Digital India
Power To Empower

Azadi Ka Amrit Mahotsav

MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA
सत्यमेव जयते

OPEN, SAFE & TRUSTED AND ACCOUNTABLE INTERNET

FREQUENTLY ASKED QUESTIONS (FAQs)

on PART II of
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Table of Contents

Frequently Asked Questions (FAQs)
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Introduction

In order to ensure an Open, Safe & Trusted Internet and accountability of intermediaries including the social media intermediaries to users, Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter referred to as "IT Rules, 2021") on 25th February, 2021.

These Rules prescribe the due diligence to be followed by all intermediaries as well as the additional due diligence to be followed by significant social media intermediaries.

The Rules also provide guidelines to be followed by publishers of news & current affairs and also online curated content providers.

These Rules supersede the earlier notified Information Technology (Intermediaries Guidelines) Rules, 2011. The Rules are available at

https://egazette.nic.in/WriteReadData/2021/225464.pdf

The Rules have two segments:

(i) Intermediary Guidelines (Part-II of the Rules, except rule 5*) administered by MeitY.

(ii) Digital Media Ethics Code (Part-III of the Rules) administered by the Ministry of Information & Broadcasting (MIB) in line with the distribution of subjects under the Government of India (Allocation of Business Rules), 1961.

* Rule 5 in Part-II is related to due diligence to be observed by an intermediary in relation to news and current affairs content made available on their platform by such publishers and shall be administered by MIB, Govt. of India.

The following FAQs have been prepared to bring clarity as well as to explain the nuances of the due diligence to be followed by intermediaries. The FAQs are limited to Part II of these Rules to be administered by MeitY. For the purposes of this document, these Rules will be referred to as "**IT Rules, 2021**".

Note: This document is in response to general queries received by MeitY. It is not a legal document and in no way whatsoever replaces, amends or alters any part of the IT Act/ IT Rules, 2021.

The FAQ is an evolving document and hence the versions of this document may undergo changes. It is requested that the concerned stakeholders verify the version of this document from MeitY.

Section I: Basic Information

1. Why were the erstwhile Information Technology (Intermediaries Guidelines) Rules of 2011 revised with the new IT Rules, 2021?

Ans: In order to ensure an Open, Safe & Trusted Internet and accountability of intermediaries including the social media intermediaries to users and in tune with the changing requirements, the Rules have been revised.

Some of the reasons which led to the introduction of the IT Rules, 2021 are as follows:

- Two significant Supreme Court orders on 11th December, 2018 in the Prajwala matter *[In Re: Prajwala letter dated 18.2.2015* Videos of Sexual Violence and Recommendations– *SMW (Crl.) No(s).3/2015]* and on 24th September, 2019 in the Facebook transfer petition *[Facebook Inc. v Union of India & Ors. Transfer Petition (Civil) Nos 1943-1946 of 2019]* besides other court judgements;
- The Right to Privacy being confirmed as a fundamental right by the Supreme Court in *Justice KS Puttaswamy (Retd.) & Anr. vs. UOI & Ors. [(2017) 10 SCC 1].*
- Commitment given in the Parliament on 26th July, 2018 on prevention of misuse of social media platforms in view of concerns raised by members;
- Recommendations made by the Rajya Sabha Ad-hoc Committee on Pornography in February 2020;
- Growing concerns of safety and security of users particularly women and children on the internet, wherein the victims had no forum for redressal of their grievances;
- Significant expansion of online intermediary ecosystem;
- Growth of online social media platforms and their influencing capabilities;
- International developments in social media regulation;
- Compelling need to have a framework to deal with fake/hate messages which have become viral and have resulted in riots, mob lynching or other heinous crimes including those concerning dignity of women and sexual abuse of children;

- Alignment with the requirements of the Law Enforcement Agencies (LEAs) and other Appropriate Governments or their agencies;
- Need to contemporize the intermediary liability framework.

2. Since when the Rules have come into effect?

Ans: The Rules have come into effect from the date of their publication in the Gazette (i.e., 25th February, 2021). The threshold criteria [Ref. rule 2(1)(v)] for significant social media intermediaries (SSMI) was published on 26th February, 2021. Additional due diligence for SSMI have come into effect from 26thMay, 2021.

3. What process was followed for amendments in the erstwhile Information Technology (Intermediaries Guidelines) Rules, 2011?

Ans:

- MeitY proposed amending the erstwhile Information Technology (Intermediaries Guidelines) Rules, 2011 and invited public comments on the draft new Rules on 24.12.2018**.**
- Based on public comments as well as suggestions received during various stakeholders' meetings, and also taking into account the change of Allocation of Business Rules (AoBR) of MIB in November, 2020, the Rules were finalised and integrated as one common set of Rules, namely the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021" replacing the earlier Information Technology (Intermediaries Guidelines) Rules, 2011.

4. What are the major changes in the Rules over the erstwhile Information Technology (Intermediaries Guidelines) Rules, 2011?

Ans: Some of the significant changes in the IT Rules, 2021 as applicable to the intermediaries are:

(a) Intermediary due diligence now includes:

- Due diligence to be followed by all intermediaries (rule 3).
- Additional due diligence requirements for SSMI (rule 4).
- Additional due diligence rules, as applicable, for other intermediaries as and when specifically notified by the Central Government (rule 6).

(b) Increased User Safety: Provision for direct requests by the affected individuals for content takedown in specific cases of content relating to breach of bodily privacy, impersonation, morphed imagery of the concerned individual in order to address the immediate need to prevent harm and emotional distress, particularly in instances of revenge porn and other similar cases [Ref. rule 3(2)(b)].

(c) Alignment with the Supreme Court's Order in Prajwala case (for SSMIs):

- The Supreme Court in a suo motu writ petition (Prajwala case), in its order dated 11/12/2018, had observed that the Government of India may frame necessary guidelines to eliminate child pornography, rape and gang-rape imageries, videos and sites in content-hosting platforms and other applications.
- The new IT Rules, 2021 provide that the SSMI should make an endeavour to deploy technology-based measures for identification of above such content available on their platform, in accordance with the safeguards provided in these Rules [Ref. rule 4(4)].

(d) Revision in terms and conditions offered to users by the intermediaries:

- The terms and conditions have been made clearer, simpler and revised to reflect emerging issues.

(e) Clear timelines have been provided for:

- Grievance Redressal: 24 hours for acknowledgement/15 days for disposal [rule 3(2)].

- Information takedown from platform upon actual knowledge based on court order or notice from appropriate government authorised by law: 36 hours [rule 3(1)(d)].
- Providing information on a lawful request: 72 hours [rule 3(1)(j)].
- Removal of revenge porn (sexual extortion/non-consensual porn publication/sexual act or conduct involving impersonation, etc.) and other similar content: 24 hours [rule 3(2)(b)].

5. How do these Rules enhance the safety of women and children?

Ans: The new IT Rules, 2021 have a clear objective of enhancing online safety of users, particularly women & children. Various provisions of these Rules focus on enhanced safety of women and children. These include:

- Specific inclusion of certain requirements to be explicitly conveyed in the terms and conditions [rule 3(1)(b)].
- Reporting by the aggrieved individual in respect of revenge porn and similar content breaching physical privacy and taking action within 24 hours for content removal [rule 3(2)(b)].
- Enhanced grievance redressal mechanism by intermediaries [rule 3(2)(a)].
- Additional provision for SSMI to appoint a Resident Grievance Officer, a Chief Compliance Officer and a nodal contact person, all to be residents in India; and a physical contact address of the significant social media intermediary to be in India [rule 4(1) and 4(5)].
- The Rules also have provisions that intermediaries shall cooperate with Law Enforcement Agencies (LEA) to identify the first originator of information related to rape, sexually explicit material or child sexual abuse material (CSAM) for investigation and prosecution [rule 4(2)].
- The significant social media intermediaries shall endeavour to deploy technology-based measures to identify any imagery of child sexual abuse, rape, etc. whether real or simulated in accordance with the safeguards in the Rules [rule 4(4)].

6. Do these Rules affect the right to privacy of individuals?

Ans: Privacy is a fundamental right in India. The IT Rules, 2021 are consistent with this fundamental right. The Rules, therefore, have a clear focus on protecting online privacy of individuals. Various provisions of these Rules, as stated in Part-II, focus on the protection of privacy. These include:

- Intermediaries are required to convey to users that they should not share information that is invasive of another person's privacy, including bodily privacy [rule 3(1)(b)].
- Intermediaries are required to periodically inform users that in case of non-compliance with their privacy policies, the intermediary has the right to terminate access or block such information [rule 3(1)(c)].
- In case an individual comes across any content of a platform that depicts such person in full/ partial nudity, in a sexual act or through morphed images, such person may make a complaint to the concerned intermediary, which is then obliged to take all reasonable and practical measures to remove such content within 24 hours of such complaint [rule 3(2)(b)].

Even with regard to identification of the first originator of messages, there are a number of safeguards in place in rule 4(2) to ensure that the privacy of users is not violated. Some of these safeguards are:

- SSMIs in the private messaging space are only required to enable identification of the first originator upon receiving authorised directions. They do not enjoy the authority to identify such users or information on their own in the absence of appropriate orders.
- Such appropriate orders can only be passed by a competent court or a competent authority under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
- Such orders can be passed only in relation to certain specified grounds contained in the Rules, such as sovereignty, national security, public order, rape or child abuse, etc.
- Such orders shall not be passed when other alternative measures are available.

7. Do these Rules affect the right to free speech and expression?

Ans: No. Article 19 of the Constitution guarantees right to freedom of speech and expression and article 19(2) defines the reasonable restrictions. The new IT Rules, 2021 have been framed consistent with these rights. The Rules place no additional obligations on users and do not contain any sort of penalties applicable on users. Further, a robust grievance redressal mechanism has been put in place to ensure that users whose content or access is unreasonably removed may highlight such error to the intermediary for remedial action.

8. How will users be benefitted from these new Rules?

Ans: The IT Rules, 2021 are meant to benefit a general user, who is using any intermediary platform. These Rules specially provide for:

- increased safety of users and also ensure accountability of intermediaries to the users;
- establishment of a robust grievance redressal mechanism by Intermediaries (including appointing a Resident Grievance officer for SSMI). This will ensure that Intermediaries are responsive to the concerns and grievances of users;
- a physical contact address in India for communication (for SSMI), to make sure that users can meaningfully reach out to SSMIs to voice their concerns, as many SSMIs are international organizations;
- periodic reminders by intermediaries to users that content which may be illegal or harmful to other users, such as those falling under harassment, insults, fake news, misrepresentation, invasions of privacy, paedophilic, pornographic, defamatory and obscene should not be posted;
- expeditious removal of content violative of physical privacy (generally considered as revenge porn material);

- yearly reminders about privacy policy and other terms and conditions offered by the intermediary;
- prior notice before content/account deletion/suspension in certain cases;
- voluntary verification;
- public accountability and transparency of SSMI.

These features are likely to benefit all concerned. These measures are intended to empower users in the online space, and protect their rights and dignity. The Rules, by providing these reasonable mechanisms and remedies, strive to ensure that social media platforms remain a safe space for all users, free from cyber threats, harassment and unlawful content.

9. Whether platforms and Apps, which act as news aggregators, qualify as intermediaries or whether they will also be covered as Publishers under the IT Rules, 2021?

Ans: Some entities may be functioning both like an intermediary as well as a "news aggregator" or "publisher of news and current affairs content" as defined in rule 2(o) and rule 2(t). Further clarification with respect to rule 5, and Part III of the Rules relating to news and current affairs content may be sought from the Ministry of Information & Broadcasting (MIB).

Section II: Basic Terminology and Scope of the Rules

10. Which entities are covered under the scope of Part II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 administered by MeitY?

Ans: Any intermediary as defined under section 2(1)(w) of the Information Technology (IT) Act, 2000.

11. Which entities can qualify as 'intermediary' under the IT Rules, 2021?

Ans: The section 2(1)(w) of the Information Technology Act, 2000 (21 of 2000) defines an intermediary as:

"intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

With the evolution of technologies and hence proliferation of digital businesses and services, many other platforms of different kinds may qualify as intermediaries with respect to the third-party content made available, shared, hosted, stored or transmitted on their platforms including websites and mobile Apps.

12. Which intermediaries will qualify/ not qualify as a 'social media intermediary' under these Rules?

Ans: The IT Rules, 2021 define 'social media intermediary' as an intermediary which **primarily or solely enables online interaction between two**

or more users and allows them to create, upload, share, disseminate, modify or access information using its services.

To qualify as a social media intermediary, enabling of online interactions should be the **primary** or **sole purpose** of the intermediary. Therefore, typically, an entity which has some other primary purpose, but only incidentally enables online interactions, may not be considered as a social media intermediary.

Indicative features that may clarify the scope of the phrase "*enables online interaction*" *inter-alia* are as follows:

(a) Facilitates **socialization/social networking,** including the ability of a user to increase their reach and following, within the platform via specific features like "follow"/"subscribe" etc.;
(b) Offers opportunity to interact with unknown persons or users;
(c) Ability of enabling **virality of content** by facilitation of sharing. Virality, in this context, means the tendency of any content to be circulated rapidly and widely from one internet user to another.

Typically, any intermediary whose primary purpose is enabling commercial or business-oriented transactions, provide access to internet or search-engine services, e-mail service or online storage service, etc. will not qualify as a social media intermediary.

13. Which social media intermediaries will qualify as 'significant social media intermediaries'?

Ans: As per the notification made by the Central Government, a social media intermediary having **fifty lakh (five million) registered users in India** shall be considered as a significant social media intermediary. The Gazette Notification in this regard can be accessed at:

https://egazette.nic.in/WriteReadData/2021/225497.pdf

Registered users for the purpose of computing the threshold for a SSMI are those users who have registered/created an account with SSMI.

Section III: Due Diligence by an Intermediary

14. Rule 3(1)(d) requires an intermediary to remove or disable access to certain information about which the intermediary is notified/ requested by the Appropriate Government or its agency within 36 hours. What kind of details pertaining to the said notice/ request will be provided by the Appropriate Government authority?

Ans: This rule was already present in the IT (Intermediaries Guidelines) Rules, 2011, and therefore, there is a clear and existing practice in relation to the orders of law enforcement or Appropriate Government authorities to communicate this information to the intermediary. Typically, this communication should contain-

(a) the platform specific identified URL(s);
(b) the law that is being administered by the Appropriate Government/ authorised agency and the specific clause of the law which is being violated;
(c) justification and evidence; and
(d) any other information (e.g., time stamp in case of audio/ video, etc.) as may be relevant.

15. Rule (3)(1)(h) requires an intermediary to retain information collected from user for registration on its computer resource for 180 days after any cancellation or withdrawal of registration. Is the intermediary required to store only the data that was collected at the time of registration, or the intermediary is required to save all data pertaining to usage of computer resource after registration (like IP address, user log, etc.)?

Ans: The IT Rules, 2021 warrant the intermediary to store or retain data that have been collected from the user at the time of registration (mainly the location, time and date stamp of the user to understand when and where the account was created) if the user has withdrawn from the platform or in case of cancellation of account by the intermediary. Regarding the information that has been collected

after registration and before withdrawal, it will vary from platform to platform. How much information should a platform store otherwise would be addressed through the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and notifications under Section 67C of the IT Act 2000.[1]

16. Do the intermediaries need to publish the name of the Grievance Officer?

Ans: Yes, the intermediaries need to prominently publish the name of the Grievance Officer and his/her contact details as well as mechanism adopted for grievance redressal on their platforms [rule 3(2)(a)]. The Grievance Officer will be responsible for handling grievances and facilitating an effective grievance redressal system. It is expected that the platform would provide grievance registration process in easy-to-understand terms for the benefit of the users.

17. What are the timeframes for action by an intermediary?

Ans:

S.N.	Actions to be taken by the intermediaries	Timeframe	Reference in the Rules
1.	Grievance Acknowledgement	24 Hours	Rule 3(2)(a)
2.	Response to Grievance	15 days	Rule 3(2)(a)

[1]Section 67C of Information Technology (IT) Act 2000 refers to preservation and retention of information by intermediaries. It states the following: (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe, (2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

S.N.	Actions to be taken by the intermediaries	Timeframe	Reference in the Rules
3.	Removal/ disabling of content which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual	Within 24 hrs	Rule 3(2)(b)
4.	Content removal on receipt of court order or notice from Appropriate Government or its agency	36 hours	Rule 3(1)(d)
5.	Provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities	Within 72 hours of the receipt of an order	Rule 3(1)(j)
6.	Preservation of information and associated records relating to removal/ disabling of access to such information	180 days or as may be required	Rule 3(1)(g)
7.	Retaining user's registration information after cancellation or withdrawal of his registration	180 days	Rule 3(1)(h)

Section IV: Additional Due Diligence by Significant Social Media Intermediaries (SSMI)

18. Rule 4(1) mandates significant social media intermediaries to appoint a Chief Compliance Officer responsible for ensuring compliance with the IT Act 2000, a nodal contact person for 24x7 coordination with law enforcement agencies and a Resident Grievance Officer. Can one person be appointed to fulfil the roles of the nodal contact person as well as the Resident Grievance Officer? If not, can one person be appointed to fulfil the diverse roles of the Chief Compliance Officer as well as the Resident Grievance Officer?

Ans: As mentioned in the rule 4(1) of the IT Rules, 2021, the Chief Compliance Officer and the nodal contact person cannot be the same person, whereas the roles of the nodal contact person and the Resident Grievance Officer may be performed by the same person. However, keeping in view the functional requirements of the nodal contact person and the Resident Grievance Officer, it is desirable that SSMI appoints separate persons for the two roles. The Government, through this rule, expects the intermediary to provide separate contact details for grievances submitted by users and the requests/orders made by the Government or authorized Government agencies, since the nature of requests might vary in view of different compliance timelines.

19. In case a parent company owns multiple products/ services that cross the threshold for significant social media intermediaries, can the parent company appoint common officers across all such products/ services or do they have to be appointed individually for each product/ service?

Ans: A parent SSMI can appoint common officers across its products/ services. However, the contact details to approach these officers are required to be clearly mentioned on each of those product/ service platforms separately.

20. Rule 4(1)(d) requires a significant social media intermediary to publish periodic compliance reports every month mentioning the details of complaints received and action taken thereon. Does the intermediary have to submit a physical copy of this report to MeitY? Is the intermediary required to publish the report on its website? Is there a particular format for publishing this report including details on the type of information that is essential or the level of granularity of the information published?

Ans: The intermediary does not have to submit a physical copy of the compliance report to MeitY. Rather, the intermediary is required to publish the monthly compliance report on its platform. The report should contain details of the preceding month.

No specific format of monthly compliance report has been prescribed in the Rules. However, the essential requirements that are already mentioned in the Rules should be included in the monthly compliance report. It is left to the discretion of the SSMI to decide other details of the report.

Insofar as actions taken by an SSMI on the user complaints received by it are concerned, ideally, the report should contain summary details of the complaints received, e.g., the subject under which the complaint is received (e.g., copyright) and action taken under these different heads. This information could be disclosed in the aggregated form, without disclosing granular details of all cases.

With regard to the voluntary actions taken by an SSMI, mentioning the number of communication links removed by the SSMI would serve the purpose of this rule.

The intermediary, while publishing such a report, also needs to ensure that it does not impinge upon the privacy and safety of its users while publishing such details.

21. Rule 4(6) requires the intermediary, to the extent reasonable, to provide the complainant with reasons for any action taken or not taken. Is there a criterion on what would qualify as 'reasonable'? In case of frivolous complaints, would it not be reasonable to desist from providing reasons for inaction?

Ans: The objective of this rule is to allow aggrieved users (including those whose content have been taken down or whose accounts have been disabled) to understand how their complaint is being dealt with by the Resident Grievance Officer of the intermediary, and promote a two-way communication between the aggrieved users and the intermediary.

It is expected that the intermediary provides a reasonable explanation to the aggrieved user. In case of a frivolous complaint, the nature of the complaint can be cited as the reason for any action not taken. The rules provide flexibility to the intermediaries to decide the best way to give an explanation and due process to the user, keeping in mind the safety of the reporting party. The idea is to promote accountability while giving flexibility. It is expected that the intermediary provides details of its grievance redressal mechanism for the benefit of the aggrieved users.

22. Rule 4(8) requires the significant social media intermediary to notify the user whose information is taken down or made inaccessible by the intermediary on its own accord and also allow adequate opportunity to dispute the action. Should the user be notified in all such scenarios?

Ans: The user may be notified only in a scenario where the content is removed or disabled by an SSMI "on its own accord" for violation of terms and conditions of the service. The term "*on its own accord*" implies, where SSMI:

(i) uses automated tools/filters or some national or international agency/ specialised organisation has identified child sexual abuse materials (CSAM) and related materials;

(ii) concludes that the content falls under the prohibited category as defined under any law for the time being in force;

(iii) is of the opinion that the content is blatantly illegal and notifying might harm the complainant in any way; or

(iv) removes the content as advised by its Resident Grievance Officer in accordance with its grievance redressal mechanism.

SSMI need to notify the user in such cases falling under the categories (ii) and (iv) as mentioned above.

23. The requirement to issue notification to users in case their content is removed may compromise the ability of an intermediary to counter activity by bots. If bots are notified about action taken, they may tweak their attack strategy. In such a case, does rule 4(8) allow for an intermediary to not send a notification to suspected bots and/or to implement a lag in notification to help the intermediary handle bot activity?

Ans: There might be situations, e.g., in case of a bot activity or malware, terrorism related content, spam, etc., where the intermediary may not find it prudent to inform the user prior to taking down their content. In such a scenario, it is expected that the intermediaries may undertake steps while handling a non-human user, to effectively counter bot activity.

24. Would detection of first originator of the message in the messaging platforms compromise end-to-end encryption?

Ans: The intent of this rule is not to break or weaken the encryption in any way but merely to obtain the registration details of the first Indian originator of the message. The electronic replica of the message (text, photo or video, etc.) will be shared by the requesting agency along with a lawful order. A typical principle of detection is based on the hash value of the unencrypted message, wherein identical messages will result into a common hash (message digest) irrespective of the encryption used by a messaging platform. How this hash will be generated or stored needs to be decided by the concerned SSMI, and SSMI are free to come up with alternative technological solutions to implement this rule. The rationale of this requirement is that if the intermediary has to convey to its users not to upload or share a particular type of content as part of its terms of use, it should have the capability of determining so or else the platform loses its own capability to enforce its own terms of usage. While encryption ensures safety and security of the data, and the privacy norms self-imposed by the intermediary may be needed, it is also imperative that the platforms should not be used to carry out sharing of any unlawful content as specified under the IT Rules, 2021 and other applicable laws.

25. What additional information can MeitY call for from significant social media intermediaries (SSMI) under sub-rule (9) of rule 4 of the IT Rules, 2021?

Ans: Under sub-rule (9) of rule 4, MeitY can only call for information that is in the power and possession of SSMI pertaining to their grievance redressal mechanism, which may include compliance reports in relation to the complaints received and action taken thereon and such additional information that MeitY is empowered to seek under the IT Act for effective implementation of Part II of the IT Rules, 2021. This would typically exclude any commercially sensitive, trade secret or otherwise confidential information held by the intermediaries.

26. Where an SSMI publishes ads, owned/ licensed content and identifies such content as advertised, promoted etc., or pays third parties to upload certain types of content, will it still qualify as an intermediary and be eligible to claim immunity under Section 79?

Ans: Rule 4(3) is intended to provide transparency to users so that they are aware whether the content being accessed by them is based on commercial considerations or otherwise. Hence, the rule requires appropriate labelling of such content so that the users can make an informed choice at the time of accessing it. It does not change the basic character of the intermediary and their ability to avail of the exemptions (safe harbour provisions), which shall be determined based on the provisions under Section 79 of the IT Act as judicially interpreted from time to time.

Section V: Non-Compliance to Intermediary Rules

27. What would be the impact of non-compliance by an intermediary to these Rules?

Ans: The intermediary shall lose its exemptions from liability as provided under section 79 of the IT Act and rule 7 of these Rules may become applicable with respect to the extant law violated.

28. Are there any penalties that users may face under these Rules?

Ans: No. However, users do need to ensure that the content they share on intermediary platforms is not violative of the IT Act (e.g., under sections 67, 67A, 67B, etc.) or other existing laws such as the Indian Penal Code, the Copyright Act, etc. as they may be liable to be prosecuted/ penalized under all such laws.

****

ACRONYMS

AoBR	Allocation of Business Rules
CSAM	Child Sexual Abuse Material
LEA	Law Enforcement Agency
MeitY	Ministry of Electronics and Information Technology
MIB	Ministry of Information & Broadcasting
SMW	Suo Motu Writ Petition
SSMI	Significant Social Media Intermediary
URL	Uniform Resource Locators

Printed by:

Ministry of Electronics and Information Technology
Government of India

Electronics Niketan, 6, CGO Complex, New Delhi 110003