The Information Technology
[Intermediaries Guidelines (Amendment) Rules]
2018

1. **Short title and commencement** — (1) These rules may be called the Information Technology [Intermediaries Guidelines (Amendment) Rules, 2018. (2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions** — (1) In these rules, unless the context otherwise requires,--

   (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
   (b) "Appropriate Government" means appropriate Government as defined in clause (e) of sub-section (1) of section 2 of the Act;
   (c) "Communication link" means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item; the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element;
   (d) "Computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
   (e) "Critical Information Infrastructure" means critical information infrastructure as defined in Explanation of sub-section (1) of section 70 of the Act;
   (f) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
   (g) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
   (h) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;
   (i) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub-section (1) of section 70B of the Act;
   (j) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
   (k) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
   (l) "User" means any person who accesses or avails any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary;

   (2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. **Due diligence to be observed by intermediary** — The intermediary shall observe following due diligence while discharging his duties, namely: —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person
(2) Such rules and regulations, privacy policy ~~terms and conditions~~ or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a) belongs to another person and to which the user does not have any right ~~to~~;

(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonates another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) 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.

(j) 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;

(k) threatens critical information infrastructure.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

Provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule(2):

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

~~(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,~~[1]

(4) The intermediary shall inform its users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.

(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.

(6) 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.

(7) The intermediary who has more than fifty lakh users in India or is in the list 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; and

(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.

(8) The intermediary 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 shall remove or disable access to that unlawful acts relatable to Article 19(2) of the

[1] This sub-rule has been modified as per Supreme Court Judgment in the matter of Shreya Singhal Vs UOI dated 24.03.2015.

Constitution of India such as 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 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. Further the intermediary shall preserve such information and associated records for at least ~~ninety days~~ one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.

(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content

(10) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(11) The intermediary shall not knowingly deploy or install or modify the technical configuration of 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.

(12) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule (3) can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint;

(13)The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.