_____".

2. I understand and I have the knowledge of the purpose for which my sensitive personal data or information is being collected.

3. I have the knowledge of the intended recipients of the information.

4. I have the knowledge of the name and address of the agency that is collecting the information, and the agency that will retain the information.

5. I understand that I have the option not to provide the data or information sought to be collected by "_____" .

6. I permit "_____" .or any person on its behalf to transfer sensitive personal data or information to any other body corporate or a person in India, or located in any other country, that follows the security practices and procedures provided either in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 or The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System - Requirements.

7. I understand that I also have an option (while availing the services of "_____" .or otherwise) to withdraw my consent given earlier to "_____". I understand and accept that such withdrawal of the consent shall be sent in writing to "_____" .and in such case "_____" .shall have the option not to provide goods or services for which the said information was sought.

10. Privacy Policy (Employees)

Privacy policy for handling of or dealing in personal information including sensitive personal data or information as mandated by Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Definitions

For the purposes of this and related documents, unless the context otherwise requires,

1. "Act" means the Information Technology Act, 2000 (21 of 2000);

2. "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

3. "Body corporate" means "_____"

4. "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

5. "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being

processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

6. "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

7. "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;

8. "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

9. "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

10. “Sensitive personal data or information of a person” means such personal information which consists of information relating to;

(ix) password;

(x) financial information such as Bank account or credit card or debit card or other payment instrument details ;

(xi) physical, physiological and mental health condition;

(xii) sexual orientation;

(xiii) medical records and history;

(xiv) Biometric information;

(xv) any detail relating to the above clauses as provided to body corporate for providing service; and

(xvi) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information.

Declaration under Rule 5 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Body Corporate makes the following declaration under Rule 5 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

1. The sensitive personal data or information (see Annexure 1) is being collected for a lawful purpose (see Annexure 2) connected with a function or activity of Body Corporate or any person on its behalf.

2. The collection of the sensitive personal data or information is considered necessary for the purpose above.

3. Body Corporate shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

4. The information collected shall be used for the purpose for which it has been collected.

5. Body Corporate or any person on its behalf shall permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible: provided that Body Corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to Body Corporate or any other person acting on behalf of Body Corporate .

6. Body Corporate shall keep the information secure as per security practices and procedures provided in The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System -

Requirements. Any person on behalf of Body Corporate shall keep the information secure as per security practices and procedures provided either in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 or The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System - Requirements.

7. Body Corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose Body Corporate designates _____ as the Grievance Officer. His / her contact number is _____ and his / her email address is _____. The Grievance Officer shall redress the grievances of provider of information expeditiously but within one month from the date of receipt of grievance.

Declaration under Rule 6 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Body Corporate makes the following declaration under Rule 6 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

1. This sensitive personal data or information may be disclosed to any person, if such disclosure is required for a lawful purpose connected with a function or activity of Body Corporate or any person on its behalf.

2. This sensitive personal data or information may be disclosed where the disclosure is necessary for compliance of a legal obligation.

3. This sensitive personal data or information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.

4. Body Corporate or any person on its behalf shall not publish the sensitive personal data or information.

5. The third party receiving the sensitive personal data or information from Body Corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

6. This sensitive personal data or information shall be disclosed to any third party by an order under the law for the time being in force.

Declaration under Rule 7 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Body Corporate makes the following declaration under Rule 7 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

Body Corporate or any person on its behalf may transfer sensitive personal data or information including any

information, to any other body corporate or a person in India, or located in any other country, that follows the security practices and procedures provided either in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 or The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System – Requirements.

Annexure 1

Type of personal or sensitive personal data or information collected under rule 3 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Personal Information

Sensitive personal data or information

Annexure 2

Purpose of collection and usage of personal or sensitive personal data or information collected under rule 3 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Consent, in writing through letter or Fax or email, from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

1. I understand and I have the knowledge that my sensitive personal data or information is being collected by "_____".

2. I understand and I have the knowledge of the purpose for which my sensitive personal data or information is being collected.

3. I have the knowledge of the intended recipients of the information.

4. I have the knowledge of the name and address of the agency that is collecting the information, and the agency that will retain the information.

5. I understand that I have the option not to provide the data or information sought to be collected by "_____" .

6. I permit "_____" .or any person on its behalf to transfer sensitive personal data or information to any other body corporate or a person in India, or located in any other country, that follows the security practices and procedures provided either in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 or The International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System - Requirements.

7. I understand that I also have an option (while availing the services of "_____" .or otherwise) to withdraw my consent given earlier to "_____". I understand and accept that such withdrawal of the consent shall be sent in writing to "_____" and in such case "_____" shall have the option not to provide goods or services for which the said information was sought.

11. Relevant provisions of the IT Act

43 A. Compensation for failure to protect data

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation – For the purposes of this section,-
(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;
(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

45. Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

72A. Punishment for disclosure of information in breach of lawful contract.

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

12. Data privacy rules

G.S.R. 313(E).—In exercise of the powers conferred by clause (ob) of sub- section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. **Short title and commencement** — (1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions** — (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);
(b) "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;
(c) "Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;
(d) "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
(h) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;
(i) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. **Sensitive personal data or information**.— Sensitive personal data or information of a person means such personal information which consists of information relating to;—
(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:
provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in

force shall not be regarded as sensitive personal data or information for the purposes of these rules.

4. **Body corporate to provide policy for privacy and disclosure of information.—** (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) Clear and easily accessible statements of its practices and policies;

(ii) type of personal or sensitive personal data or information collected under rule 3;

(iii) purpose of collection and usage of such information;

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8.

5. **Collection of information**.— (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of —

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force..

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such boy corporate or any other person acting on behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance.

6. **Disclosure of inform**ation.— (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with

Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

7. **Transfer of information**.- A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

8. **Reasonable Security Practices and Procedures**.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central

Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

13. Clarification on Data Privacy Rules

Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000

PRESS NOTE

The Department of Information Technology had notified Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under section 43A of the Information Technology Act, 2000 on 11.4.2011 vide notification no. G.S.R. 313(E).

These rules are regarding sensitive personal data or information and are applicable to the body corporate or any person located within India. Any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 & 6. Body corporate, providing services to the provider of information under a contractual obligation directly with them, as the case may be, however, is subject to Rules 5 & 6. Providers of information, as referred to in these Rules, are those natural persons who provide sensitive personal data or information to a body corporate. It is also clarified that privacy policy, as prescribed in Rule 4, relates to the body corporate and is not with respect to any particular obligation under any contract. Further, in Rule 5(1) consent includes consent given by any mode of electronic communication.