DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Google

FAQs for SMBs

Information Technology (Amendments) Act 2008

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Contents

DEFINITIONS

What are digital signatures and how are they obtained?

It is a block of data at the end of an electronic message that attests to the authenticity of the message. Digital signatures are an actual transformation of an electronic message using public key cryptography. It requires a key pair (private key for encryption and public key for decryption) and a hash function (algorithm). Digital signature is a two way process, involving two parties: signer (creator of the digital signature) and the recipient (verifier of the digital signature). A digital signature is complete, if and only if, the recipient successfully verifies it.

How are digital signatures different from electronic signatures?

Digital signature is a sub-set of electronic signature. The Amendment Act, 2008, in order to maintain continuity with the regime of the digital signature, has introduced the concept of 'electronic signature'. Examples of electronic signatures may include biometric signatures, passwords, PINs and encryption applications.

What is Public Key Infrastructure (PKI) and what are the statutory requirements that companies have to follow while obtaining digital signatures?

Public Key Infrastructure (PKI) is the management and regulation of key pairs by allocating duties between contracting parties (Controller of Certifying Authorities (CAs) /Certifying Authorities/ Subscribers), laying down the licensing and business norms for CAs and establishing business processes/ applications to construct contractual relationships in a digitized world. The idea is to develop a sound,

public key infrastructure for efficient allocation and verification of digital signatures certificates. It is important that companies obtain digital signatures from licensed certifying authorities only. Further, digital signatures are never issued in the name of the company, partnership or association. These can only be issued to company personnel individually and never collectively.

How are cyber contraventions different from cyber offences?

The difference between 'cyber contravention' and 'cyber offence' is more about the degree and extent of criminal activity than anything else. For example, a mere unauthorized access to a computer, computer system or computer network may amount to 'cyber contravention' but for a 'cyber offence' it is the specific criminal violation that results from the unauthorized access to a computer, computer system, computer network or computer resource, that has to be taken into consideration.

Cyber Contraventions	Cyber Offences
Deals primarily with unauthorized access to computer, computer system or computer network or computer resource	Deals with computer, computer system or computer network or computer resource related serious offences
Offender to face civil prosecution	Offender to face criminal prosecution
Offender liable to pay damages by way of or fine compensation	Offender punishable with imprisonment term or with both

What are the different types of cyber contraventions under Section 43 the Act?

Section 43 of the Act identifies ten different circumstances causing damage to computer, computer system or computer network. It primarily takes into account all such contraventions that result from unauthorized access to computer, computer system, computer network or computer resources. These are being referred under Section 43(a) to Section 43(j) in the following manner:

a) Section 43(a) covers instances of hacking, computer trespass, data theft, privacy violation, software piracy/theft, etc.
b) Section 43(b) covers instances of unauthorised downloading, copying, extraction of data, computer databases, computer database theft, violation of privacy, etc.
c) Section 43(c) covers instances of deletion, alteration, damage, modifications of stored computer data or computer programs leading data interference
d) Section 43(d) covers instances related to computer/online fraud, forgery, privacy violations, etc.
e) Section 43(e) covers instances leading to denial of service attacks, spamming, etc.
f) Section 43(f) covers instances of system interference, misuse of computer devices, etc.
g) Section 43(g) covers instances of unauthorised access to computer, computer system, computer network, misuse of computer devices, etc.
h) Section 43(h) covers instances leading to computer/online fraud, phishing, identity theft, etc.
i) Section 43(i) covers instances of hacking, data theft, data interference, data loss, denial of service attacks, online frauds/forgeries, etc.

j) Section 43(j) covers instances related to copyright violations, piracy or theft of computer source code

Any person who commits any of the contraventions as referred in Section 43(a)-Section 43(j) is liable to pay compensation up to five crore rupees to the person so affected.

What are the various cyber offences listed under the Act?

The Act has categorised cyber offences under following categories:

a) Computer related offences, including unauthorized access, disruption, damage, destruction, etc. of computer resource. This covers Sections 65, 66, 66B, 66C, and 66D
b) Obscenity in electronic form (including child pornography). This covers Sections 66E, 67, 67A, and 67B
c) Non-compliance of directions, cyber terrorism etc. (including cyber security). This covers Sections 66F, 67C, 68, 69, 69A, 69B, 70, and 70B
d) Breach of confidentiality, privacy etc. This covers Sections 72, 72A (may also include Sections 66, 66B, 66C, & 66D depending upon circumstances)
e) Offences related to Electronic Signatures Certificate. This covers Sections 71, 73 & 74

What is meant by the term, "reasonable security practices and procedures"?

a) 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

b) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred above

c) 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, shall get its codes of best practices duly approved and notified by the Central Government for effective implementation

d) 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 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 out 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

What constitutes "SENSITIVE PERSONAL DATA OR INFORMATION (SPDI)"?

SPDI of a person means such personal information which consists of information relating to:

a) password
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
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,

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 SPDI.

What does term 'Data Subject' mean?

Data subjects are the providers of information, are those natural persons who provide SPDI to a body corporate.

What does terms 'Password' and 'Biometrics' mean, as defined in the Act?

'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.

'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.

What are the various data and privacy protection measures under the Act?

The Act provides numerous provisions to protect data and privacy. These are given under Sections 7, 43(a)-43(j), 43A, 65, 66, 66B, 66C, 66D, 66E, 66F, 67C, 70, 72, 72A and 84A and includes the following aspects of data and privacy protection:

a) Section 7 provides for retention of electronic records
b) Section 43(a)-43(j) provides for penalty and compensation for unauthorised access to computer, computer system, computer network or computer resource
c) Section 43A provides for compensation for failure to protect data
d) Section 65 provides punishment for tampering with computer source documents
e) Section 66 provides punishment for unauthorised access to computer, computer system, computer network or computer resource dishonestly or fraudulently
f) Section 66B provides punishment for dishonestly receiving stolen computer resource

g) Section 66C provides punishment for identity theft
h) Section 66D provides punishment for cheating by personation by using computer resource
i) Section 66E provides punishment for violating 'bodily' privacy
j) Section 67C provides for preservation and retention of information by intermediaries
k) Section 72 provides penalty for breach of confidentiality and privacy to those, who have been granted powers under the Act, and
l) Section 72A provides punishment for disclosure of information in breach of lawful contract

Who is an intermediary?

An '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.

The definition of 'intermediary' is intended to cover both professional and non-professional intermediaries, i.e., any person (other than the originator and the addressee) who performs any of the functions of an intermediary.

The Amendment Act, 2008 has given an inclusive definition of 'intermediary' and identified a set of service providers as 'intermediary' – 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.

What is the jurisdictional extent of the Act?

It applies to any offence or contravention committed whether outside or inside India by any person, irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

SCOPE

Whether this Act has an overriding effect?

Section 81 provides that this Act will prevail notwithstanding anything inconsistent therewith contained in any other law for the time being in force. In other words, this Act being a special Act, its provisions shall have an overriding effect on any other similar provisions of other enactments. However, later a proviso introduced by the amendment Act, 2008 defined the scope of overriding effect shall not restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970. The idea behind the new proviso is to protect the rights of 'intellectual property rights holder' under the Copyright Act and Patents Act.

Whether electronic contracts are valid under the Act?

The Act provides legal certainty as to the conclusion of contracts by electronic means. The electronic contracts include all click wrap, web-based, SMS, email contracts, oral contracts over VoIP and call, among others. The Act deals not only with the issue of contract formation but also with the form in which an offer (proposal) and an acceptance may be expressed. It covers not merely the cases in which both the offer and the acceptance are communicated by electronic means but also cases in which only the offer or only the acceptance (or revocation of proposals and acceptances) is communicated electronically.

What are the documents or transactions to which this Act shall not apply?

The documents or transactions to which this Act shall not apply are as follows:

a) A negotiable instrument (other than a cheque) as defined in Section 13 of the Negotiable Instruments Act, 1881 (26 of 1881)
b) A power-of-attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882)
c) A trust as defined in Section 3 of the Indian Trusts Act, 1882 (2 of 1882).
d) A Will as defined in clause (h) of Section 2 of the Indian Succession Act, 1925 (39 of 1925) including any other testamentary disposition by whatever name called
e) Any contract for the sale or conveyance of immovable property or any interest in such property

Whether an office being operated from home would constitute a public place?

Yes, if a home is also being used as an office, then the said premises could be seen as a public place. More so, if the home address is also the registered office address.

Whether police officers are authorised to investigate any contravention under Section 43 of the Act?

Only on the request of the Adjudicating Officer, police officers not below the rank of inspector, may investigate any contravention under the Act.

Whether companies are bound to follow the directions given by CERT-In under the Act?

Under Section 70B(6) of the Act, companies, including service providers, intermediaries, data centers, body corporate and any other person, are bound to follow the directions given by CERT-In.

Whether CERT-In plays any role in blocking the websites?

No, CERT-In does not play any role in blocking websites. It is significant to note that vide notification no. G.S.R. 181(E) dated 27/02/2003, CERT-In had been designated as the single authority for issuing of instructions in the context of blocking of websites. Subsequently, vide notification no. G.S.R. 410(E) dated 17/05/2010, the above stated notifications, i.e., 181(E) has been rescinded.

Whether a company can use Section 43 provisions against its employees or ex-employees?

A company has a right to initiate proceedings before the Adjudicating Officer under Section 43 against any current or ex-employee, if any such personnel have violated any of the provisions.

Whether tempering of computer source code is punishable under the Act?

Yes. The Act provides, that whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or

maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Is hacking an offence under the Act?

Yes, hacking is an offence under the Act. It is important to note that the term 'hacking' per se is not defined, nevertheless, it can be seen as part of Section 65 'tampering of computer source code', Section 66 'computer related offences', Section 66B 'dishonestly receiving stolen computer resource etc.', Section 66C 'identity theft', Section 66D 'cheating by personation by using computer resource', & Section 66F 'cyber terrorism'.

Is ethical hacking an offence under the Act?

The Act does not distinguish between 'hacking' and 'ethical hacking'. Both 'hacking' and 'ethical hacking' could be treated as computer related offences as articulated under Section 66 of the Act. It is also possible that based upon the set of circumstances, an incident of ethical hacking may result from unauthorised access to computer, computer network or computer resource and thus can be classified as cyber contravention as mentioned under Section 43 of the Act.

Whether violating bodily privacy is an offence?

Yes, under Section 66E violating bodily privacy is an offence. Section 66E provides that whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. It is imperative

that service providers be careful regarding installation of CCTVs or other installation devices within the office premises. Under no circumstances such devices should be installed in changing rooms or washrooms.

Whether cyber terrorism has been defined under the Act?

Section 66F defines cyber terrorism. It is an intention to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any Section of the people by using computer resource to access restricted information, data or computer database with reasons to believe that such restricted information, data or computer database may cause or likely to cause injury to:

a) the interests of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or
b) in relation to contempt of court,
c) defamation, or
d) incitement to an offence, or
e) the advantage of any foreign nation, group of individuals or otherwise.

The offence of cyber terrorism is punishable with imprisonment which may extend to imprisonment for life.

Whether obscenity in electronic form has been declared as an offence under the Act?

Yes, obscenity in electronic form is an offence. Following Sections have made obscenity in electronic form an offence:

a) Section 67 deals with publishing of information, which is obscene in electronic form,
b) Section 67A deals with punishment for publishing or transmitting of material containing sexually explicit Act, etc. in electronic form, and
c) Section 67B deals with punishment for publishing or transmitting of material depicting children in sexually explicit Act, etc. in electronic form.

Whether a company can be held responsible if one of its employees is found using company's computer resources to view, browse, download, publish or transmit obscene material in electronic form?

If an employee uses company's computer resources to view, browse, download, publish or transmit obscene material in electronic form while inside the company premises, then the company may also be held responsible for contributory negligence.

Does the Act provide any mechanism for computer forensics?

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Whether a company can be held liable for offences under the Act?

A company can be held liable under Section 85 for offences under the Act. This Section introduces the concept of contributory liability. It provides that every person who, at the time the contravention was committed, was in charge of, and was responsible to the company for the conduct of business of the company as well as the company,

shall be guilty of the contravention and shall be liable. However, if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, then he shall not be held guilty.

This section further provides that if any contravention under the Act has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

What mandate has been given under the Act to provide policy for privacy and disclosure of information by the body corporate?

The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of data subject, needs to provide a privacy policy stating how SPDI is handled or dealt with and ensure that the policy is available for view by data subjects under the lawful contract. Such policy shall be published on the website of body corporate or any person on its behalf and shall provide following details:

a) Practices and policies followed in clear and easily accessible statements
b) Type of personal or SPDI that has been collected
c) Purpose of data collection and data usage
d) Disclosure of collected information including SPDI
e) Reasonable security practices and procedures followed

In the clarification issued later by the government, it is mentioned that the privacy policy, as prescribed in Rule 4 under Sec 43A, relates to the body corporate and is not with

respect to any particular obligation under any contract. So a Service Provider (Data Processor) is not obligated to publish privacy policy on its website for all its contractual engagements with Data Controllers.

Whether the Act provides any information or guidelines for collecting the sensitive personal data of data subjects?

As per the Act, the body corporate or any person on its behalf can collect SPDI if it is:

a) Collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf
b) Considered necessary for that purpose defined

While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take necessary steps in order to ensure that the data subject is having the knowledge of the fact that the information is being collected, purpose for which the information is being collected, the intended recipients of the information etc. Service Providers (or Data Processors) who are providing services to a Body Corporate (Data Controllers) under contractual obligation are not subject to the requirement of above provisions.

Whether the Act provides any provisions for obtaining consent while collecting sensitive personal data of data subjects?

Body corporate or any person on its behalf shall obtain consent in writing through letter or fax or email or by any mode of electronic communication from the provider of the SPDI regarding purpose of usage before collection of such information. Service Providers (or Data Processors) who are providing services to a Body Corporate (Data

Controllers) under contractual obligation are not subject to the requirement of above provisions.

Does the Act mandate organizations on data usage and retention after collecting the data from data subjects?

The Act says that the information collected shall be used by the body corporate for the purpose for which it has been collected. Body corporate or any person on its behalf holding SPDI shall not retain that information for longer than required for lawful or legal compliance purposes. However, till date, no specific time duration has been prescribed under the provisions of the Act.

Whether the Act mandates organizations to allow data subjects for reviewing and updating the information provided by them?

The act asks body corporate or any person on its behalf, to have mechanism under which data subject can review the information provided by them and in case of incorrect information, the same can be updated, on request. Body corporate shall not be responsible for the authenticity of the personal information or SPDI supplied by the data subject. It will maintain the record as was provided by the data subject, even if it was incorrect. Service Providers (or Data Processors) who are providing services to a Body Corporate (Data Controllers) under contractual obligation are not subject to the requirement of above provisions.

Whether the Act asks body corporate to provide choice to data subjects for providing the information?

Body corporate or any person on its behalf shall, before collecting the information, provide an option to the data subject to not to provide the data or information sought. The data subject, at any time while availing the services or otherwise, shall 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 data subject not providing information or withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought. Service Providers (or Data Processors) who are providing services to a Body Corporate (Data Controllers) under contractual obligation are not subject to the requirement of above provisions.

Who is a grievance officer? How has been his/her role defined in the Act?

The Act has mandated the body corporate to appoint or designate a grievance officer who is required to address any discrepancies and grievances of its data subjects with respect to processing of SPDI in a time bound manner. The body corporate is required to publish his/her name and contact details on its website and the grievance officer shall redress the grievances within one month from the date of receipt of grievance.

Whether the Act mentions the provisions to be taken by the organizations before disclosing the sensitive personal data to third party?

Disclosure of SPDI by body corporate to any third party shall require prior permission from the data subject. The only exceptions are in case of a contract allowing such disclosure, or where the disclosure is necessary for legal compliance. Further, the

third party receiving the SPDI from body corporate or any person on its behalf shall not disclose it further. The government agency shall send a request in writing to the body corporate possessing the SPDI 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.

REGULATION

Who is the regulator and what is the role defined under the Act?

Primarily, it is the Adjudicating Officer of a State who has been empowered to adjudicate upon any contraventions under Sections 43-45 of the Act. The Adjudicating Officer is the 'First Court of Adjudication' and thus plays a very important link in the entire judicial process. His quasi-judicial authority covers not only the entire range of computer-related contraventions, especially under Section 43, but also includes adjudging body corporates vis-à-vis any failure to protect data, including sensitive personal data.

Who is an Adjudicating Officer?

The Central Government as per the Gazette Notification for Information Technology Rules, 2003 under the short title 'Qualification and Experience of Adjudicating Officer and Manner of Holding Enquiry' vide Gazette Notification G.S.R. 220(E), dated 17th March, 2003 has notified 'Eligibility for Adjudicating Officer' [Rule 3]. In pursuant to this, the Central Government notified the appointment of the Secretary of Department of Information Technology of each of the States or of Union Territories as Adjudicating Officer for the purposes of the Act vide Gazette Notification G.S.R. 240(E), dated 25th March, 2003.

What is the jurisdiction of an Adjudicating Officer?

The Adjudicating Officers shall exercise jurisdiction in respect of the contraventions in relation to Chapter IX of the Act and the matter or matters or places or area or

areas in a State or Union Territory of the posting of the person. The complaint shall be made to the Adjudicating Officer of the State or Union Territory on the basis of complainant's location of computer system or computer network. For example, if there is a data theft which has occurred at the company's premises located in Town A, then the complaint would lie before the Adjudicating Officer of the State or Union Territory under which the said Town A falls.

Is it possible for the Adjudicating Officer to transfer the case to the Magistrate?

Yes, if the adjudicating officer is convinced that the scope of the case (under adjudication) extends to the cyber offence(s) under Sections 65-74 of the Act, needing appropriate punishment instead of mere financial penalty, then as per the aforesaid rules, he should transfer the case to the Magistrate having jurisdiction to try the case.

Who grants licences to the Certifying Authorities?

It is the Controller of Certifying Authorities who grants licences to the Certifying Authorities. Presently, the following are licensed Certifying Authorities: (a) National Informatics Centre (NIC), (b) Tata Consultancy Services (TCS), (c) SafeScrypt (d) Centre For Development Of Advanced Computing (C-DAC) (e) Code Solutions, (f) Institute for Development & Research in Banking Technology (IDRBT), and (g) eMudhra.

Who has the power to investigate offences under the Act?

Police officers not below the rank of inspector have the power to investigate offences under Section 78 of the Act.

Whether police officers and other designated officers as appointed by the Central Government or State Government authorized by the Central Government in this behalf have the authority to enter any public place and search any company's premises?

Yes, police officers or other designated officers as appointed by the Central Government or State Government (authorized by the Central Government) have the authority to enter any public place and search any company's premises and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. A company is within its rights to ask for a copy of search warrant before letting any police officer or other designated officers as appointed by the Central Government or State Government (authorized by the Central Government) to enter and search company's premises.

Who is responsible under the Act to issue directions for interception or monitoring or decryption of any information through any computer resource?

The Secretary in the Ministry of Home Affairs, in case of the Central Government; or the Secretary in charge of the Home Department, in case of a State Government or Union Territory, as the case may be, act as the 'Competent Authority' to issue directions for interception or monitoring or decryption of any information through any computer resource.

Whether a company can be called to monitor and collect traffic data or information through any computer resource for cyber security?

The Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology is the Competent Authority to issue directions for monitoring and collection of traffic data or information.

What are the roles of CERT-In?

The Indian Computer Emergency Response Team (ICERT or CERT-In) serves as the national agency for performing the following functions in the area of Cyber Security–

a) Collection, analysis and dissemination of information on cyber security incidents
b) Forecast and alerts of cyber security incidents
c) Emergency measures for handling cyber security incidents
d) Coordination of cyber incidents response activities
e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents and
f) such other functions relating to cyber security as may be prescribed

COMPLAINTS & PENALTIES

To whom, a subscriber of a digital or electronic signature, should approach in case of a dispute with his licensed Certifying Authority?

The subscriber should approach the Controller of Certifying Authorities for any such dispute resolution.

What are the quasi-judicial powers that have been granted to the Adjudicating Officers under the Act?

The Act provides the following quasi-judicial powers to the Adjudicating Officers:

a) to exercise jurisdiction in respect of the contraventions in relation to Chapter IX [Penalties and Adjudication] of the Act
b) to receive complaint from the complainant
c) to issue notices together with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings
d) to hold an enquiry or dismiss the matter or may get the matter investigated
e) to enforce attendance of any person or persons
f) to fix a date and time for production of documents (including electronic records) or evidence and
g) to hear and decide every application, as far as possible, in four months and the whole matter in six months.

For what sort of cyber contraventions companies (or any individual) can approach the Adjudicating Officer and what is the maximum compensation which can be awarded by the Adjudicating Officer

Companies (or any individual) can approach an Adjudicating Officer appointed under the Act for any cyber contraventions related issues under Section 43 and 43A. The Adjudicating Officer can award financial compensation upto five crore rupees under the Act to the affected company.

What is the course of action available to a company that has suffered financial losses much more than five crore rupees?

If the affected company assesses the value of damage caused to him beyond rupees five crore, then the said company may have to approach the competent judicial court for redressal.

While adjudging the quantum of compensation what set of factors does the Adjudicating Officer take into consideration?

Under the Act, the Adjudicating Officer is required to take into consideration the following factors, while adjudging the quantum of compensation:

a) The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default
b) The amount of loss caused to any person as a result of the default and
c) The repetitive nature of the default

To whom a company (or any individual) aggrieved by the order of adjudicating officer, should approach?

A Company (or any individual) may approach Cyber Appellate Tribunal (CAT) if aggrieved by the order of the Adjudicating Officer. The company (or any such individual) has to file an appeal against the order of the Adjudicating Officer within forty five days from the date on which a copy of the order made by the Controller or the Adjudicating Officer is received by the person so aggrieved. Moreover, the Tribunal may entertain an appeal even after the expiry of the said period of forty five days, if it is satisfied that there was sufficient cause for not filing it within that period.

Whether the appeal against the order of the Adjudicating Officer can be filed before any civil court?

The Act empowers both Adjudicating Officer and the Cyber Appellate Tribunal to have an exclusive jurisdiction to entertain any suit and proceeding in respect of any matter under this Act. The objective behind such a legislative provision is to create specific enforcement jurisdiction involving the Adjudicating Officer and the Cyber Appellate Tribunal.

Which Forum should a company (or individual) aggrieved by the order of CAT approach?

The Act provides a second forum of appeal in the form of the High Court (the first being the Cyber Appellate Tribunal) to any person aggrieved by any decision or order of the Cyber Appellate Tribunal. An appeal is to be filed within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order.

What are the remedies available to a company if it is a victim of hacking?

A company can take recourse to both civil and criminal liabilities under the Act. It can file a complaint before the Adjudicating Officer under Section 43 seeking appropriate compensation and also simultaneously file a police complaint taking cognisance of Sections 66, 66B, 66C, 66D, and 66F.

What is the punishment for dishonestly receiving stolen computer resource or communication device?

Whoever dishonestly receives or retains any stolen computer resource or communication device, knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term, which may extend to three years or with fine which may extend to rupees one lakh or with both. This provision could be seen as a data protection measure in view of the definition of computer resource.

What is the punishment for identity theft prescribed under the Act?

Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to rupees one lakh. It covers all such instances of identity theft including phishing, denial of service, data theft, installation of spyware and cookies among others.

What is the punishment for cheating by personation by using a computer resource?

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. It covers all such instances of creating clone websites, email frauds, email forgeries, data theft and loss of privacy, among others.

What is the penalty for breach of confidentiality and privacy?

Any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material, without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

What is the punishment for disclosure of information in breach of lawful contract?

Any person, including an intermediary who has secured access to any material containing personal information about a person, discloses such information without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain to such a person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. It is thus imperative that, all service providers should frame requisite terms of service

conditions and privacy policy giving details of mode, manner and extent of personal information captured and used by them.

Whether the Act has provided punishment for abetment of offences?

Section 84B of the Act takes into account 'abetment of offences' and prescribes punishment of such abetment. An abettor is to be punished with the same degree of punishment as provided for the offence under this Act.

Whether the Act has provided punishment for attempt to commit offences?

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

GUIDELINES

Whether the Act provides for any statutory requirement regarding the format and period of retention of electronic records?

Section 7 of the Act lays down the following conditions for retention of electronic records:

a) Accessibility so as to be usable for a subsequent reference
b) Retention in the format in which it was originally generated, sent or received or in a format, which can be demonstrated, to represent accurately the information originally generated, sent or received
c) The details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record

The Act provides no time period for retention of records in electronic form. Records pertaining to any subject matter should be retained in electronic form for that duration as mandated under that specific legal framework for the time being in force.

Whether there exists any statutory and timeline requirement regarding audit of documents, records, and information, maintained in electronic form?

It would be as per the law for the time being in force for that specific area/subject matter. For example, if under the Income Tax Act, 1961, law requires audit of documents, records or information on annual/ bi-annual or quarterly basis, the same audit period or duration would have to be followed by the assesse, if he is processing and maintaining records in electronic form.

Under what circumstances body corporates can be held responsible for failure to protect data?

Where a body corporate, possessing, dealing or handling any SPDI 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.

It creates onus on 'body corporate' to implement and maintain 'reasonable security practices and procedures' in order to protect sensitive personal data of an individual (data subject).

What are the online contractual guidelines?

It is a settled law that if the contract is being made using modern communication devices, like telephones then the contract is complete only when the acceptance is received by the offer or (a person who makes an offer) and the contract is made at the place where the acceptance is so received. While entering into a contract, it is imperative that parties to contract should frame their online contractual guidelines giving details on:

a) Process of acknowledgement of electronic records
b) Time and place of despatch of electronic records
c) Place of business and
d) Identifying/ naming the designated email ID, which will be used to transmit and receive electronic records

Whether there are any provisions related to third country transfer of data within the Act?

A body corporate or any person on its behalf may transfer SPDI 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. 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.

Whether the Act provides for different levels of encryption for (a) data at rest, and (b) data in transit?

The Act under Section 84A makes no distinction between level of encryption for data at rest and data in transit. The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption. The Central Government came out with draft rules prescribing the modes and methods for encryption under Section 84A, which were later withdrawn. The Government is presently working to bring out revised set of rules.

Notes

Notes

DATA SECURITY COUNCIL OF INDIA

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | **E:** info@dsci.in | **W:** www.dsci.in

FOLLOW US

Data Security Council of India

DSCI_Connect

DSCI.Connect

DSCIvideo