KHAITAN &CO

Advocates since 1911

Privacy and Data Protection in India



CONSTITUTION OF INDIA, THE BEDROCK OF PRIVACY

The Constitution of India recognises the right to privacy, that is the right to be left alone, under Article 21 of the Constitution of India which is protection of life and personal liberty. The right of privacy is only available against the State. This right is subject to reasonable restrictions under Article 19 of the Constitution of India. The case laws on right to privacy date from as far back as six decades ago.

LEGISLATIVE FRAMEWORK

Indian data protection law is still evolving. The Information Technology Act, 2000 ("IT Act") and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules") deal with protection of data in digital form. Initially the reach of the IT Rules was very wide, but a clarification issued by the Ministry of Communications and Information Technology ("Ministry of IT") by way of a press note has made these more workable. The IT Rules have brought India in line with international standards for data protection.

(a) IT Act

On 27 October 2009 two statutory provisions were added in the IT Act which deal with sensitive personal data or information and personal information. Section 43A deals with compensation for failure to protect sensitive personal data or information and Section 72A deals with personal information and provides punishment for disclosure of information in breach of a lawful contract or without the individual's consent. Both these provisions form the basis of data protection in India.

(b) IT Rules

The IT Rules were introduced on 11 April 2011 and these rules implement Section 43A of the IT Act. The IT Rules require all body corporates (organisations) engaged in commercial or professional activities to follow these rules when dealing with sensitive personal data or information.

(c) Press Note dated 24 August 2011 by the Ministry of IT.

The Press Note dated 24 August 2011 of the Ministry of IT exempts outsourcing companies in India from the requirement of collection and disclosure. It clarifies that the IT Rules deal with sensitive personal data or information and are applicable to a body corporate (organisations) located in India.

WHAT KIND OF DATA IS COVERED UNDER THE IT RULES?

Sensitive personal data or information consists of the following:

(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; and

(vi) Biometric information;

This would also include details relating to any of these items. The definition of sensitive personal data or information may vary in different jurisdictions. In UK racial and ethnic origin, political affiliation and religious orientation are defined as sensitive personal data; however, in India these do not qualify as sensitive personal data or information. Personal information has been defined under the IT Rules as information that relates to a natural person which is capable of identifying such

person. However, the IT Rules only deal with sensitive personal data or information.

THE FIVE ESSENTIAL PRINCIPLES

(a) What should a privacy policy contain?

All body corporate (organisations) in India possessing, dealing and handling sensitive personal data or information have to provide for a clear and accessible privacy policy on the website giving a statement of its practices with regard to collection, disclosure, type of sensitive personal data collected, purpose of collection, usage and reasonable security practices.

(b) What does collection entail?

Before collection of sensitive personal data or information a body corporate (organisation) is required to take a written consent of the individual (opt-in consent) and also follow the collection requirements like lawful purpose, knowledge, retention, review, opt-out and grievance officer when dealing with sensitive personal data or information. Written consent can be obtained by letter, email, fax or any other electronic mode.

(c) Can data be disclosed?

Disclosure to third parties is permitted with prior permission or by contract with the individual. However no consent is required from the individual if the disclosure is to comply with a legal obligation, to a government agency or by an order under law.

(d) Can data be transferred?

Transfer within India or outside India of sensitive personal data or information is permitted if the same level of data protection is adhered to by the body corporate (organisation) to whom the data is being transferred. Transfer can only be by consent or by a contract with the individual.

(e) What kind of security practices are required?

All body corporate (organisations) in India dealing with sensitive personal data or information are required to follow reasonable security practices. The international standard (IS / ISO / IEC 27001) is recommended or an association can have its code of best practices approved and notified by the Government of India. Compliance of reasonable security practices is ensured by yearly audits through independent auditors approved by the Government of India.

WHO IS EXEMPT?

Outsourcing companies in India under a contractual obligation with a legal entity within India or outside India are exempt from the requirement of Rule 5 (Collection of Information) and Rule 6 (Disclosure of Information). Outsourcing companies in India however cannot be exempt from the requirements under Rule 6 with regard to disclosure under a legal obligation, sharing of information with government or any order by court. Of course the outsourcing companies in India have to follow the rest of the IT Rules.

BENEFITS OF THE NEW LAW

(a) Allows individuals to exercise their rights like review of data, right to withdraw (opt-out);

(b) Provides for independent investigation by government approved auditors to ensure compliance of reasonable security practices;

(c) Gives comfort to customers of the outsourcing industry that their data is secure as these rules contain adequate data security safeguards.

© KHAITAN & CO, 2013
FOR PRIVATE CIRCULATION ONLY

This Primer provides some basic information pertaining to the issues and should not be construed as a legal opinion or legal advice. It may neither be relied upon by any person for any purpose, nor is it to be quoted or referred to in any public document or shown to, or filed with any government authority, agency or other official body.

If you would like further information or specific advice please contact: primers@khaitanco.com

Bangalore
Simal, 2nd Floor
7/1 Ulsoor Road
Bangalore 560 042, India

T: +91 80 4339 7000
F: +91 80 2559 7452
E: bangalore@khaitanco.com

Kolkata
Emerald House
1B Old Post Office Street
Kolkata 700 001, India

T: +91 33 2248 7000
F: +91 33 2248 7656
E: kolkata@khaitanco.com

Mumbai
One Indiabulls Centre
13th Floor, Tower 1
841 Senapati Bapat Marg
Mumbai 400 013, India

T: +91 22 6636 5000
F: +91 22 6636 5050
E: mumbai@khaitanco.com

New Delhi
Ashoka Estate, 12th Floor
24 Barakhamba Road
New Delhi 110 001, India

T: +91 11 4151 5454
F: +91 11 4151 5318
E: delhi@khaitanco.com

www.khaitanco.com