

Data Security Council of India

A Self - Regulatory Organization



DSCI

A **NASSCOM** Initiative

DATA
SECURITY
COUNCIL
OF INDIA

DSCI

DATA
SECURITY
COUNCIL
OF INDIA

Privacy vis-à-vis Security: Privacy & data protection in India

Vinayak Godse | Sr. Manager, Security Practices

DATA SECURITY COUNCIL OF INDIA (DSCI) | A NASSCOM® Initiative

Topic of discussion

- Privacy Culture & Perceptions in India
- Privacy perceptions- Changing landscape
- How regulators are responding?
- How industry is responding?
- Outsourcing to Offshore- risk to Privacy?
- India- Data Protection & Privacy Legal Model
- DSCI as a SRO for Data Protection
- Privacy landscape
- Use of biometrics

Privacy Culture in India

Indian Culture & Society

Joint family structure

Collectivist, Hierarchical,
Relationship oriented

Low IDV (Individualism Index)
ranking

Less awareness about privacy among Indians

No sophisticated understanding of privacy

Relate privacy to personal space- privacy
to physical, home and living space

Less concern about computerization of data

Broadband penetration still at 2 %

Less frequent use of credit cards and many
retail shops do not yet computerize any data

Less awareness to identity theft

Concept of \Big Brother.“- unaware
of the government tracking them.

Collectivist societies have more trust and faith in other people than individuals in individualist societies..

..... Hofstede, *Cultural and Organizations* -

Privacy Perceptions in India

While 61% of the respondents in the US related **privacy to some form of control of information** only 14% of the subjects in India related privacy to these concepts.

48% of the respondents in India related **privacy to physical, home and living space**, but only 18% of the subjects in the US related privacy to these concepts.

79% of the subjects in the US were concerned about **keeping computerized information secure**, while the concern level was 21% among Indian subjects.

Knowledge of and Need for Privacy Laws

Scenarios	India	US
To use computer records and other methods to determine shopping habits	13 %	43 %
To determine reading habits	19 %	40 %
To connect to peoples' cell phones or computers and send them customized advertisements	18 %	56 %

Indian companies **tend not to provide opt-in and opt-out** options to customers.

Reference

Privacy Perceptions in India and the United States: An Interview Study conducted by Carnegie Mellon University, 2005

Privacy Perceptions in India- Changing Landscape

Quantum jump in the use of technological solutions for delivery of financial services

Phenomenal increase in the number of credit cards issued by the banks

Expansion of telecom & mobile connectivity

Increasing e-Commerce applications & emergence of m-Commerce

Huge investment in the e-Governance projects

Travel, Airline & Hospitality industry goes online

Adoption of Web 2.0 services, social networking

Transformation from Joint to Nuclear family structure

Fast climbing individualism ladder

New emerging segment – 25-35 years

Emergence of personalize services



Leading to issues like

Annoyance over telemarketing calls and messages

Increased awareness of personal information being collected

Rising concerns over computer and internet security

Media coverage of national & international data breaches

Increased exposure of IT/ITES industry to global data protection regulations

How Compliance Authorities are responding?

Ethical Guidelines for Biomedical Research

By Indian Council of Medical Research, 2000

- Identity & records of the human subjects of the research or experiment are as far as possible kept **confidential**;
- No details about identity of said human subjects are disclosed without valid scientific and legal reasons, without the specific **consent** in writing of the human subject concerned,

The Telecom Unsolicited Commercial Communication (UCC) Regulations, 2007,

By TRAI

- Do Not Call Registry
- the **LICENSEE** condition to take necessary steps to safeguard the **privacy and confidentiality** of any information about a third party & its business to whom it provides the SERVICE

Reserve Bank of India, Master Circular, July 2007

- Banks/NBFCs/ their agents should **not resort to invasion of privacy** viz., reveal any information relating to customers to any other person or organization without obtaining their **specific consent**
- regards **the purpose/s for** which the information will be used and the organizations with whom the information will be shared.
- Banks/NBFCs would be solely responsible for the **correctness** of information, In case of providing information relating to credit history / repayment, the bank/NBFC may explicitly bring **to the notice** of the customer.
- the staff, of both the banks and their DSA/DMA's should be properly
- briefed and trained privacy of customer information

How Industry is responding?

Privacy Commitment - Wir
http://www.icicibank.com

Privacy Commitment

In the course of using this and questionnaires, ICICI customers, including inform

ICICI Bank is strongly con and reasonable measures through the world wide web in accordance with this Priv

ICICI Bank endeavours to s ICICI Bank uses 128-bit en level of encryption in India. encryption, the Customer ensuring the best level of s

The Customer would be r information, and it is recor that no unauthorised acce others to guess, the Cust (like !, @, #, \$ etc.). The (any written or other record

ICICI Bank undertakes not to disclose the information provided by such action is necessary to:

- Conform to legal requirements or comply with legal process;
- Protect and defend ICICI Bank's or its Affiliates' rights, interest
- Enforce the terms and conditions of the products or services;
- Act to protect the interests of ICICI Bank, its Affiliates, or its n persons.

The Customers shall not disclose to any other person, in any mann to ICICI Bank or its Affiliates of a confidential nature obtained in the

Done



Cleartrip is fana

By accessing this Site, certain spent, along with other simila

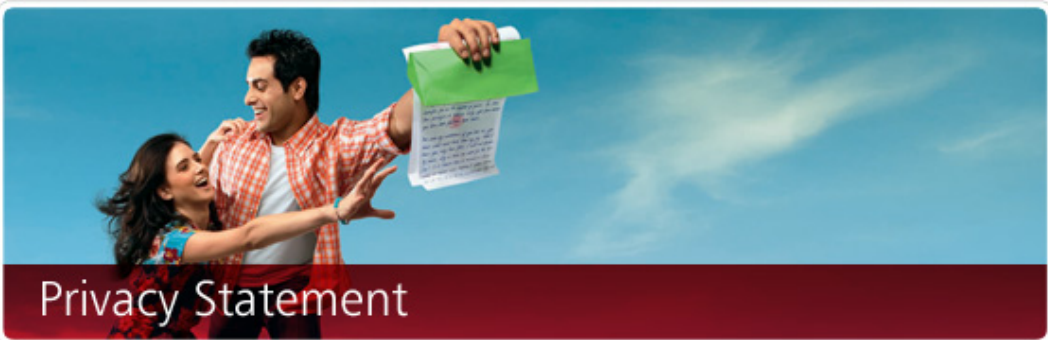
Such stored information may may deem appropriate.

If you provide unique identify

Any personally identifiable inf sell, share or in any way revea

We want you to feel confident guarantee security, we have i prevent unauthorized access, technologies.

Media Centre | Careers | Airtel Innovation Fund | Contact Us



Home » [Privacy Statement](#)

Privacy Statement

Airtel is committed to providing you with the highest levels of customer service. This includes protecting your privacy. This privacy statement sets out the approach of Airtel in relation to the treatment of your personal information. It includes information on how Airtel collects, uses, discloses and keeps secure, individuals' personal information.

Your personal information

"Personal Information" is any data that identifies you. The personal information given to us is presumed to be true, complete and accurate in all respects and you agree to notify us immediately of any changes to that. Personal information held by Airtel may include your name, date of birth, current and previous addresses, telephone/mobile phone number, email address, bank account or credit card details, occupation, driver's licence number and your Airtel PIN, username or password. Airtel also holds details of your Airtel account.

How do we use personal information

Your personal information may be used to:

- > Verify your identity
- > Assist you to subscribe to Airtel's services
- > Provide the services you require
- > Administer and manage those services, including charging, billing and collecting debts
- > Inform you of ways the services provided to you could be improved

How Industry is responding?

- > About Shaadi.com
- > Shaadi.com On Dish TV
- > Getting Started
- > Login / Password
- > Partner Search

1.41 crore possibilities. Search now.

Ashik Mehta's story
With a busy schedule like mine this is certainly the best way to find someone to share my life



Looking for: Bride with photo

of Age: 20 to 25

of Religion: Select

of Community: Doesn't Matter

of Country: India Search >

View by Profile ID Go > Search by Caste >>>
All search options >>>

1 Register
and create your free profile.

2 Search
for members who meet your criteria.

3 Contact
members you like via email, phone or chat.

Register Free!

Assamese | Bengali | Gujarati | Hindi | Kannada | Malayalam | Marathi | Marwari | Oriya | Parsi | Punjabi | Sindhi | Tamil | Telugu | Urdu

Brand Showcase

For all your wedding related needs. [Shop >](#)

Gift Your Loved One The Perfect Gift.

Over 1 million members have found their life partner on Shaadi.com, so can your loved one ... >>

Miracles do happen!
622,073 matches and counting

Hi, I am glad to write our success story and share with all of you. I was quite active on ... >>



Jigar & Tanvi >>

Religion Matrimonials - Hindu, Muslim, Sikh, Christian, Jain, Buddhist, Parsi, Jewish, more matrimonial sites >>

Regional Matrimonials - India Matrimonials, USA, Canada, UK, Pakistan, UAE, Saudi Arabia, Australia, more matrimonial sites >>

Partner with us > Site Map > Matrimonial Sites > Privacy Policy > Contact Us > Terms of Use > Careers > About Us > Privacy, Protection & You
Indian matrimonial classifieds > Indian wedding > Marriage India > Astrology services > Shaadi SEAL > Shop > Matrimony > Advertise with us

Network Sites: AstroLife.com | Map.com | ShaadiTimes.com | Makaan.com | Shaadi.com Centres | ShaadiPages.com | 99-1Helix

Privacy Statement for Shaadi.com Matrimonial Services (Effective date: 28th November 2008)

People Interactive (India) Pvt. Ltd. is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent organization whose mission is to enable individuals and organizations to establish trusting relationships based on respect for personal identity and information by promoting the use of fair information practices. This privacy statement covers the site www.shaadi.com. Because we want to demonstrate our commitment to our user's privacy, we have agreed to disclose our privacy practices and have them reviewed for compliance by TRUSTe.



TRUSTe program covers only information that is collected through this Web site, and does not cover information that may be collected through software downloaded from this site.


If you have questions or concerns regarding this statement, please [write to us](#). If you do not receive acknowledgment of your inquiry or it is not satisfactorily addressed, you should then contact TRUSTe through the TRUSTe Watchdog Dispute Resolution Process (http://www.truste.org/consumers/watchdog_complaint.php). TRUSTe will serve as a liaison with the Web site to resolve users' concerns.

Privacy Policy FAQs

This section covers Shaadi.com's treatment of personally identifiable information that Shaadi.com collects when you are on our site.

Read on for information on the following aspects about our Privacy Policy:

1. What information does Shaadi.com collect/track about me?
2. What does Shaadi.com do with the information it collects/tracks?
3. With whom does Shaadi.com share the information it collects/tracks?
4. Tell me about links with other sites.
5. Tell me about Cookies.
6. Tell me about Shaadi.com policy on correcting, updating or removing personal information.
7. How will I know of changes in Shaadi.com privacy policy?
8. Tell me about security of my personal information.
9. Tell me about Shaadi.com's email policy.
10. Tell me how to contact Shaadi.com.



Sajji & Simi

{ 822,073 matches }

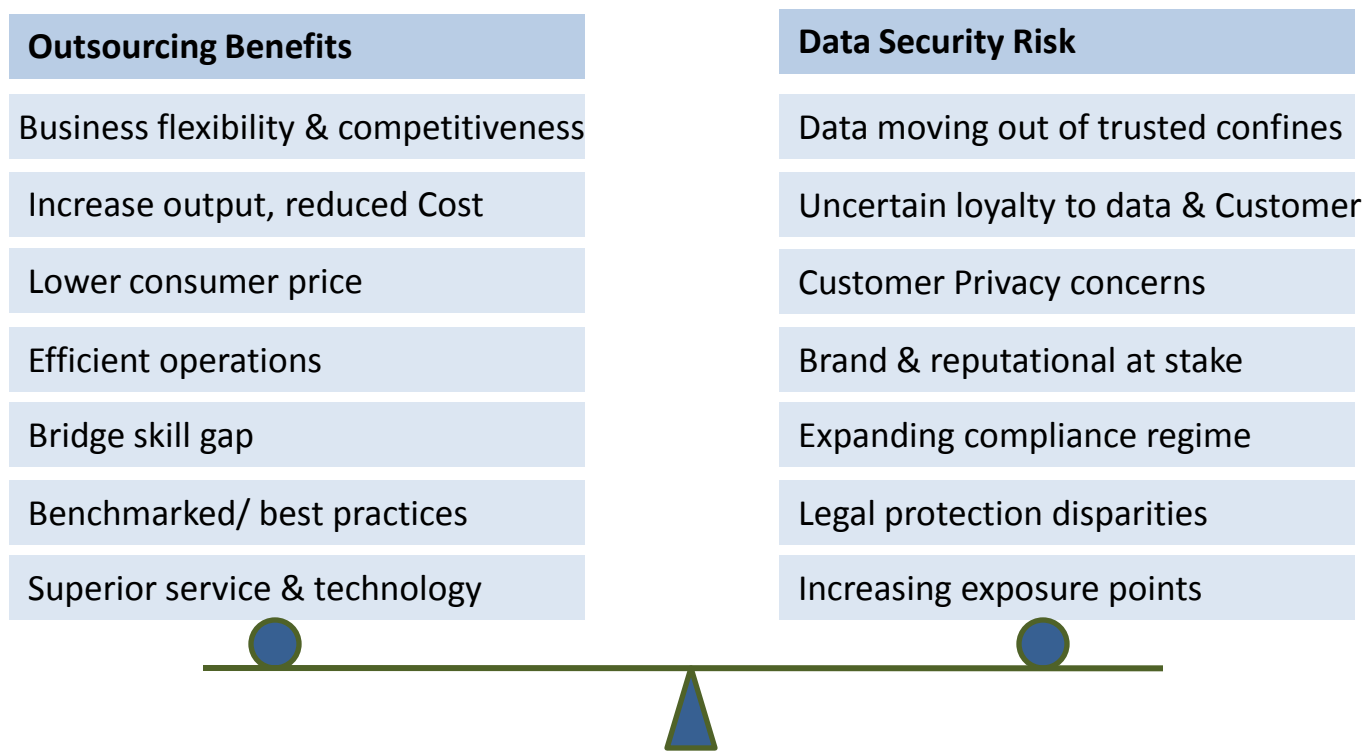
Shaadi Ringtones

Invite Friends

Need Help?

Security Tips

Outsourcing to offshore- risk to privacy?



- Protecting corporate information is difficult enough in your own environment; outsourced and offshore information exchange requires even greater scrutiny from both a technological and cultural perspective
... Security And Privacy Essentials For IT Outsourcing Deals, **Forrester**, May 08
- Strong cultural differences and perceptions around security, privacy and IP protection are probably the most difficult and insidious issues faced by global outsourcing environment.. **Gartner**, 2007

Transborder Data Flow- What and how

- Personally identifiable Information
- Personal financial information
- Business strategy documents, board presentations, MoMs etc
- Business plan, marketing plan, proposals, RFPs, presentations etc
- IPR data
- Credit Card Numbers and its authorization information
- Critical design, images, and diagrams
- Application design, product design
- Databases, data files, spreadsheets,
- Project plans, project reports etc
- Source code, libraries and reusable components etc.
- Financial information- payroll, receipts and expenditure, transaction logs and reports
- Knowledge assets, research and market analysis reports
- Media files

Access to application hosted at client side

Application hosting at outsource service provider

Access to underlying systems and servers

Direct sharing of the data for processing

Access to collaboration tools- SharePoint, mails

Access to development, test and production systems

Test data sharing

Outbound/ inbound calls to/ from client and client customers

Transborder Data Flow- Security Concerns

Call Center data theft

Trojan infection

Social Engineering

VOIP threats

Personal Information Leak

Compromised Credit Card details

Network Penetration

Botnets

Hack into servers

Credential stealing

Malware propagation

Network Sniffing

Unauthorized access

Man-in-middle attack

WLAN- Compromise

Storage Leakage

Corporate data loss

Database worms

Complex regime of Data Protection Legislations...us

Computers & Communications

- Computer Fraud and Abuse Act of 1986 (CFAA)
- The Electronic Communications Privacy Act (1986)
- Telephone Consumer Protection Act of 1991
- Communications Opportunity, Promotion and Enhancement Bill – 2006 COPE
- Telecommunications Act of 2005
- Wireless Communications and Public Safety Act (1999)
- Cable Communications Policy Act of 1984
- Cyber Security Enhancement Act of 2002
- Cyber Security Act 2009
- U.S. Safe Web Act

Children's Privacy

- **Children's Online Privacy Protection Act – 1998 (COPPA)**
- Children's Internet Protection Act of 2001 (CIPA)
- Children's Online Protection Act of 1998 (COPA)

Financial Information

- **Gramm-Leach-Bliley Act (1999)**
- Fair Credit Reporting Act (1970)
- Fair and Accurate Credit Transactions Act (2003)
- Right to Financial Privacy Act (1978)
- **Federal Trade Commission Act**
- Taxpayer Browsing Protection Act (1997)
- Electronic Funds Privacy Act (EFTA)

Privacy of Government Collections

- Census Confidentiality Statute of 1954
- **Freedom of Information Act - 1966 (FOIA)**
- **Privacy Act of 1974**
- Computer Security Act of 1987
- Homeland Security Act 2002
- US Patriot Act 2001
- E-government Act of 2002
- Federal Information Security Management Act of 2002 (FISMA)

Health / Medical Records

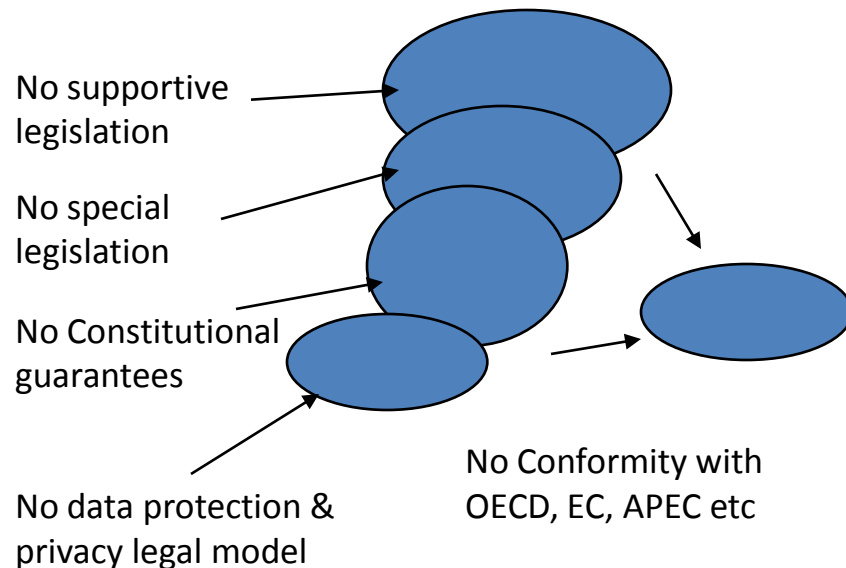
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- 21 C.F.R

Miscellaneous Records and Activities

- Administrative Procedure Act
- **Family Education Rights and Privacy Act (1974)**
- Privacy Protection Act of 1980
- Video Privacy Protection Act of 1988
- Employee Polygraph Protection Act of 1988
- Driver's Privacy Protection Act of 1994
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
- Do-Not-Call Implementation Act of 2003
- Americans with Disabilities Act (ADA)
- Consumer Credit Reporting Reform Act of 1996 (CCRRA)

India- Data Protection & Privacy Legal Model

A Spiral of Myths



Data Protection & Privacy Model

Fundamental Rights (Art.21)

Supportive Legislation(s)

- The Indian Penal Code, 1860
- The Indian Telegraph Act, 1885
- The Indian Contract Act, 1872
- The Specific Relief Act, 1963
- The Public Financial Institutions Act, 1983
- The Consumer Protection Act, 1986
- Credit Information Companies (Regulation) Act, 2005

Special Legislation(s)

- The Information Technology Act, 2000
- The Information Technology (Amendment) Act, 2008

International Conventions

- International Covenant on Civil and Political Rights, 1966
- Universal Declaration of Human Rights, 1948

Ref: Vakul Sharma, Advocate, Supreme Court

Data Protection: Sections 43A and 72A

- **New Section 43A:** Data protection has now been made more explicit through insertion of a new clause 43A that provides for compensation to an aggrieved person whose personal data including sensitive personal data may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices.
- **Penalty for breach of confidentiality and privacy:**
Under section 72A punishment for disclosure of information in breach of a lawful contract is prescribed. Any person including an intermediary who has access to any material containing personal information about another person, as part of a lawful contract, discloses it without the consent of the subject person will constitute a breach and attract punishment with imprisonment of up to three years and/or a fine of five lakh rupees. This will bring those responsible for breaching data confidentiality, under lawful contracts, to justice, and also act as a deterrent.

Improvement to include
“stealing of computer source code”

Data Protection- explicit new clause 43 A

“Compensation to an aggrieved person” whose personal data including **“sensitive personal data”** may be compromised by a company

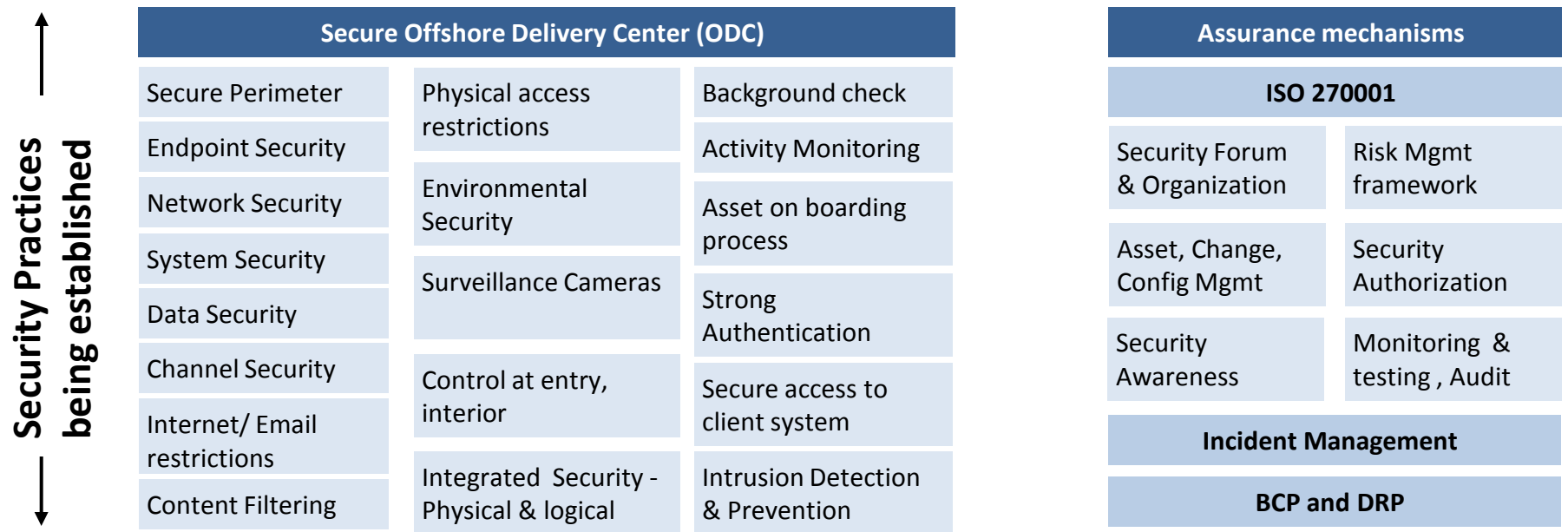
Compromised because of
“negligence in implementing or maintaining reasonable security practices”

“Disclosure without the consent” of the subject person
“will constitute a breach

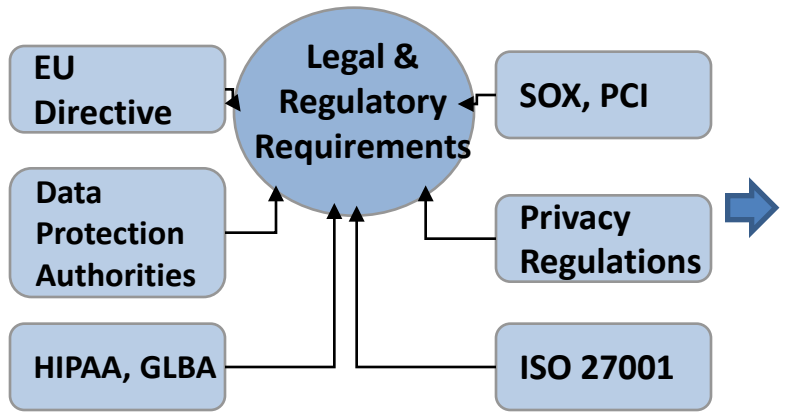
India- Data Protection & Privacy Legal Model

Privacy Principles	IT Act, 2000 and IT Act (Amendment) 2008
<p>Definitions: ‘Personal information’, ‘</p>	<p>Legal definition of ‘Personal information’ under section 43A.</p>
<p>Collection Limitation Principle: advocates limits to the collection of personal data; any such data collected should be obtained by lawful means and with the consent of the data subject,</p>	<p>Section 43A defines “sensitive personal data or information” Further section 72 A refers to punishment for disclosure of information in breach of lawful contract. Also, section 7 of the Act does refer to lawful retention of electronic records.</p>
<p>Purpose Specification Principle: The purposes for which personal data are collected should be specified at the time of data collection and limit the use for those purposes only</p>	<p>section 43 A, 72 A [Electronic Records] equivalent to purpose specification principle.</p>
<p>Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for other purposes except: (a) with the consent of the data subject; or b) by the authority of law.</p>	<p>Section 72 of the IT Act provides protection to personal data, albeit its scope is limited. Further under section 72 A disclosure of personal data is an offence,</p>
<p>Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.</p>	<p>The IT Act has defined “secure system” which (i) is reasonably secure from unauthorized access and misuse; (ii) provides a reasonable level of reliability and correct operations; (iii) (iv) adheres to generally accepted security procedures. Section 43 A [reasonable security practices & procedures]</p>

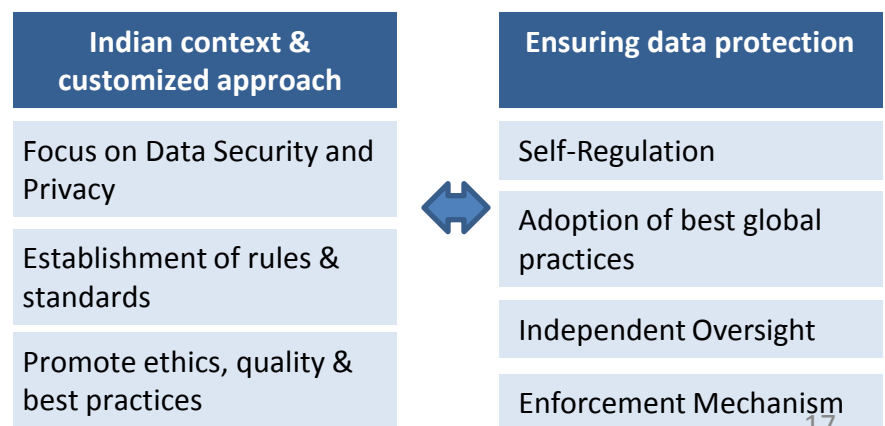
Indian IT/ ITES- Maturing security practices & ensuring industry initiative



Expanding compliance regime

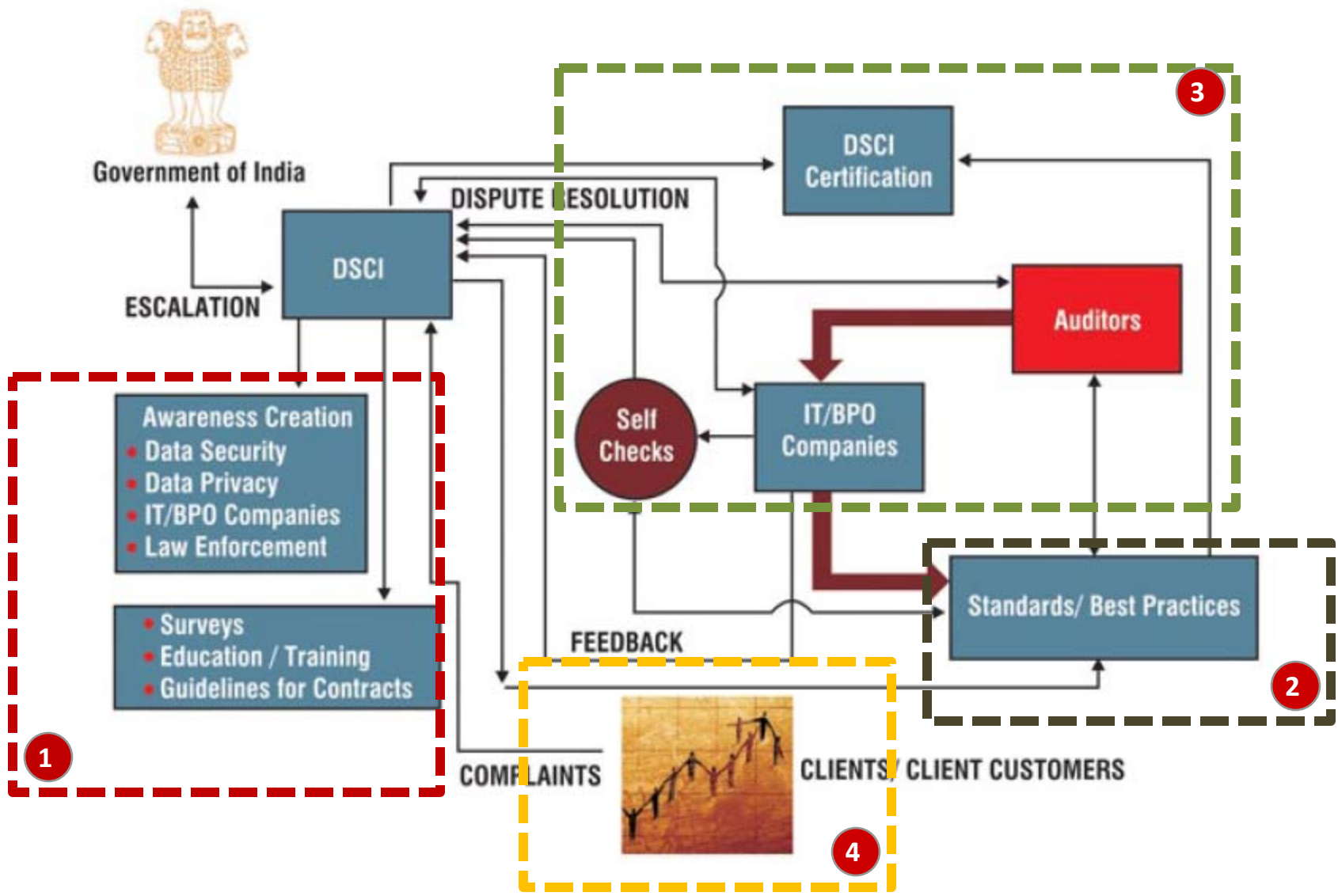


Data Security Council of India (DSCI)



DSCI as a SRO for Data Protection

DSCI SRO Framework



Privacy Landscape in India

Industry Initiative

Privacy policy & processes

Privacy techniques & technology

Customer consent, data correctness & notice

Outsourcing Industry

Biomedical- ethical guidelines

Data security & privacy initiatives

Implementation of Assurance mechanisms

Privacy Landscape

Increased customer awareness

Rising concerns over the personal data being gathered

Data Security Council of India

Self Regulatory Organization for data protection

Awareness, Best practices, enforcement & dispute resolution

Legal Model

Constitutional Guarantee

Special regulation- IT Act, IT Act (Amendment)

Supporting regulations

Conformity with international regulations

Regulatory bodies

DNCR, License condition- TRAI, DOT

Biomedical- ethical guidelines

RBI Master circular

Use of Biometrics

Private Organizations

Data Center Access

Critical system access

Ecommerce transactions

E-Governance Roadmap- \$ 6 Billion investment

Total projects- 26 mission mode + 6 support

Use of Biometrics



Biometric Passports in India by 2010

Biometric PAN card using iris scan

Plan of use of Biometric card for beneficiaries of NREG, SSP

Integrated Prisons Management Systems

Health Management Information Systems [HMIS]

Promotion of Biometrics ethics

Incorporate biometric data as a personal information – rules for IT Act (Amendment) 2008

Ethics standards for biometric use by NISG (National Institute of Smart Governance)

Awareness campaign for users, vendors, organizations and policy makers

Thank you