THE INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011

ADV. K. SALMA JENNATH

INTRODUCTION

- Commonly referred to as the SPDI Rules
- Rules passed by the Central Government
- Under the Information Technology Act, 2000 – S. 43A
- Main focus of IT Act is information security, not data protection - "*An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents…*"

SOME IMPORTANT DEFINITIONS

- "**Biometrics**" – technologies that measure and analyse human body characteristics for authentication purposes (fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements, DNA)
- "**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.
- "**Information**" – includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fibre

SOME IMPORTANT DEFINITIONS

- "**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.
- "**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 processes 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.

SENSITIVE PERSONAL DATA OR INFORMATION

- Means such personal information which consists of information relating to:
  - Password
  - Financial information such as Bank account/credit or debit card/ other payment instrument details
  - Physical, physiological and mental health condition
  - Sexual orientation
  - Medical records and history
  - Biometric information
  - Any other details relating to the above provided to body corporate for providing a service or received by body corporate for processing, stored or processed under lawful contract or otherwise

EXCEPTION

- Information that is freely available or accessible in public domain
- Furnished under the Right to Information Act, 2005
- Or under any other law

PRIVACY POLICY

- Body corporate or any person who on behalf of body corporate
- Collects, receives, possess, stores, deals or handle information
- To provide a privacy policy for handling or dealing in personal information including sensitive personal information
- Policy to be published on website of body corporate
- Clear and easily accessible statements
- Type of personal or sensitive personal data or info collected
- Disclosure of information including sensitive personal data or info
- Reasonable security practices and procedures.

COLLECTION OF INFORMATION

- Body corporate or person on its behalf
  - to obtain consent in writing
  - from provider of sensitive personal data (SPD) or info
  - regarding purpose of usage
  - before collection of such information.
- Body corporate or person on its behalf shall not collect SPD unless –
  - Collected for a lawful purpose connected with the activity or function
  - Collection of SPD is considered necessary for the purpose

COLLECTION OF INFORMATION

- Body corporate or person on its behalf to take steps to ensure that the person whose data is collected is aware of -
  - The fact that information is being collected
  - The purpose
  - The intended recipients
  - Names and addresses of agency collecting info and that will retain info
  - Body corporate or person on its behalf shall not retain info longer than is necessary

COLLECTION OF INFORMATION

- Used for the purpose for which it was collected
- Permit providers of info to review that it is accurate and not deficient (on request) and correct or amend
- Body corporate is not responsible for the authenticity of the info provided
- To provide an option to the provider of info to not to provide it.
- Provider can withdraw their consent at any time – in writing.
- If consent is not given or is withdrawn, body corporate shall have the option not to provide the goods or service for which such info was sought.

COLLECTION OF INFORMATION

- Keep the information secure
- Address discrepancies and grievances of the provider – processing of information in a time bound manner.
- Grievance Officer – name and designation to be published on the website
- Redressal of grievances – expeditiously but within one month

DISCLOSURE OF INFORMATION

- Disclosure to third parties
- Prior permission of provider
- Exceptions - (i) unless already agreed to under contract or (ii) necessary for compliance of a legal obligation (iii) with Govt agencies mandated under law to obtain info for the purpose of verification of identity or for prevention, detection, investigation including cyber incidents, prosecution and punishment of offences (with request in writing – to mention that the info shall not shared or published) (iv) by an order under law
- No further disclosures.

TRANSFER OF INFORMATION

- May transfer to any other body corporate or person in India or another country
- That ensures the same level of data protection that is adhered to as per these Rules.
- Only if it is necessary for the performance of the lawful contract between body corporate and provider of info or if the provider has consented to data transfer.

REASONABLE SECURITY PRACTICES AND PROCEDURES

- Security measures commensurate with the information assets being protected.
- In case of security breach, body corporate to show that they have implemented security control measures as per their documented information security programme and information security policies.
- IS/ISO/IEC 27001 or codes of best practices for data protection.
- Certified or audited on a regular basis by an independent auditor at least once a year.

COMPARISON

	SPDI RULES	DPDP ACT
Responsibility	Body corporates	Data Fiduciary – any person
Grievance redressal	Grievance Officer	Data Fiduciary/Consent Manager/Data Protection Officer – to answer questions/ Board
Collection	No such mention	digital or non-digital digitised subsequently
Format	Simple rules alone	Illustrations
Applicability	Prospective effect	Retrospective effect
Process data	More clear about purpose	"Certain legitimate uses"
Notice	Reasonable steps to ensure	Notice for consent

	SPDI RULES	DPDP ACT
Children	No specific protection	Special provision
Duties of Data Principal	No duty	S. 15 lays down duties
Exemption	Very few	Many exemptions
Board	No such instrumentality	Data Protection Board – digital office
Assign	No such provision	Consent Manager/ Nominee
Accuracy	No obligation on body corporate	Data Fiduciary is responsible at times