Complying with the

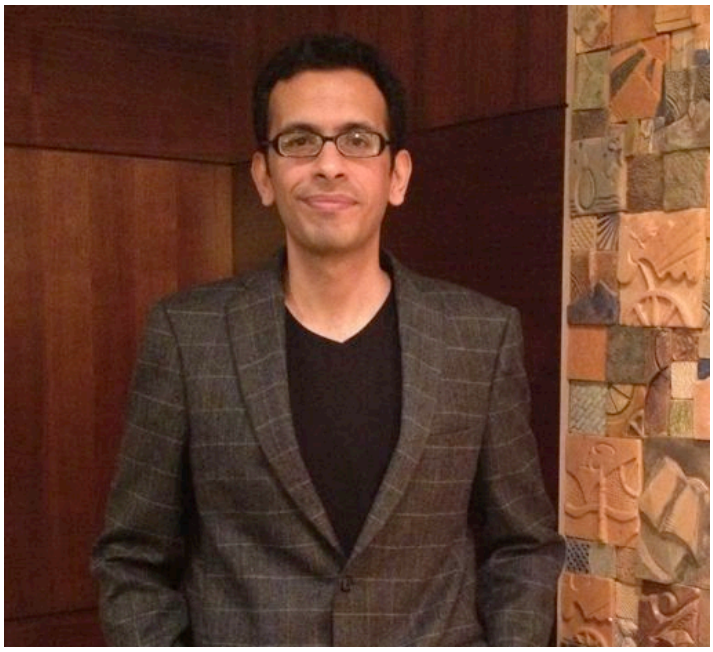
Data Privacy Law in India

Rohas Nagpal
Asian School of Cyber Laws

Published in 2012 by Asian School of Cyber Laws.

Asian School of Cyber Laws

Follow Asian School of Cyber Laws on facebook:
https://www.facebook.com/asianschoolofcyberlaws



Rohas Nagpal

Rohas Nagpal is a lawyer by qualification, a cyber crime investigator by profession, a hacker at heart and a programmer by passion.

He advises corporates, law firms, Governments and law enforcement agencies on issues relating to technology law, cyber crime investigation, information warfare and cyber terrorism. He has assisted the Government of India in drafting rules and regulations under the Information Technology Act. He is an active public speaker on technology issues and has addressed thousands of students, law enforcement personnel, lawyers and other professionals around the world.

Rohas conducts training programs in technology law and cyber crime investigation and has authored several books, papers and articles on these topics.

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.

Papers authored by him include Internet Time Theft & the Indian Law (Bangalore, 2001), Legislative Approach to Digital Signatures (Ecuador, 2001), Indian Legal position on Cyber Terrorism, Encryption and preventive measures

(on behalf of the Karnataka Police for Otto Schily, Interior Minister, Federal Republic of Germany), Defining Cyber Terrorism (Nagpur, 2002), The mathematics of terror (Nagpur, 2002) and Cyber Terrorism – A Global Perspective (Spain, 2002).
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.

He was part of the team that developed the world's smallest cyber crime investigation device, pCHIP a Portable Mega Investigation & Forensic Solution. This device is capable of capturing volatile evidence from a live computer, has an easy to use interface, and provides detailed reports.

He is the founder of CyberAttack, an open community working for cyber security. He also maintains www.bugs.ms, a specialized search engine that tracks bugs and vulnerabilities in Microsoft® products. He is also the founder of the proudIndian.me project and the Woman 2.0 Foundation.

He is a member of Information Systems Audit and Control Association (ISACA), International Association for Cryptologic Research (IACR), and a Sustaining Member of the Internet Society (ISOC), which is the organizational home of the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRTF) - the standards setting and research arms of the Internet community.

In 1999, Rohas Nagpal co-founded Cyber Tribe which today is comprised of 10 organizations - Asian School of Cyber Laws, TechJuris Law Consultants, ASCL Law School, Data64 Techno Solutions Pvt. Ltd., Republic of Cyberia, Association of Digital Forensic Investigators, Security Standards and Controls Development Organization, Corporate Crime Control Organization, Lexcode Regulatory Compliance Technologies Pvt. Ltd. and Data64 Technologies Pvt. Ltd.

Introduction to Data Privacy Law in India

The Data Privacy Law in India is contained primarily in:

1. Section 43A of the Information Technology Act
2. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
3. Section 72A of the Information Technology Act

This eBook focuses on the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, which came into effect on 11 April, 2011. These are referred to as *Data Privacy Rules* in this book.

This eBook also provides:

1. Checklists for compliance
2. Sample policy for Customers
3. Sample policy for Employees

Non-compliance with any of the provisions of the *data privacy rules* is penalized with a compensation /penalty of upto Rs. 25,000 under section 45 of the Information Technology Act.

Additionally, in some cases there may be liability under section 43A of the Information Technology Act. Under the original Information Technology Act, 2000, compensation claims were restricted to Rs. 1 crore. Now claims upto Rs 5 crore are under the jurisdiction of Adjudicating Officers. Claims above Rs 5 crore are under the jurisdiction of the relevant courts.

Additionally, in some cases there may be liability under section 72A of the Information Technology Act. This section provides for imprisonment upto 3 years and / or fine upto Rs 5 lakh.

The *Data Privacy Rules* relate to information of two primary types:

1. "**Personal information**" which 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. "**Sensitive personal data or information**" of a person which means such personal information which consists of information relating to:
    a. password[1];

[1] Password means a secret word or phrase or code or passphrase or secret key, or encryption or

b. financial information such as Bank account or credit card or debit card or other payment instrument details ;
c. physical, physiological and mental health condition;
d. sexual orientation;
e. medical records and history;
f. Biometric information[2];
g. any detail relating to the above clauses as provided to body corporate for providing service; and
h. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Sensitive personal data or information does not include any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law.

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.

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.

[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;

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

7. **Call centers, BPOs, LPOs** etc.

All these entities are required by law 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

All these entities must obtain consent from the provider of the information regarding purpose of usage **before** collection of such information.

The next few pages contain a sample policy for customers and for employees. These are followed by checklists for compliance.

Privacy Policy (Customers)

To be published on the official website.

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. 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;

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.

Privacy Policy (Employees)

To be published on the official website.

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. 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;

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.

Information Technology Audit & Compliance

Sensitive Personal Data or Information Rules

ITAC-SPDIR

Checklist Code: ITAC-SPDIR

Applicable Law: Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 read with section 43A of the Information Technology Act, 2000 as amended.

Note: The term "organization" in this document refers to a body corporate or any person on its behalf.

ITAC-SPDIR-1

Clear and easily accessible statements of its practices and policies

Checklist Number: ITAC-SPDIR-1

Primary Law: Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether the organization has published clear and easily accessible statements of its practices and policies on its website.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		

Notes:

ITAC-SPDIR-2

Type of personal or sensitive personal data or information collected

Checklist Number: ITAC-SPDIR-2

Primary Law: Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether the organization has published on its website the type of personal or sensitive personal data or information collected by it.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		

Notes:

ITAC-SPDIR-3

Purpose of collection and usage of personal information

Checklist Number: ITAC-SPDIR-3

Primary Law: Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether the organization has published on its website the purpose of collection and usage of personal or sensitive personal data or information collected by it.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-4

Disclosure of Information

Checklist Number: ITAC-SPDIR-4

Primary Law: Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether the organization has published on its website the details about the disclosure of personal or sensitive personal data or information collected by it.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended. In some cases imprisonment upto 3 years and / or fine upto Rs. 5 lakh under section 72A may be applicable.		
Notes:		

ITAC-SPDIR-5

Reasonable security practices and procedures

Checklist Number: ITAC-SPDIR-5

Primary Law: Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether the organization has published on its website the reasonable security practices and procedures followed by it.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-6

Obtaining consent prior to collection of information

Checklist Number: ITAC-SPDIR-6

Primary Law: Rule 5(1) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the organization obtains 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.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-7

Purposes for collection of information

Checklist Number: ITAC-SPDIR-7

Primary Law: Rule 5(2) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the organization does not collect sensitive personal data or information unless — (1) the information is collected for a lawful purpose connected with a function or activity of the organization; and (2) the collection of the sensitive personal data or information is considered necessary for that purpose.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-8

Person concerned has knowledge of information being collected

Checklist Number: ITAC-SPDIR-8

Primary Law: Rule 5(3) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that while collecting information directly from the person concerned, the organization takes 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.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-9

Retention of information

Checklist Number: ITAC-SPDIR-9

Primary Law: Rule 5(4) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that organization does 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.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-10

Usage of information solely for the purpose for which it has been collected

Checklist Number: ITAC-SPDIR-10

Primary Law: Rule 5(5) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the information collected is used solely for the purpose for which it has been collected.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-11

Review and amendment of information

Checklist Number: ITAC-SPDIR-11

Primary Law: Rule 5(6) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the organization permits the providers of information, as and when requested by them, to review the information they had provided and ensures that information found to be inaccurate or deficient is corrected or amended as feasible.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-12

Option to not provide information

Checklist Number: ITAC-SPDIR-12

Primary Law: Rule 5(7) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that prior to the collection of information, an option is provided to the provider of the information to not provide the data or information sought to be collected.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-13

Option to provider to withdraw consent

Checklist Number: ITAC-SPDIR-13

Primary Law: Rule 5(7) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the provider of information has an option to withdraw the consent given earlier.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-14

Security of information

Checklist Number: ITAC-SPDIR-14

Primary Law: Rule 5(8) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the information collected is kept secure as per IS/ISO/IEC 27001 or Schedule II (Information Technology Security Guidelines) of Information Technology (Certifying Authorities) Rules, 2000.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-15

Designation of Grievance Officer

Checklist Number: ITAC-SPDIR-15

Primary Law: Rule 5(9) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether a Grievance Officer has been appointed and his / her name and contact details have been mentioned on the organization's website.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-16

Redressal of grievances

Checklist Number: ITAC-SPDIR-16

Primary Law: Rule 5(9) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to address any discrepancies and grievances of their provider of the information, with respect to processing of information, expeditiously but within one month from the date of receipt of grievance.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended.		
Notes:		

ITAC-SPDIR-17

Disclosure of information to third parties

Checklist Number: ITAC-SPDIR-17

Primary Law: Rule 6(1) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that disclosure of sensitive personal data or information by the organization to any third party shall be done only under the following circumstances: (1) with prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, (2) if such disclosure has been agreed to in the contract between the organization and provider of information, or (3) where the disclosure is necessary for compliance of a legal obligation.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended. In some cases imprisonment upto 3 years and / or fine upto Rs. 5 lakh under section 72A may be applicable.		
Notes:		

ITAC-SPDIR-18

Prohibition on publication of information

Checklist Number: ITAC-SPDIR-18

Primary Law: Rule 6(3) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the organization does not publish the sensitive personal data or information.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended. In some cases imprisonment upto 3 years and / or fine upto Rs. 5 lakh under section 72A may be applicable.		
Notes:		

ITAC-SPDIR-19

Disclosure of information by third parties

Checklist Number: ITAC-SPDIR-19

Primary Law: Rule 6(4) of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the third parties, to whom information is disclosed, do not disclose it further.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended. In some cases imprisonment upto 3 years and / or fine upto Rs. 5 lakh under section 72A may be applicable.		
Notes:		

ITAC-SPDIR-20

Transfer of information

Checklist Number: ITAC-SPDIR-20

Primary Law: Rule 7 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Audit Question	Answer	Auditor's Comments
Whether systems are in place to ensure that the organization transfers personal information to any person in India or abroad, only under the following circumstances: (1) the other person ensures the same level of data protection that is adhered to by the organization under the law (2) the transfer is necessary for the performance of the lawful contract between the organization and provider of information or (3) where such person has consented to data transfer.		
Liability for non-compliance: Penalty not exceeding Rs 25,000 under section 45 of the Information Technology Act, 2000 as amended. In some cases imprisonment upto 3 years and / or fine upto Rs. 5 lakh under section 72A may be applicable.		
Notes:		

Annexure

Section 43A of the Information Technology Act, 2000 (as amended)

43 A. Compensation for failure to protect data[1]

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.

Section 45 of the Information Technology Act, 2000 (as amended)

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.

Section 72A of the Information Technology Act, 2000 (as amended)

72A. Punishment for disclosure of information in breach of lawful contract.[2]

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.

[1] Inserted by Information Technology (Amendment) Act, 2008.

[2] Inserted by Information Technology (Amendment) Act, 2008.

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)
NOTIFICATION
New Delhi, the 11th April, 2011

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 information.— (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.