

IAMAI Directive on Data Protection and Privacy

-Vakul Sharma

Introduction

‘Data protection’ is about the collection, maintenance, use and dissemination of personal information. Over the years data protection has gained prominence on account of technological advances and its effect on safeguarding personal information. It is significant to note that the use that is made of personal data, the interests of the individual and the interests of society may conflict and need to be resolved in the same way as in the context of individual liberty. With data protection the solution must take the same form: a balance must be found between the interests of the individual and the interests of the rest of society, which include the efficient conduct of industry, commerce and administration (governance).

An underlying purpose of the data protection principles is to protect privacy with respect to the processing of personal data. That is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and obligations on those who process data, or who exercise control over such processing.

One of the major policy objectives of data protection is the application of fair information practices, an organized set of values and standards about personal information defining the rights of record subjects and the responsibilities of record keepers. This is an important subset of privacy law.

Since, common law does not know a general right of privacy and the Indian Parliament has so far been reluctant to enact one. However, it is felt by IAMAI to encourage members to address consumer concerns regarding online privacy through self-regulation. Effective self-regulation remains desirable because it allows companies to respond quickly to technological changes and employ new technologies to protect consumer privacy. Accordingly, a private-sector response to consumer concerns that incorporates widely-accepted fair information practices and provides for effective enforcement mechanisms could afford consumers adequate privacy protection.

Data Protection and Privacy: A Self-regulatory Approach

IAMAI believes self-regulation is the least intrusive and most efficient means to ensure fair information practice, given the rapidly evolving nature of Internet and computer technology.

We are hopeful that self-regulation will achieve adequate online privacy protections for consumers. This Directive is an attempt on the part of IAMAI to demonstrate that it has developed and demonstrate broad-based and effective self-regulatory programs.

This Directive is, in accordance with cultural and legal traditions and practices of India and may play a valuable role in safeguarding public interests' vis-à-vis individual liberty and thereby could usefully complement regulation in the context of the future development of new media services.

This Directive represents a form of privacy protection to be adopted by IAMAI members.

This Directive may be known as IAMAI Directive on Data Protection and Privacy.

Article 1 Objective of the Directive

In accordance with this Directive, Members shall protect the fundamental rights of natural persons as enshrined under the Constitution of India, and in particular, their right to privacy with respect to the processing of personal data.

Article 2 Definitions

For the purpose of this Directive:

“**Access**”, with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

“**Computer**” means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

“**Computer Network**” means the inter-connection of one or more computers through-

- (i) the use of satellite, microwave, terrestrial line or other communications media; and
- (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

“**Computer system**” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

“**Data**” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized 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;

“**Computer database**” means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

“**Consumer**” means any natural person who is acting for purposes, which are outside his trade or profession;

“**Disclosure**”, in relation to data, includes disclosing information extracted from the data.

“**Electronic form**”, with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device;

“**Information**” includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

“**Personal data**”, means data consisting of information, which relates to a living individual who can be identified from that information (or from that and other information in the possession of the member or any data user).

“**Processing**”, in relation to data, means amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of those operations by reference to the consumer.

“**Recipient of the service**”, means any person who, for professional ends or otherwise, uses any information service, in particular for the purposes of seeking information or making it accessible;

“**Record**”, means any item, collection or grouping of information about a consumer that is maintained by a member – including but not limited to, his education, financial transactions, disposable income, preferences, marital status, family details, browsing habits and that contains his name, or the identifying number, symbol or other identifying particulars assigned to the consumer.

Article 3 Application

This Directive apply to the processing of the personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 4 Scope

The scope of the Directive to cover all information and content related services using electronic means using computer, computer system or computer network between businesses and between businesses and consumers, even if those services are being provided free of charge to the recipient.

Article 5 Principles relating to data collection, quality and purpose

Member shall provide that personal data undergoing automatic processing shall be:

- (a) obtained and processed fairly and lawfully;
- (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
- (d) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 Consumers Right

At the *option* of the member, a consumer shall have the right:

- (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him;
- (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Article 7 Information to the Consumers

Member to inform consumers of privacy risks presented by use of the services before they subscribe to or start using services. Such risks may concern data integrity, confidentiality, the security of the network, or other risks to privacy such as the hidden collection or recording of data.

Article 8 Data Security

Member shall use appropriate procedures and available technologies, preferably those that have been certified, to protect the privacy of the consumers concerned especially by ensuring data integrity and confidentiality as well as physical and logical security of the network and of the services provided over the network.

Member shall establish appropriate administrative, technical and physical safeguards to insure security and confidentiality of records stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

Article 9 Use of technology

Member while using technology to provide effective privacy protection, should use such technologies which must meet the following conditions:

- (a) technology respecting fair information practices must exist;
- (b) these technologies must be deployed; and
- (c) the implementation of these technologies must have a privacy protecting default configuration.

Article 10 No disclosure without consent

No member shall disclose any record of a user which is contained in a system of records by any means of communication to any person, *except* pursuant to any agreement, terms of service condition, written request by, or with prior written request of, the individual to whom the record pertains.

Article 11 Exemptions

Notwithstanding anything contained in Article 10, a member shall have a right to disclose personal data of a consumer in order to maintain:

- (a) sovereignty or integrity of India;
- (b) security of the State;
- (c) friendly relations with foreign States;
- (d) public order; or
- (e) prevention of incitement to the commission of any cognizable offence,

to any such competent authority or officer on receipt of a written request from such competent authority or officer.

Article 12 General Exemptions

In addition to the exemption(s) as granted under the Article 11, the following categories of individuals and/or data users are also exempted from the 'no disclosure without consent' rule as enumerated in Article 10:

- (a) To those officers and employees of the member which maintains the record who have a need for the record in the performance of their duties.
- (b) With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.
- (c) To a recipient who has provided the member with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.
- (d) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.
- (e) Pursuant to the order of a court or authority of competent jurisdiction.

Article 13 Disclosure record

Each member, with respect to each system of records under its control, must keep a record of the date, nature, and purpose of each disclosure of a record to any person, or competent authority and the name and address of the person or competent authority to whom the disclosure is made.

Article 14 Accountability

A member may be held accountable for not complying with measures, which give effect to the principles stated above.

Article 15 Consumer Complaint Redressal

IAMAI to appoint an independent counselor to accept consumer complaints related to data protection and privacy violation against any member.

It shall be the responsibility of the independent counselor to proactively investigate, and initiate proceedings against such privacy violators.

Article 16 Measures

In order to attain the effectiveness of this Directive, the following actions supporting and promoting measures to be taken in by the Member

- promotion of members' self-regulation and content-monitoring schemes.
- Encouraging members to provide filtering tools and rating systems, which allow parents and teachers to select content appropriate for children in their care while allowing adults to decide what legal content they wish to access.
- Increasing awareness of services provided by members among consumers.
- Supporting actions such as assessment of legal implications.
- Restricting the circulation on the Internet and/or mobile devices of illegal or harmful content.
- Activities fostering international cooperation in the areas enumerated above.