ANNEXURE

The Digital Trade Facilitation Bill, 2026

A Bill to provide legal recognition, validity and enforceability to electronic trade documents and to regulate the use, management and cross-border recognition of digital identity and trust services and for matters connected therewith or incidental thereto.

CHAPTER I	**PRELIMINARY**
Short title and commencement	1. (1) This Bill may be called The Digital Trade Facilitation Bill, 2026. (2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.
Definitions	2. In this Bill, unless the context otherwise requires, — (a) "competent authority" means the authority as designated by the Central Government under this Bill; (b) "control" means the exclusive authority to exercise rights over an electronic trade document, including the ability to amend, endorse, extinguish, or otherwise deal with such rights, in accordance with this Bill, using electronic means, including identity credentials, electronic authentication, or any secure digital representation recognised by this Bill or by rules made thereunder. (c) "electronic archiving service" means a service that ensures long-term preservation and integrity of electronic data and documents by reliable, auditable, and tamper-evident means. (d) "electronic identification" means the process of establishing or verifying the identity of a natural person, a legal person, or a natural person authorised to act on behalf of a legal person,

	using electronic means. (e) "electronic registered delivery service" means a service that provides evidence of sending and receiving electronic data, and protects the data transmitted against loss, theft, or unauthorised alteration. (f) "electronic seal" means data in electronic form which is attached to or logically associated with other electronic data to ensure its origin and integrity, and which is created by a reliable method under this Bill. (g) "electronic time stamp" means data in electronic form which binds the date and time to other electronic data, ensuring that such data existed at that time, and is created by a reliable and auditable method. (h) "electronic trade document" means any trade document or instrument in electronic form, as may be notified by the Central Government in the First Schedule, that entitles the holder to claim the performance of the obligation indicated therein and complies with all the requirements specified in section 6 of this Bill. (i) "identity credentials" means the data, or the physical object upon which the data may reside, that a person may present for electronic identification. (j) "identity management service provider" means a person who has been granted an authority to provide identity management services. (k) "identity management system" means a set of processes and technologies used to identify, authenticate, and verify the identity of a person, system, or device, using reliable methods

	as may be prescribed. (l) "paper trade document" means any trade document or instrument, in physical paper form, specified in the First Schedule, which entitles the holder thereof to claim the performance of the obligation indicated therein. (m)"relying party" means a person who acts on the basis of the result of identity management services or trust services; (n) "subscriber" means a person who enters into an arrangement for the provision of identity management services or trust services with an identity management service provider or a trust service provider; (o) "trust services" means an electronic service that provides assurance of certain qualities of a data message or an electronic trade document and includes the services for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving, electronic registered delivery services, or any such other services as may be notified by the Central Government. (p) "trust service provider" means any natural or legal person, who provides one or more trust services as defined in clause (o) of this section. (q) all other words and expressions used herein but not defined and defined in the Information Technology Act, 2000 (Act No. 21 of 2000), shall have the meanings respectively assigned to them in that Act.
Interpretation of this Bill	3. (1) If any question arises concerning any matter not expressly dealt with in this Bill, such matter shall be settled in accordance with the general principles of commercial practice commonly accepted in India, regard being had to the international origin of

	this Bill and the need to promote uniformity in its application. (2) This Bill shall be read in conjunction with, and shall not derogate from, the provisions of the Consumer Protection Act, 2019 and the Information Technology Act, 2000.
Application	4. (1) This Bill shall apply to such electronic trade documents as are specified in the First Schedule. (2) Nothing in this Bill shall affect- (a) the application of any law for the time being in force relating to data privacy or data protection; or, (b) any paper trade document or any electronic trade document issued before the date on which this Bill comes into force; or, (c) the provisions of the Information Technology Act, 2000 (21 of 2000), or any rules or regulations made thereunder, in relation to trust services already existing or regulated under that Act. (3) The Central Government may, by notification in the Official Gazette, add to, omit from, or otherwise amend the First Schedule or the Second Schedule.
CHAPTER II	**ELECTRONIC TRADE DOCUMENTS**
Legal recognition of Electronic Trade Documents	5. An electronic trade document shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form, provided it complies with the provisions contained in this Chapter.
Requirements for Electronic Trade Documents	6. (1) Where the law requires a paper trade document specified in the First Schedule, that requirement shall be deemed to be met by an electronic trade document if: (a) the electronic trade document contains at least the

	information required to be contained in a corresponding paper trade document. (b) a reliable method is used, - (i) To identify the electronic trade document. (ii) To render that electronic trade document capable of being subject to control from its creation until it ceases to have any effect or validity. (iii) To retain the integrity of that electronic trade document; and, (iv) to provide a verifiable audit trail from the creation to the extinction of the document. (c) the method used to establish control, integrity and authenticity is deemed to be reliable as specified under this Chapter or as notified by the Central Government. (2) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Chapter, including but not limited to - (a) prescribing standards and methods for ensuring the authenticity, integrity, and control of electronic trade documents. (b) specifying, determining, or prescribing what constitutes a reliable method for the purposes of this Chapter. Provided that the implementation of such standards or rules, shall, as far as practicable, be technology neutral and promote interoperability. (3) The place of business of a party shall not be deemed to be at any location by reason only of— (a) the location of any equipment or technology supporting

	an information system used by such party in connection with an electronic trade document; or, (b) the fact that an information system used in connection with an electronic trade document may be accessed by other parties at such location; or, (c) the sole fact that such party makes use of an electronic address or any other element of an information system connected to a specific country.
Additional Information in Electronic Trade Documents	7. Nothing in this Chapter precludes the inclusion of information in an electronic trade document in addition to that contained in a corresponding paper trade document.
Control, Transfer, Endorsement and Amendment of Electronic Trade Documents	8. (1) Where the law requires or permits possession of a paper trade document, such requirement shall be deemed to be satisfied, in relation to an electronic trade document, if a reliable method is used- (a) to establish control of the electronic trade document by a person; and, (b) to identify that person as the person in control. **Explanation:** For the purposes of this Bill or any other law for the time being in force, the establishment of control over an electronic trade document by a reliable method shall be deemed to confer possession of the document and shall carry the same legal consequences as possession of a paper trade document. (2) The person who is identified, in accordance with a reliable method, as having control over an electronic trade document shall be deemed to be the holder thereof and entitled to

	exercise all rights and obligations attached thereto. (3) The transfer of control, endorsement, or amendment of an electronic trade document, effected by a reliable method, shall have the same legal effect as the transfer of control, endorsement, or amendment of a paper trade document.
Change of Form	9. (1) A paper trade document may be converted into an electronic trade document, and an electronic trade document may be converted into a paper trade document, as the case may be, if: (a) a reliable method for the change of form in accordance with this chapter is used, and, (b) a statement that the document has been converted is included in the document in its new form. (2) Where a document is converted in accordance with subsection (1), in such case, - (a) the document in its old form ceases to have effect, and, (b) all rights, obligations and liabilities relating to the document continue to have effect in relation to the document in its new form.
CHAPTER III	**IDENTITY MANAGEMENT AND TRUST SERVICES**
Legal Recognition of Identity Management Services and Trust Services	10. The result of electronic identification, the use of an identity management service or credential, or the use of a trust service shall not be denied legal effect, validity, enforceability, or admissibility as evidence solely on the ground that such identification, service, credential, or trust service is in electronic form.
Reliability Standards for Identity Management Services and	11. (1) Where the law requires- (a) the identification of a person for any purpose, such requirement shall be deemed to be satisfied if a reliable method is used for the identity proofing and electronic

Trust Services	identification of the person for that purpose; or (b) the use of a trust service for any purpose, such requirement shall be deemed to be satisfied if a reliable method is used for the trust service for that purpose. Explanation- For the purpose of this sub-section, 'reliable method' means a method used to authenticate any person or trust service, including use of electronic and digital signatures. (2) For the purposes of sub-section (1), a method shall be considered reliable if it is proven in fact by or before a court or an authority notified by the Central Government in this behalf to have fulfilled the relevant function for which it is being used, either alone or together with other evidence. (3) In determining the reliability of a method under sub-section (2), all relevant circumstances shall be taken into account, including but not limited to- (a) compliance by the identity management service provider or trust service provider, as the case may be, with the obligations specified in this Chapter; (b) compliance of the operational rules, policies and practices of the identity management service provider or trust service provider, as the case may be, with any applicable recognised international standards and procedures relevant for the provision of identity management services or trust services, including level of assurance and reliability frameworks; (c) in the case of identity management services, the adequacy of governance, information security management,

	technical controls, and oversight or audit mechanisms; (d) in the case of trust services, the security of systems and resources, the existence of relevant accreditation or independent audit, the purpose for which the trust service is used, and any relevant agreement between the parties, including any limitation on the purpose or value of the transaction. (4) In determining the reliability of the method, no regard shall be had to (a) the geographic location where the identity management service or trust service is provided; or, (b)the geographic location of the place of business of the identity management service provider or trust service provider. (5) A method used by an identity management service or trust service notified as reliable by the Central Government or any authority notified by it in this behalf shall be presumed to be reliable. (6) The presumption under sub-section (5) shall not limit- (a) the ability of any person to establish in any other manner the reliability of a method; or, (b) the right of any person to adduce evidence of the non-reliability of a method used by an identity management service or trust service notified as reliable.
Obligations and Liabilities of Service Providers	12. (1) Every identity management service provider or trust service provider, as the case may be, shall (a)establish and maintain operational rules, policies, and

	practices appropriate to the purpose and design of the service, including, where applicable,- (i) in case of identity management services, enrolment and identity proofing, attribute updates, issuing, activating, suspending, revoking, and renewing credentials, and managing identification factors and mechanisms; and, (ii) in case of trust services, a plan to ensure continuity in case of termination of activity. (b) act in accordance with its operational rules, policies, practices, and any representations made with respect to them; (c) ensure online availability and proper operation of the service, as applicable; (d) make its operational rules, policies, and practices easily accessible to subscribers, relying parties, and other relevant persons; (e) provide means for subscribers to report security breaches; (f) provide means for relying parties to ascertain any limitations on use or liability, including- (i) any limitation on the purpose or value for which the service may be used; and (ii) any limitation on the scope or extent of liability stipulated by the provider; (g) in the event of a breach of security or loss of integrity having a significant impact on the service, take all reasonable steps, including (i) containing the breach or loss, including, where appropriate, suspending the affected service or revoking the affected credentials or means of

	access; (ii) remedying the breach or loss; (iii) notifying the breach or loss to affected subscribers, relying parties, and any competent authority as may be prescribed; and, (iv) upon receiving a notification of a potential breach or loss fromany person, promptly investigate and take appropriate action asspecified in clauses (i) to (iii). (2) The identity management service provider or trust service provider, as the case may be, shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations under this section. (3) Notwithstanding anything contained in subsection (2), the provider shall not be liable to a subscriber for loss arising from the use of the service to the extent that- (a) such use exceeds the limitations on the purpose or value of the transaction for which the service is used; and (b) such limitations are contained in the arrangement between the provider and the subscriber. (4) Notwithstanding anything contained in subsection (2), the provider shall not be liable to a relying party for loss arising from the use of the service to the extent that- (a) such use exceeds the limitations on the purpose or value of the transaction for which the service is used; and, (b) the provider has complied with its obligations under clause (f) of subsection (1) with respect to that transaction. (5) Every identity management service provider or trust service

	provider, as the case may be, shall comply with the financial, managerial, operational, technical, and information security measures as may be prescribed by the Central Government.
Obligations of subscribers	13. Every subscriber to an identity management service or trust service shall notify the respective service provider, using the means provided by the service provider or otherwise using reasonable means, if- (a) the subscriber knows that the subscriber's identity credentials or the data or means used for access to or use of the trust service have been compromised; or, (b) circumstances known to the subscriber give rise to a substantial risk that the subscriber's identity credentials or the data or means used for access to or use of the trust service may have been compromised.
Notification of identity management service and trust services	14. (1)The Central Government or any authority notified by the Central Government in this behalf may, subject to the provisions of this Bill, notify any identity management service or trust service, taking into account relevant circumstances, including those specified in this Chapter. (2) The Central Government or the authority referred to in sub-section (1) shall maintain and publish a public list of identity management services, trust services, and their respective providers notified as reliable under sub-section (1).
Electronic Trust Services	15. (1) Where a law requires a signature of a person, or provides consequences for the absence of a signature, that requirement shall be deemed to have been met in relation to a data message if a reliable method in accordance with Section 11 is used, - (a) to identify the person; and (b) to indicate the person's intention in respect of the information contained in the data message.

	(2) Where a law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement shall be deemed to have been met in relation to a data message if a reliable method in accordance with Section 11 is used, - (a) to provide reliable assurance of the origin of the data message; and, (b) to detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display. (3) Where a law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement shall be deemed to have been met in relation to a data message if a reliable method in accordance with Section 11 is used, (a) to indicate the time and date, including by reference to the time zone; and (b) to associate that time and date with the data message. (4) Where a law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement shall be deemed to have been met in relation to a data message if a reliable method in accordance with Section 11 is used,- (a) to make the information contained in the data message accessible soas to be usable for subsequent reference.

	(b) to indicate the time and date of archiving and associate that time and date with the data message. (c) to retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and (d) to retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received. (5) Where a law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement shall be deemed to have been met in relation to a data message if a reliable method in accordance with Section 11 is used, - (a) to indicate the time and date when the data message was received for delivery and the time and date when it was delivered. (b) to detect any alteration to the data message after the time and date when the data message was received for delivery to the time and date when it was delivered, apart from the addition of any endorsement or information required by this section, and any change that arises in the normal course of communication, storage and display; and, (c) to identify the sender and the recipient.

	(6) Where a law requires website authentication, or provides consequences for the absence of website authentication, that requirement shall be deemed to have been met if a reliable method in accordance with Section 11 is used,- (a) to identify the person who holds the domain name for the website; and, (b) to associate that person with the website.
CHAPTER IV	**MISCELLANEOUS**
Cross-border recognition	16. (1) An electronic trade document shall not be denied legal effect, validity or enforceability on the sole ground that it was issued or used outside India. (2) The result of electronic identification or the use of an identity management service, credential, or trust service provided outside India shall have the same legal effect in India, if the method used offers,- (a) at least an equivalent level of assurance or reliability, as the case may be, where the assurance or reliability levels recognised by India and the foreign jurisdiction are identical; or, (b) a substantially equivalent or higher level of assurance or reliability, in all other cases. (3) An identity management system, identity management service, identity credential or trust service shall be presumed to satisfy sub-section (2), if the Central Government or any authority notified by it in this behalf has determined that the method used offers an equivalent level of assurance or reliability, as the case may be, having regard to the relevant provisions of this Bill and as per prescribed guidelines.

	Provided that the Central Government may, by notification in the Official Gazette, recognise specific foreign digital trade documentation frameworks, identity management systems, or trust services as equivalent for the purposes of this Bill, including under any bilateral, plurilateral or multilateral arrangements, and such recognition shall be binding on all authorities recognised under any law for the time being in force.
Protection of action taken in good faith	17. No suit, prosecution or other legal proceedings shall lie against the Central Government or any authority appointed under this Bill in respect of anything which is done or intended to be done or any action taken in good faith under this Bill or any rules or regulations made thereunder.
Evidentiary value of electronic trade documents and trust services	18. (1) Subject to sub-section (2), an electronic trade document issued or transferred using a reliable method shall be presumed to be authentic and shall be admissible as evidence in any legal proceeding, including civil, commercial or regulatory proceedings, in accordance with the provisions of the Bhartiya Sakshya Adhiniyam, 2023. (2) The presumption under sub-section (1) may be rebutted by evidence showing that the electronic trade document or trust service is not authentic or has been materially altered, unless such alteration occurred in the normal course of communication, storage, or display and is verifiably logged. (3) Where any law requires a trade document or signature to be presented, produced or retained for evidentiary purposes, such requirement shall be deemed to be satisfied if the corresponding electronic trade document or trust service complies with the requirements specified under this Bill and any rules made thereunder. (4) For the purposes of sub-section (1), a reliable method shall be deemed to include digital signatures or electronic records

	authenticated in accordance with the provisions of the Information Technology Act, 2000 or certified by a trust service provider notified under this Bill.
Power to make rules	19. (1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Bill. (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely: - (a) standards for reliability, security and operation of electronic trade documents, identity management services and trust services; (b) procedures, standards, or criteria for the notification, supervision, certification, recognition, or accreditation of reliable identity management service providers and trust service providers as specified in the Second Schedule, including those recognised by the Controller of Certifying Authorities or any other competent authority under any law for the time being in force; (c) the form and manner in which documents specified in the First Schedule may be issued, transferred or dealt with in electronic form, including those recognised by the Controller of Certifying Authorities under the Information Technology Act, 2000 and the rules made thereunder, or by any other competent authority under any law for the time being in force; (d) the manner and procedure for resolution of disputes arising under this Bill, including the appointment or designation of an Authority, officer, or agency by the Central Government for such resolution, through mechanisms as

	may be prescribed. (e) any other matter which is required to be, or may be, prescribed under this Bill.
Amendments to certain Acts	20. (1) In the First Schedule of the Information Technology Act, 2000, Sl. No. 1 shall be omitted. (2) The Negotiable Instruments Act, 1881 shall be amended in the following manner, namely: — (a) In section 4, after the words "in writing", the words "or in electronic form" shall be inserted; (b) In section 5, after the words "in writing", the words "or in electronic form" shall be inserted; (c) In section 13, after Explanation (iii), the following Explanation shall be inserted, namely: — Explanation (iv)— For the purposes of this section, a promissory note, bill of exchange, or cheque includes such instrument in both physical and electronic form. (d) In section 14, after the words "transferred to any person", the words “in whatever form, whether physical or electronic" shall be inserted. (3) The Indian Stamp Act, 1899 shall be amended in the following manner, namely: — (a) In sub-section (14) of section 2, the following Explanation shall be inserted, namely: — Explanation— For the purposes of this section, the term "instrument" shall also include an electronic trade document as defined in clause (c) of section 2 of The Digital Trade Facilitation Bill, 2025.

SCHEDULE	
THE FIRST SCHEDULE	DOCUMENTS TO WHICH THE BILL SHALL APPLY
THE SECOND SCHEDULE	LIST OF RELIABLE IDENTITY MANAGEMENT SERVICE PROVIDERS AND TRUST SERVICES PROVIDERS

****