RNP Learning Session Finance, Compliance & Legal Essentials for CSOs (June 2025)

> Read the information below in 15+ languages by selecting your preferred language using the translation tool in the top left corner of the screen.

Part 1: Discover PATTIC - Your Partner for Trust & Transparency

https://www.youtube.com/embed/CNsyPGbFdDY?si=0240TxgwRGf3LMRf

PATTIC — the People's Alliance for Trust & Transparency in CSOs

PATTIC is a community-driven platform that helps CSOs stay informed and compliant. It offers an online library of curated training materials, a forum where we can ask questions and learn from each other, and a compliance calendar to help stay on top of deadlines. The platform is regularly updated with the latest regulations and is designed to be accessible in 15+ Indian languages. The session highlighted how PATTIC supports the sector in building trust and staying transparent — all while keeping the process simple and collaborative.

Part 2: Navigating NPO Compliance Challenges in 2025

https://www.youtube.com/embed/RpmD1MBXzmE?si=A6HIcy4vxNW2Qr6Z

Challenges Around Compliances

- **Regulatory Landscape:** The regulatory landscape is ever-changing and complex.
- **Reporting Burden:** There is a significant burden of compliance and a high level of detail required in reporting.
- **Digitization:** Increased digitization and technology have led to a lack of face-to-face interface.
- **Penalties:** Non-compliance carries stiff penalties, posing an existential risk.
- **Internal Capacity:** There is a need to address internal capacity on institutional matters.
- **Governance:** Governance structures need to be strengthened.

Preparation for Compliances in 2025

1. Renewal of 12A Registration and 80G Approval

- The current 5-year period ends on March 31, 2026.
- Form 10AB must be filed by September 30, 2025.
- Small NGOs will be eligible for a 10-year approval.

2. Settle Outstanding Income Tax and TDS Matters

- It is important to watch for any proceedings and address outstanding matters in a timely manner.
- Smooth renewal of 12A and 80G is more likely if all proceedings are closed.

3. FCRA

- Expect a more elaborate Form FC4, requiring detailed information on assets.
- Chartered Accountants (CAs) will have higher responsibility and reporting requirements.
- The application process for registration and prior permission has been rationalized.

4. Likely Rollout of Labor Codes

- The definition of "Wage" is expected to change.
- This will result in higher social security contributions and lower take-home pay.
- Contract workers will not be permitted in core activities.
- Gratuity liability will extend to fixed-term employees.
- It is advised to comply with social security laws in a phased manner.

5. Draft Income Tax Bill, 2025

- The bill aims to consolidate the current complex and dispersed provisions.
- Commercial activities will be strictly barred.

6. Updating NGO Darpan Profile

- The NGO Darpan is likely to become the de-facto KYC for NGOs in the future.
- All fields on the profile should be fully populated and kept up-to-date.

7. Prepare for a Complex Regulatory Landscape

- Stay abreast of continuous regulatory and statutory changes.
- Improve in-house capacity, as non-compliance can be damaging.

8. Risk Management

- The external and internal environments are challenging and complex, highlighting the importance of internal controls.
- Organizations should formulate a risk management policy.
- Implement a risk management process, including risk registers and risk mitigation strategies.

Part 3: Understanding the Digital Personal Data Protection (DPDP) Act, 2023

https://www.youtube.com/embed/gmEBcAVZUds?si=VWR-23dZvBoj1EOM

DPDP

What is DPDP?

- The Digital Personal Data Protection Act was passed in August 2023.

- India’s first umbrella data protection legislation
- Brings all digital personal data within its ambit
- The Draft Rules, released for comments in January, show the pathways to achieve the intent of the Act

Are there data protection compliances applicable to your CSO?

All organizations are subject to data protection laws if they collect digital personal data.

Concepts and Terminology under the DPDP Act

Data Principal and Fiduciary

- Data Principal: an individual whose personal data is collected and processed by an organization.
- Data fiduciary: an individual, company, or organization that decides how personal data is processed.
- Data processor: any person who processes data on behalf of data fiduciaries.

What is Personal Data in Relation to CSOs?

Examples of personal data you may collect:

- Name
- Age
- Govt ID
- Photographs
- Profession
- Religion

Sources/channels of collection:

- Survey
- Beneficiary records
- Meeting records
- Workshop attendance records
- Donation forms

Consent and Notice

Consent is the primary basis for the processing of Personal Data.

It must be:

- freely given
- taken for a specific purpose
- taken with full information as to why it is collected
- how it will be used
- who will have access
- taken unconditionally (not involve a threat)

Each request for consent must be accompanied by a notice. It should provide information about the process of:

- withdrawing consent
- addressing grievances
- filing a complaint with the Data Protection Board

DPDP and Legal Compliances for CSOs

Implications for CSOs

- NGOs should obtain explicit and informed consent from individuals (Data Principals) before collecting or processing their personal data.
- NGOs are required to provide detailed information to Data Principals about their data processing practices.
- NGOs should only collect such personal data as is necessary for their stated purposes. Data must be retained only for as long as required by law or operational necessity. Once the purpose has been fulfilled, NGOs are expected to delete the data, ensuring that unnecessary retention does not compromise individual privacy.
- In cases where NGOs process personal data without explicit consent, as permitted by certain exceptions under the DPDP Act (such as compliance with legal obligations), it must notify the Data Principals about the processing activity.
- NGOs should have organizational data protection policies.

- NGOs must appoint a Data Protection Officer (DPO) to ensure compliance with the DPDP Rules, and publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer.
- If NGOs share data with service providers/ M&E partners, the risk of non-compliance with law will arise. In such cases, it is important to have data sharing agreements in place.
- Implement reasonable security measures, including encryption, controlled access, and regular system monitoring. If NGOs rely on third-party service providers (Data Processors) for data handling, they must ensure these entities also comply with the same security standards, and ensure that they implement appropriate checks of these compliances.
- In case of breach, the data fiduciary is obliged to intimate:
  - The data principal from whom the data is collected, without delay, through her user account or any mode of communication registered by her with the Data Fiduciary.
  - The Data Protection Board, within seventy- two hours.
- Obtain verifiable parental consent of children and persons with disabilities before collection of their data.

Data Belonging to Children and Persons with Disabilities

What do the Acts and Rules say on children's data?

1. The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed. Explanation—For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable.
2. A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.
3. A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.
4. The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.
5. The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify

for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify.

Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian:

A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to-

- reliable details of identity and age available with the Data Fiduciary; or
- voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued by an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.

Who is exempt from obtaining verifiable parental consent?

1. Healthcare Professionals

1.	A Data Fiduciary who is a clinical establishment, mental health establishment or healthcare professional	Processing is restricted to provision of health services to the child by such establishment or professional, to the extent necessary for the protection of her health.
2.	A Data Fiduciary who is an allied healthcare professional	Processing is restricted to supporting implementation of any healthcare treatment and referral plan recommended by such professional for the child, to the extent necessary for the protection of her health.

2. Educational Institutions

“Educational institution” shall mean and include an institution of learning that imparts education, including vocational education.

3.	A Data Fiduciary who is an educational institution	Processing is restricted to tracking and behavioural monitoring— • for the educational activities of such institution; or • in the interests of safety of children enrolled with such institution.
4.	A Data Fiduciary who is an individual in whose care infants and children in a crèche or child day care centre are entrusted	Processing is restricted to tracking and behavioural monitoring in the interests of safety of children entrusted in the care of such institution, crèche or centre.
5.	A Data Fiduciary who is engaged by an educational institution, crèche or child care centre for transport of children enrolled with such institution, crèche or centre	Processing is restricted to tracking the location of such children, in the interests of their safety, during the course of their travel to and from such institution, crèche or centre.

Compliances for Special Categories of Data Fiduciaries

Implications for Educational Institutions

“educational institution” shall mean and include an institution of learning that imparts education, including vocational education.

As part of their regular compliance obligations, educational institutions must:

- Obtain explicit and verifiable parental consent for processing children's personal data.

- Not carry out behavioural monitoring and tracking of children through data collection except for educational or safety-related purposes.
- Draft a robust data privacy, data protection, data use and data retention policy along with well-established processes to implement these policies in letter and spirit.
- Establish robust data breach response mechanisms to contain and mitigate security incidents.
- Train staff members on data protection best practices and compliance requirements under the DPDP Rules.
- Appoint a Data Protection Officer (DPO) to oversee compliance and governance.

Implications for Healthcare Professionals

- Data Security: Strong security measures such as encryption, controlled access, and regular audits must be implemented to protect health data from breaches or unauthorized use.
- Consent Management: In cases where explicit consent is required, NGOs must ensure that it is informed, specific, and freely given. They must also provide mechanisms for individuals to withdraw consent.
- Transparency: NGOs must inform individuals (Data Principals) about the purpose of data collection, their rights under the DPDP Act, and how their data will be used and stored. Clear communication channels must be established for grievances or inquiries.
- Retention Policies: Health data must only be retained for as long as necessary to achieve the stated purpose. Once the purpose is fulfilled, NGOs must ensure secure deletion of the data.
- Accountability: NGOs must appoint a Data Protection Officer (DPO) to oversee compliance with the DPDP Rules, conduct audits, and ensure proper handling of health data.

Name Boards

Requirements	Sec. 8 Company	Trust	Society	Notes

Mandatory Name Elements	Specific suffixes such as “Foundation”, “Association”, “Forum” (not “Limited”)	Display registered name	Display registered name	Rule 8(7) of Companies Incorporation Rules applies for Sec. 8 Companies. Trusts and Societies should follow their registration documents
Display of Registered Name	Mandatory	Mandatory	Mandatory	
Registered Address	Mandatory	Often Required	Common Practice	Section 12(1) of the Companies Act, 2013 clearly states, “A company shall, within thirty days of its incorporation and at all times thereafter, have a registered office capable of receiving and acknowledging all communications and notices as may be addressed to it.” For Trusts and Societies, it varies based on specific Trust/Society Acts and registration procedures.

Karnataka Specific Rules	Kannada name board should be predominant	Kannada name board should be predominant	Kannada name board should be predominant	Rule 24 – A of the Karnataka Shops and Commercial Establishments Rules, 1963, and the Sec. 17(6) of the Kannada Language Comprehensive Development Act, 2022 mandate that 60% of the display text to be in Kannada for all physical establishments.

Websites

Principles and best practices for websites:

- Display of Identity and Contact: The registered name, address, and contact information should be prominently displayed
- Organizational Information: Clearly state the NPO's objectives, mission, and registration details. For Section 8 companies, the website should also have the Corporate Identification Number (CIN).
- Governance: Information about the governing body (Board of Directors/Trustees/Committee members) fosters accountability
- Financial Transparency: Consider publishing annual reports and audited financial statements to build trust
- Activities and Impact: Detail the work being done and its impact to inform stakeholders
- Data Privacy: If collecting personal data, a clear and compliant privacy policy is essential
- Secure Transactions: For online donations, ensure secure payment gateways
- Website Address Disclosure (Section 8): Section 134(3)(d) of the Companies Act, 2013, requires the website address to be included in the Board's Report
- FCRA (Foreign Contribution Regulation Act) regulations: The Ministry of Home Affairs (MHA), which administers FCRA, has clear guidelines for public disclosure, much of which

is expected to be accessible via the organization's website. All FCRA-registered organizations are mandated to place their audited annual accounts (including Income & Expenditure Statement, Receipt & Payment Account, and Balance Sheet) on their official website for every financial year.

Revision #9
Created 2025-06-13 13:15:19 UTC by Pooja
Updated 2025-06-22 14:52:40 UTC by Pooja