MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Electronices and Information Technology)

NOTIFICATION

New Delhi, the 21st July, 2016

G.S.R. 711(E).— In exercise of the powers conferred by sub section (1) of section 87 and clause (wa) of sub-section (2) of section 87 read with section 6A and section 67C of the Information Technology Act, 2000 (21 of 2000) the Central Government hereby makes the following rules for the preservation and retention of information by intermediaries providing Digital Locker Facilities, namely:—

1. Short Title and Commencement.— (1) These rules may be called the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

(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) "access gateway" means authorised system to provide access to repositories under Digital Locker system;

c) "application program interface (API)", means a set of routines, protocols, and tools for building software applications;

d) "body corporate" means body corporate as defined in *Explanation (1)* to section 43A of the Act;

e) "DeitY" means the Department of Electronics and Information Technology in the Ministry of Communications and Information Technology, Government of India;

f) "DigiLocker" means the Government owned and operated web and mobile based hosting of Digital Locker system;

g) "Digital Locker" means a service of preservation, retention of electronic records by the subscriber and delivery of electronic records to the subscriber;

h) "Digital Locker authority" means an authority as designated by the Government for the licensing, empanelment and management of Digital Locker service providers;

i) "Digital Locker Directory" means a web page managed by the Government or Digital Locker authority for registration and providing details of registered locker providers, issuers, requester, repositories and access gateways providers;

j) "Digital Locker Portal" means a web and mobile based system to provide access to documents under Digital Locker System to the users;

k) "Digital Locker Practice Statement" means a statement by the Digital Locker service provider describing the services and flow of the services being offered by the provider;

l) "Digital Locker service provider" means an intermediary including a body corporate or an agency of the appropriate Government, as may be notified by the Government, to provide Digital Locker, access gateways and, or, repository facilities electronically, in accordance with these rules;

m) "Digital Locker system", means an application based system to provide Digital Locker services to the users with the help of authorised service providers, providing Digital Locker, access gateways and, or, repositories facilities;

n) "equivalently authenticated electronic record" means an electronic record authenticated by any other means other than digital signatures as prescribed under the Digital Locker standard guidelines;

o) "Government" means the Central Government;

p) "issuer" means any State or Central department or agency or body corporate issuing digitally signed or equivalently authenticated electronic records to the subscriber under Digital Locker system;

q) "License" means binding agreement between the Digital Locker authority and any Digital Locker service provider;

r) "repository" means an electronic repository of digitally signed and, or, digitised electronic records, maintained by any Digital Locker service provider or an issuer for the purpose of accessing such records and delivering them to the users;

s) "requester" means any State or Central department or agency or body corporate requesting access to subscriber's digitally signed or equivalently authenticated electronic records preserved and retained in the repository created and managed under Digital Locker system;

t) "subscriber" means subscriber to a Digital Locker under the Digital Locker system;

u) "Uniform Resource Identifier (URI)", means unique reference to a document stored in a Digital Locker repository;

v) "user" means a subscriber, issuer or requester of the Digital Locker system.

(2) Words and expressions used and not defined in these rules but defined in the Act and various rules made thereunder shall have the same meanings assigned to them in the Act and the said rules respectively.

3. Appointment of Digital Locker Authority.— (1) The Government shall appoint the Digital Locker authority to establish, administer, and manage Digital Locker system to preserve and retain information for efficient delivery of services to the users through Digital Locker system.

(2) The Digital Locker authority shall discharge its functions as notified under these rules subject to the general control and directions of the DeitY.

(3) The Digital Locker authority shall authorise the Digital Locker service provider to provide Digital Locker, access gateway and, or, repository facility electronically, in accordance with these rules.

4. Digital Locker System.— (1) For the purpose of providing preservation and retention of machine readable, printable, shareable, verifiable and secure State or Central department or agency or body corporate issued electronic records, the Government and other service providers to provide a Digital Locker system of limited electronic storage to all users.

(2) The Government through Digital Locker authority and in accordance with the technical standards as laid down by the DeitY from time to time shall provide for the administration of Digital Locker system.

(3) Subject to sub-rule (1), the Digital Locker system shall act as web and mobile based portal for State or Central department or agency or body corporate issued electronic records maintained in a prescribed format.

5. Operation of Digital Locker System.— (1) Any individual who is resident of India shall be able to open and gain access to Digital Locker portal after submitting duly prescribed application form to the authorised Digital Locker service provider.

(2) Subject to the sub-rule (1), any individual may obtain the services of the licensed or empanelled Digital Locker service providers for the purpose of accessing locker, gateways and repository services using web or mobile based Digital Locker Portal.

(3) Digital Locker Portal shall provide access to repositories and access gateway for issuers to issue and requesters to access digitally signed or equivalently authenticated electronic records respectively in a uniform way in real-time.

(4) Digital Locker Directory shall provide following details, namely:—

(a) Registration facility for issuers, requesters, locker providers, repository providers and gateway providers;

(b) issuer (name, ID, registration date, contact details), Requester ID ((name, ID, registration date, contact details), Gateway ID (name, ID, registration date, contact details) and repositories (name, ID, registration date, contact details);

(c) standards, application forms, and other particulars;

(d) electronic workflow to request, approve, and publish new ID for new issuers, gateways and repositories, as the case may be; and

(e) any other information as prescribed by the Government.

6. Location of the Facilities.— The infrastructure associated with all functions of Digital Locker system as well as maintenance of directories containing information about the status of Digital Locker system shall be installed at any location within India

7. The manner in which Digital Locker system be used by Subscriber.— A Digital Locker shall be used by the subscriber to,—

(a) access and register for Digital Locker on the web or mobile based Digital Locker Portal;

(b) upload documents, or as the case may be, digitally sign, the uploaded documents in the Digital Locker as provided by the Digital Locker service provider;

(c) access documents from issuers using the document URI's available in the Digital Locker account.

(d) grant access to the requester to access State or Central department or agency or body corporate issued records by providing unique document URI; and

(e) provide consent to the issuer to deposit document URI's and to the requestor to access documents;

8. The manner in which Digital Locker system be used by requester.— A Digital Locker shall be used by the requester to,—

(a) register on the Digital Locker directory;

(b) access documents uploaded by the subscriber on the Digital Locker portal;

(c) use authorised gateway providers to access documents stored across repositories;

(d) access subscriber's State or Central department or agency or body corporate issued documents based on the URI; and

(e) take consent from subscriber to access documents available in subscriber's Digital Locker account.

9. The manner in which Digital Locker system be used by issuer.— A Digital Locker shall be used to, —

(a) register on the Digital Locker Directory;

(b) issue new digital records in the format as prescribed by the appropriate government;

(c) provide older digitized records to the subscriber, which are verifiable, shareable, accessible and printable;

(d) gives consent to any other Digital Locker service provider to gain access to its documents;

(e) choose own repository or a repository from authorised repository service provider as issuer repository to preserve and retain issued records;

(f) use the integration interfaces, to either—

(i) push URI to Digital Locker: to push the URI's of all the records available in their repositories so that the same can be displayed to the subscriber, so as to notify the subscriber that the issuer has following documents linked to the subscriber's account;

(ii) pull URI: to allow the subscriber to query the issuer repository by providing subscriber's identifier applicable to issuer organisation to enable issuer to provide the URI's of all the records that are linked to the identifiers submitted by the subscriber.

10. Role of Digital Locker service providers.— (1) The Digital Locker system shall be supported by following Digital Locker service providers, namely:—

(a) Digital Locker portals;

(b) Repositories; and

(c) access gateways.

(2) Government or the Digital Locker authority shall authorise service providers to set up Digital Locker portals, access gateways or repositories for efficient use of Digital Locker system for the benefit of subscribers, issuers and requesters.

(3) Every authorised service provider to conform and comply with the binding authorising terms, including the standards, guidelines and specifications as laid down by the Government or Digital Locker authority.

11. Digital Locker service provider to ensure compliance of the Act, etc.— Every Digital Locker service provider shall ensure that every person employed or otherwise engaged or associated with it complies, in the course of such employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

12. Appointment of grievance officer by the Digital Locker service provider for dispute resolution.— (1) Every Digital Locker service provider shall publish on its website the name of grievance officer and his contact details as well as mechanism by which any users or aggrieved person who suffers as a result of—

(i) access or usage of Digital Locker or Digital Locker system by any unauthorised person; or

(ii) violation of authorising terms,

may notify their complaints against such access or usage or violation of licensing terms to such grievance officer.

(2) The grievance officer shall redress the complaints within one month from the date of receipt of complaint.

13. Suspension and revocation of Digital Locker account.—(1) Subject to the provisions of sub-rule (2), the Digital Locker service provider which has provided a Digital Locker account may suspend such Digital Locker account –

(a) on receipt of a request to that effect from –

(i) the subscriber listed in the Digital Locker account; or

(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is the opinion of Digital Locker authority that the subscriber's Digital Locker account should be suspended in public interest for reasons to be included in writing.

(2) A Digital Locker account shall not be suspended for a period exceeding thirty days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Locker account under these rules, the Digital Locker service provider shall communicate the same to the subscriber and other users.

Explanation.— For the purpose of these rules, suspension of Digital Locker account of subscriber implies that neither requester nor issuer shall be able to access subscriber's account during the period of such suspension.

(4) Subject to sub-rule (2), the Digital Locker authority, if not satisfied after making such inquiry, may revoke subscriber's Digital Locker account.

14. Control of Digital Locker account credentials.—(1) Every subscriber shall exercise reasonable care to retain control of the Digital Locker account credentials and take all steps to prevent its disclosure.

(2) If the Digital Locker account credentials have been compromised, then, the subscriber shall communicate the same without any delay to the Digital Locker service provider in such manner as may be specified by the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Digital Locker service provider that the Digital Locker account credentials have been compromised.

15. Fees for opening Digital Locker account.— (1) The Digital Locker service provider shall charge such fee or service charges from subscribers or users, as may be notified by the Government or Digital Locker authority.

(2) Subject to sub-rule (1), Digital Locker service provider shall provide an up-to-date fee schedule or scale of service charges to all its subscribers and users.

16. Portability of Digital Locker account of subscriber.—The Digital Locker service provider shall provide Digital Locker services to subscribers with the facility to port their Digital Locker account to any other Digital Locker service provider, and shall, *inter-alia*,—

(a) observe data retention and data migration guidelines as notified by DeitY;

(b) make reasonable efforts to ensure that the portability service is provided to the subscriber with minimal service disruption; and

(c) refund reasonable fee back to subscriber (not exceeding any fee or service charges by the service provider to the subscriber).

17. Audit.—(1) The Digital Locker service provider shall get its operations audited annually by an auditor and such audit shall include, *inter alia*,—

(a) security policy and planning;

(b) physical security;

(c) technology evaluation;

(d) Digital Locker service provider's services administration;

(e) relevant Digital Locker Practice Statement;

(f) compliance to relevant Digital Locker Practice Statement;

(g) contracts or agreements; and

(h) policy requirements as may be required under these rules.

(2) The Digital Locker service provider shall conduct,-

(a) half yearly audit of the security policy, physical security and planning of its operation;

(b) a quarterly audit of its system and all associated interfaces, systems, tools and processes.

(3) The Digital Locker service provider shall submit copy of each audit report to the Government or Digital Locker authority within four weeks of the completion of such audit and where irregularities are found, the Digital Locker service provider shall take immediate appropriate action to remove such irregularities.

18. Auditor's relationship with Digital Locker service provider.— (1) The auditor shall be independent of the Digital Locker service provider being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Digital Locker service provider.

(2) The auditor and the Digital Locker service provider shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

19. Confidential Information.—The following information shall be treated as confidential, namely:—

(a) Digital Locker account application;

(b) Digital Locker account information collected from the subscriber or elsewhere as part of the registration;

(c) subscriber agreement;

(d) Digital Locker contents;

(e) document URI; and

(f) any other information as may be notified by the DeitY.

20. Access to confidential information.— (1) Access to confidential information shall be subject to the provisions of the Act and the rules made thereunder.

(2) Access to confidential information by the employees of the Digital Locker service provider shall be on a "need-to-know" and "need-to-use" basis. The process of maintaining confidentiality of information has to be included in the Digital Locker Practise Statement.

(3) The back up of all information shall be kept offsite in the disaster recovery facility.

(4) The confidential information shall not be preserved and retained outside India.

21. Maintenance of reasonable security practices.— (1) The Digital Locker service provider to observe and maintain reasonable security practices as mandated under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011.

(2) The Digital Locker service provider shall observe and maintain Information Technology Security Guidelines as mandated under Schedule II of the Information Technology (Certifying Authorities) Rules,2000.

[F.No. 3(29)/2016-EG-II]
SANJIV MITTAL, Jt. Secy.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.