Foundation of Data Protection Professionals in India
[Section 8 Company limited by Guarantees]
[CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK First Stage, Second Block, Bangalore 560050
E mail: fdppi@fdppi.in: Ph: 08026603490: Mob:+91 8310314516

Date: 20th January 2019

To

The Ministry of Electronics and Information Technology
Room No 4016, Electronics Niketan
6 CGO Complex, CGO Complex
Lodhi Road
New Delhi 110003

Sub: Comments on the Draft Intermediary Guidelines

This has reference to the feedback sought from the General Public in respect of the Draft Intermediary Guidelines 2018.

We are pleased to provide our considered feedback in this respect.

We hope these suggestions would be useful. We will be happy to provide any further clarifications on the thoughts expressed here.

Thanking You

For Foundation of Data Protection Professionals in India

Chairman
(Na.Vijayashankar)

Foundation of Data Protection Professionals in India
[Section 8 Company limited by Guarantees]
[CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK First Stage, Second Block, Bangalore 560050
E mail: fdppi@fdppi.in: Ph: 08026603490: Mob:+91 8310314516

Date: 20th January 2019

Comments on the Draft Intermediary Guidelines 2018

The following are the comments from FDPPI on the draft Intermediary Guidelines 2018 released by the Government for public comments.

These take into account the contents of

a) Section 79 as per the ITA 2000 amended in 2008 and notified on 27th October 2009
b) Information Technology Intermediary Guidelines 2011 which is sought to be amended now
c) Information Technology (Guidelines for Cyber Café) Rules, 2011
d) Clarification issued by MEITY on 18/3/2013
e) Advisory issued on Matrimonial websites on 6th June 2016
f) Advisory issued on measures to curb online Child sexual abuse material on 18th April 2017

Apart from providing our views on the specific modifications now proposed by the Ministry, we would like to also provide some additional long term suggestions which may be considered as part of the current modifications.

General Comments

"Intermediaries" as defined in ITA 2000 are a very important segment of the economy as well as the security eco system of the nation. Regulating intermediaries is critical for Cyber Crime control as well as reducing the possible misuse of Internet by criminals, terrorists and foreign powers.

Intermediaries are also important from data protection requirements since they also control the BFSI, Health and Social Media sectors.

Therefore it is essential that Intermediaries are regulated effectively.

Since there are different types if intermediaries which may include Cyber Cafes, Matrimonial Websites, Mobile App companies, Mobile or Internet Gaming Companies, etc besides the more visible Fintech, Health care and Social Media companies, the umbrella regulations

have to be flexible enough to be supplemented by the additional sector specific guidelines. Otherwise the regulations would seek a lower common denominator or face legal challenge as unfair restrictions.

Keeping these requirements in mind, the following suggestions have been made which includes assigning the responsibility to the ssDirector General of IN-CERT to issue security guidelines as and when required for specified types if intermediaries and an **"Intermediary Dispute Resolution Policy".**

Suggestions

Rule 2: to be modified to include the definition of "Intermediary Dispute Resolution Policy" (IDRP) as follows:

> 2(m) : "Intermediary Dispute Resolution Policy" (IDRP) means a policy as defined under rule 14 below of this notification.
> 2(n): "Intermediary Dispute Resolution Center" (IDRC) means an organisation that is registered with the MEITY for the purpose of resolving any disputes arising out of compliance related to Section 79 of ITA 2000/8 (Information Technology Act 2000) and the rules and regulations issued under an IDRP adopted by the organization.
>
> 2(l) to be modified as under
>
> "User" means any person who avails the services of an Intermediary and conforming to the requirements under Section 79(2)(a) and 79(2)(b), of ITA 2000/8, which service includes, hosting, publishing, sharing, transacting, displaying or uploading information or views either on any computing platform including the mobiles.

Rule 3(1) to be modified as under:

The intermediary shall publish on the website where the services are offered to public

a) Terms of Use of the services and an appropriate Privacy Policy
b) Disclosure of ownership of the service.
c) Disclosure of registration under data protection laws if any.
d) Designated Grievance Officer as a single point of contact for the public and the Grievance redressal Mechanism applicable for resolution of any disputes.
e) Any other information relevant for the provision of the service.

Rule 3(2) to be modified as under:

A) **The terms of use** referred to under rule 1 shall include a notification to the users of the services of the intermediary that

The user shall use the services responsibly and shall take reasonable precautions

i) not to use the services in a manner that threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or

causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation

ii) not to use the services in a manner that threatens public health or safety; promotion of cigarettes or any other tobacco products or consumption of intoxicant including alcohol and Electronic Nicotine Delivery System (ENDS) & like products that enable nicotine delivery except for the purpose & in the manner and to the extent, as may be approved under the Drugs and Cosmetics Act, 1940 and Rules made thereunder;

iii) not to use the services in a manner that threatens critical information infrastructure.

iv) Not to Impersonate another person or deceives and mislead about the origin of any message or communication

v) Not to cause harm to minors

vi) Not to cause infringement of intellectual property rights such as Copyright, Trademark or Patent

vii) Not to cause distribution of any content that contains a computer contaminant/virus/malware or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

viii) Not to cause a wrongful harm to any person

B) **The Privacy Policy** referred to under rule 1 shall be compliant with the data protection laws as applicable and ensure that identifiable personal data

i) Shall be collected only to the extent necessary for the purpose of delivering the service,

ii) Shall be processed in a fair and reasonable manner that protects the Privacy of the user, for purposes that are clear, specific and lawful and only for purposes specified or for any incidental purpose

iii) Shall be retained only for the time required for fulfilling the purpose of collection unless otherwise justified by legitimate interest of the intermediary or for other legal obligations.

iv) Shall be used otherwise in complete compliance of the data protection laws as applicable

C) **The Privacy Policy and Terms of Service** referred to under rule 1 shall be compliant with the security guidelines issued by the IN CERT as applicable to the intermediary or the category of activity to which the intermediary may belong.

Rule 4: to be modified as under:

(4)

(a) The intermediary shall ensure that every user has a registered communication address through e-mail or a communication device that is verified for its correctness.

(b) An intermediary who provides an e-mail address or such other identity on the internet as a service, shall adopt such reasonable precautions as may be necessary to prevent impersonation.

(b) The intermediary shall inform its **users at least once every month, at the time of the user logging in to avail the service,** that in case of noncompliance with rules, regulations, user agreement and privacy policy for access or usage of the intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users and also remove noncompliant information.

(c) Where the user does not log in to avail the services for more than a month, a reminder as above shall be sent through E-Mail or as a message through a communication device at least once every year.

(d) Where the communication with the user through the E Mail or the communication device fails due to incorrect address of the recipient, the intermediary shall deactivate the user account until the user opts to re-activate the account.

Rule 6: to be modified

The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 **or such other security measures that may be prescribed under the data protection laws or by the Indian Computer Emergency Response Team (IN-CERT) as may be relevant.**

(P.S: Section 43A is expected to be deleted after PDPA 2018 becomes a law. Hence the Reasonable Security Practices and Procedure rules 2011 may be infructuous)

Rule 7: to be modified

The intermediary who has more than fifty lakh **registered users with identifiable location in India** or is one of intermediaries **specifically notified** by the government of India shall:

(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;

(ii) have a permanent registered office in India with physical address;

(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.

(iv) Register itself as an Intermediary with the IN-CERT with a self certified confirmation of compliance to this guideline **not later than three months** from the date of this notification with the details mentioned in para (iii) above and details of registration if any under any other law such as the data protection act if applicable.

(v) Submit an annual confirmation about the continued compliance with updated information required to be filed under para (iv) above.

Rule 8: to be modified as under

(a) The intermediary

i) upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency under section 79(3)(b) of Act

ii) about any unlawful acts relatable to Article 19(2) of the Constitution of India such as those in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States,

public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource,

shall remove or disable access to that information without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3.

(b) Further the intermediary shall preserve such information and associated records such period as may be required by the court or by government agencies who are lawfully authorised or on receipt of cancellation of the requirement by a subsequent order.

(c) Any deletion of the information under this rule without a confirmation from the relevant Court or the Government authority may be liable to be considered as destruction of evidence.

Rule 9: to be modified as under:

The Intermediary shall deploy such technology based automated tools or appropriate mechanisms, with appropriate controls, for **reasonably** identifying unlawful information or content on a proactive basis and flagging the content as **"Considered Inappropriate"**.

Such content flagged as "Considered inappropriate" shall be referred to the Grievance officer for the purpose for further action.

The Grievance officer shall record his/her views in writing and initiate further action as follows..

(a) If the Grievance officer considers that the information is not to be flagged as inappropriate, he shall record his views as a "Compliance Note" and the information shall be retained with suitable tag as may be considered necessary and the compliance note shall be made available for any security audit by the regulatory authorities if required.

(b) If the grievance officer concludes that the content is inappropriate, or he is unable to come to a conclusive decision to retain the same, he shall place the specific content under temporary obfuscation and refer it to the Competent Authority under Section 69 or 69A of Information Technology Act 2000 as may be relevant, for further instructions and act in accordance with the instructions received there from.

(c) If the Competent authority does not confirm the removal of the information for a period of one week from the date of report, the information shall be reinstated.

(d) If the competent authority confirms that the information shall remain removed, it shall be archived for legal requirement for a period not less than 3 years.

(e) While placing any inappropriate content under temporary obfuscation or removal, the intermediary shall ensure that only the part of the content which is considered inappropriate shall be obfuscated or removed and not the entire content of which the objectionable aspect is a part.

(f) Where there is any requirement for blocking of a large part of a content or removal of an entire URL, such decision shall be as determined by the competent authority.

Provided that this rule does not authorize the intermediary for decryption of encrypted information except under the requirement of an appropriate authority authorized under Section 69 of ITA 2000.

Rule 10: to be modified as under:

The intermediary shall initiate an effective Cyber Security incident report system that recognizes any event within its technical environment that is likely to cause harm to any user and report such cyber security incidents with relevant information to the Indian Computer Emergency Response Team within a reasonable time not exceeding 7 days from becoming aware of an incident.

Rule 11: to be modified as under:

The intermediary shall not knowingly deploy or install in or modify the technical configuration of the **user's** computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein **subject to it being installed only with the informed consent of the user.**

Rule 12: to be modified as under:

The intermediary shall institute an appropriate dispute resolution system and publish the details thereof in its website which shall include appointment of a Grievance Redressal officer whose contact details shall be provided on the website.

The Grievance Officer shall acknowledge the complaint and initiate action for redressal expeditiously and take such measures as may be necessary to resolve any Complaints received related to its service ordinarily within one month from the date of receipt of complaint.

The Intermediary may designate an appropriate "Ombudsman" to assist the user in resolving his complaint and also initiate action for "Mediation" and "Arbitration" as per the provisions of the relevant laws in India preferably through an Online Dispute Resolution system .

The applicable laws, the jurisdiction of supervisory Courts and place of offline arbitration shall be in India .

Rule 13: can be modified as under:

1. Since

a) there are certain advisories already issued subsequent to the issue of the Intermediary guidelines of 2011 which is presently being modified, and which are applicable to certain special categories of Intermediaries such as the need to block online Child Sexual Abuse Material, or comprehensive guidelines applicable to Cyber Cafes or Matrimonial Websites,
b) There would be other guidelines issued under the Proposed Data Protection Act or under E Commerce Regulations or other regulations, which may directly or indirectly be in conflict with these guidelines,
c) There may be other intermediary specific or sector specific due diligence guidelines that may be issued from time to time,

It is necessary to clarify as follows through modification of Rule 13 as follows:

(i) Further to the general guidelines contained herein applicable to all intermediaries, specific advisories released in respect of special categories of intermediaries such as Online Child Sexual Abuse Material or on Matrimonial Websites or any similar notifications shall continue to be applicable even after the new guidelines come into force.
(ii) The guidelines issued hereunder are only in the nature of minimal due diligence to be observed by intermediaries and does not restrict the legal responsibilities of the intermediary under any other Act including the Information Technology Act 2000 or such other relevant laws like Data Protection Act, Laws or Regulations related to E Commerce, Banking, Finance, Telecom, Health or Insurance information issued by the respective regulators etc.

Rule 14: to be introduced

Notwithstanding what is contained above, an intermediary at his sole option may opt to adopt the “Intermediary Dispute Resolution Policy “ (IDRP) as defined here under.

a) The Intermediary Dispute Resolution Policy may be created and defined by a “Intermediary Dispute Management Center” (IDMC) that intends to specialize in resolving consumer disputes related to the use of Intermediary services and registered with the IN-CERT
b) Any Intermediary can voluntarily associate itself to an “Intermediary Dispute Management Center” and adopt the Intermediary Dispute resolution Policy of that Center.

c) The IDRP shall represent the basic commitment provided by the Intermediary for compliance of the Act and other legal obligations and may include intermediary specific policies as may be required.
d) After adoption of IDRP the Intermediary may disclose the same in its terms and conditions and the Privacy Policy that it shall bind itself to the IDRP of the designated IDMC and that such IDRP shall also be binding on the users. It shall also inform the users that all disputes relating to the service shall be subject to the resolution through an Ombudsman/Mediator/Adjudicator as determined by the policy of the IDMC without any prejudice to the supervisory authority of any Court in India.
e) Adoption of the IDRP as a means of defining the Terms and Privacy Policy and it may restrict its policy declarations to only the functional aspects of its service which will supplement the IDRP.
f) Use of IDRP shall be purely voluntary on the part of the Intermediary.
g) The IN-CERT will receive the necessary applications from intending IDMC s along with their self developed "Dispute Resolution Policy Disclosure Document" and upon satisfaction, shall list such an agency as an accredited IDMC. Such approvals will be provided by a committee headed by the Secretary MEITY and consisting of the Director General of CERT-IN with three co-opted members from the industry with adequate experience and reputation.

Rule 15: To be introduced:

Since the guidelines require certain technical changes to be implemented by the industry, it is preferable if a "Compliance Date" is fixed with a time of about 3 months given to the intermediaries to comply and report compliance.

Hence a Rule 15 shall be introduced stating

These guidelines will come into effect 3 months from the date of this notification.

For Foundation of Data Protection Professionals in India

Chairman