Data Protection Guideline for Europe

ISKCON Law Department - Europe

January, 2026

1. Introduction and Purpose

ISKCON in Europe operates within a complex and evolving regulatory environment. Over recent years, European data protection and privacy laws have been applied with increasing rigor to religious, charitable, and non-profit organisations. Regulatory authorities no longer treat faith-based institutions as informal or exempt entities. Temples, centres, yatras, and affiliated entities are now expected to meet the same standards of compliance, transparency, documentation, and accountability as other organisations operating within the European Union.

ISKCON entities across Europe regularly process personal data in the course of their religious educational, administrative, and governance activities. This includes, among other things, the handling of donor records, congregational and contact databases, volunteer information, mailing lists, online platforms, and security systems such as CCTV. At present, the level of preparedness and consistency in data protection practices varies significantly across temples and ministries in different countries. In some cases, personal data is managed informally or without a clear compliance framework, creating unnecessary legal, organisational, and reputational risk.

This European Data Protection Guideline has been developed to address these challenges in a structured and proactive manner. Its purpose is to provide ISKCON leaders with a clear and practical framework for understanding how European data protection requirements apply to ISKCON's activities, without reproducing or restating the GDPR in full. The Guideline is intended to serve as a navigational document, helping leaders identify key responsibilities, risk areas, and minimum standards, rather than as a technical or procedural manual.

The Guideline applies to ISKCON entities operating within Europe, regardless of their specific legal form under national law, and is relevant to European ministries coordinated by the Euro RGB, as well as to local temples, centres, and yatras. It reflects ISKCON's organisational reality, including advisory, educational, assistive, executive, and promotional activities carried out at both regional and local levels.

Clear and respectful handling of personal data is not only a legal requirement, but also an element of good governance that contributes to the credibility, safety, and long-term stability of ISKCON's religious and charitable mission across Europe.

2. Introduction to GDPR and Its Relevance to ISKCON

The General Data Protection Regulation (GDPR) is the primary European legal framework governing the collection, use, and protection of personal data. Its purpose is to safeguard the rights and dignity of individuals by ensuring that personal information is handled lawfully, transparently, and responsibly, while enabling organisations to carry out their legitimate activities with clarity and confidence.

For ISKCON and other religious organisations, GDPR is not intended to obstruct charitable, or administrative work. Rather, it provides a common structure that promotes trust, accountability, and good governance. By setting clear standards for handling personal data, GDPR helps protect all parties involved by clarifying responsibilities, reducing uncertainty, and mitigating legal and reputational risks.

2.1 How GDPR Applies to ISKCON

Under Article 2(1) *GDPR, the Regulation applies to any organisation that processes personal data as part of its organised activities, whether through digital systems or structured paper record*s. This includes ISKCON temples, centres, yatras, and affiliated entities operating in Europe, as they routinely handle personal data such as donor records, congregational contact information, volunteer details, mailing lists, online platform data, and CCTV recordings.

Although ISKCON is registered under different legal forms across Europe, including as a religious community, non-profit organisation, or other legal entity under national law, this does not affect the applicability of the GDPR. For the purposes of GDPR, ISKCON may qualify as a religious non-profit organisation that processes personal data relating to its members and supporters in the course of its legitimate religious and organisational activities. This context is expressly recognised in Article 9(2)(d) GDPR, which allows religious bodies to process certain categories of personal data, subject to appropriate safeguards.

The exemptions set out in Article 2(2) GDPR are limited to narrowly defined situations, such as purely personal or household activities carried out by individuals, or specific functions of public authorities. These exemptions do not apply to organisations operating in a structured and institutional manner. Accordingly, ISKCON’s religious or charitable character does not remove it from the scope of GDPR.

2.2 Territorial Application of GDPR

Under Article 3(1) GDPR, the Regulation applies to the processing of personal data by any ISKCON temple, centre, yatra, or affiliated entity established within the European Union, where such processing takes place in the context of its activities, regardless of where the data is stored or processed.

In addition, Article 3(2) GDPR extends the application of the Regulation to certain activities of ISKCON entities outside the EU where they involve the processing of personal data of individuals located in the EU, for example through websites, online donation platforms, or electronic communications.

Accordingly, GDPR applies fully to ISKCON’s activities across Europe and obliges ISKCON entities to adopt a consistent, Europe-wide approach to data protection governance.

3. Key Definitions

For the purposes of effective understanding and implementation of European Data Protection Guideline, the relevant terms have been defined below. These definitions are based on *Article 4 of the General Data Protection Regulation (GDPR)* and are interpreted in light of ISKCON's religious, charitable, and organisational activities.

**Terms not defined in this section shall have the meaning given to them under the GDPR.*

3.1 Personal Data

Article 4(1) GDPR

Personal data means any information relating to an identified or identifiable natural person. This includes information that directly identifies a person, such as a name or contact details, as well as information that can indirectly identify a person. For example, In the ISKCON context, personal data includes donor records, congregational contact details, volunteer information, mailing lists, data collected through online platforms, and images or recordings from CCTV systems where individuals can be identified.

3.2 Processing

Article 4(2) GDPR

Processing refers to any operation performed on personal data, whether automated or manual. This includes the collection, storage, use, sharing, updating, or deletion of personal data. For ISKCON entities, processing occurs whenever personal data is handled in the course of religious, administrative, communicational, governance, or security-related activities.

3.3 Data Subject

Article 4(1) GDPR

A data subject is the individual to whom personal data relates. Within ISKCON, data subjects typically include devotees, donors, congregation members, volunteers, employees or service providers, website users, and visitors to temple premises.

3.4 Controller

Article 4(7) GDPR

A controller is the organisation or body that determines the purposes and means of processing personal data. In practice, ISKCON temples, centres, yatras, and European ministries may act as controllers in relation to the personal data they process, if they solely decide why such data is collected and how it is used.

3.5 Consent

Article 4(11) GDPR

Consent means a freely given, specific, informed, and unambiguous indication by which a data subject agrees to the processing of their personal data. Within ISKCON activities, consent is particularly relevant for mailing lists, newsletters, fundraising communications, and the publication of identifiable images or media, where individuals must have a genuine choice and the ability to withdraw consent.

4. Core Data Protection Principles

(Article 5 GDPR – ISKCON Context – Condensed Version with Examples)

The GDPR establishes a set of core principles that apply to all processing of personal data. These principles guide how ISKCON entities handle personal data relating to donors, congregation members, volunteers, communications, online platforms, and security systems.

4.1 Lawfulness, Fairness, and Transparency

Personal data must be collected and used only for legitimate purposes and in a manner that is fair and transparent. ISKCON entities should be able to explain, in simple terms, why personal data is collected, how it is used, and who is responsible for it. *Example:* When a temple collects contact details for festival registration, participants are informed that their data will be used for event-related communication and general temple updates, and are provided with a contact point for questions.

4.2 Purpose Limitation and Data Minimisation

Personal data should be collected for clear and specific purposes and limited to what is reasonably necessary for those purposes. ISKCON entities should avoid collecting excessive or unnecessary information and should not reuse personal data for unrelated activities without a proper basis. *Example:* When volunteers sign up for temple service, the temple records only basic contact details and availability, and does not collect unrelated personal or financial information that is not needed for volunteer coordination.

4.3 Accuracy and Storage Limitation

Reasonable steps should be taken to ensure that personal data is accurate and not kept longer than necessary. ISKCON entities should correct incorrect information when notified and avoid retaining outdated records. *Example:* If a congregation member asks to update or remove their email address from a mailing list, the list is updated accordingly and old contact details are deleted rather than kept indefinitely.

4.4 Integrity and Confidentiality (Security)

Personal data must be protected against unauthorised access, loss, or misuse. This includes limiting access to authorised persons, applying basic safeguards to digital systems and online platforms, and ensuring that CCTV recordings are used only for legitimate security purposes. *Example:* Donor records are accessible only to designated leaders such as the temple president or treasurer, and CCTV footage is viewed only when needed for security purposes and deleted after a defined retention period.

4.5 Accountability

Responsibility for compliance with these principles rests with ISKCON entities and their leadership. Leaders should be able to demonstrate, at a general level, that personal data is handled responsibly and in accordance with this Guideline. *Example:* When a donor asks what personal data the temple holds about them, temple leadership is able to explain what information is stored, why it is needed, and how it is protected, even if technical systems are managed by others.

4.6 Why This Approach Is Appropriate

This condensed presentation reflects ISKCON's operational reality by emphasising the principles most relevant to its activities while ensuring that all core GDPR principles are addressed in a proportionate and practical manner.

5. Lawful Basis for Processing Personal Data

(Articles 6 and 9 GDPR – ISKCON Context)

Under the GDPR Article 6(1)(f) legitimate interests and Article 9(2) (d), personal data may be processed only where there is a clear and lawful reason for doing so. For ISKCON entities, identifying the lawful basis for processing personal data is essential to demonstrate accountability and to reduce legal, reputational, and personal risk for leaders and trustees.

In the course of its religious, charitable, and organisational activities, ISKCON processes personal data relating to donors, congregation members, volunteers, communications, online platforms, and security systems. In most cases, such processing is carried out as part of ISKCON's legitimate organisational and religious activities. Article 9(2)(d) GDPR expressly recognises the ability of religious organisations to process certain categories of personal data relating to their members and supporters, provided that appropriate safeguards are applied.

Certain personal data is also processed in order to comply with legal and administrative obligations, such as financial record-keeping, tax requirements, or health and safety obligations. In addition, ISKCON entities may rely on consent where appropriate, particularly for mailing lists, newsletters, fundraising communications, and the publication of identifiable images or media, provided that such consent is freely given and can be withdrawn.

Finally, personal data may be processed where necessary to protect people and property, including through proportionate use of CCTV systems for security purposes. ISKCON leaders should be able, at a general level, to explain why personal data is processed and on what basis, even where day-to-day handling is delegated.

6. Risks Associated with Inadequate Data Protection Practices

ISKCON temples, centres, and yatras process personal data in connection with activities such as donor records, congregational databases, volunteer coordination, mailing lists, online platforms, and CCTV systems. Where such data is handled without clear and consistent practices, ISKCON entities are exposed to several significant risks.

Legal and regulatory risks may arise where personal data is misused, insufficiently protected, or handled without transparency. Complaints from donors, volunteers, or congregation members, as well as data breaches or poorly managed mailing lists or CCTV systems, may lead to regulatory inquiries, corrective measures, or financial penalties, as European authorities increasingly apply GDPR standards to religious and non-profit organisations.

Reputational and organisational risks are also substantial. Inadequate data protection practices can undermine trust among devotees, supporters, volunteers, and the wider public. Misuse of contact details, unclear communication practices, or perceived lack of care in handling personal information may negatively affect engagement, participation in activities, and confidence in ISKCON's professionalism and governance.

In addition, **personal responsibility risks** exist for leaders and trustees. Under the GDPR, accountability rests with those who determine how and why personal data is processed. In the absence of clear policies and shared standards, leaders may face increased uncertainty and pressure when responding to complaints, audits, or incidents.

For these reasons, inadequate data protection practices present not only a compliance issue, but a broader risk to ISKCON's credibility, leadership confidence, and long-term stability within the European context.

7. Roles, Responsibility, and Governance

Effective data protection within ISKCON Europe depends on clear responsibility, leadership awareness, and consistent governance, rather than on complex technical systems. Under the GDPR, responsibility for compliance rests with the organisations and individuals who determine the purposes and means of processing personal data. Data protection officers may not be required for most temples, unless legally mandated.

7.1 Responsibility of ISKCON Entities

Each ISKCON temple, centre, yatra, or affiliated entity operating in Europe is responsible for ensuring that personal data under its control is handled in accordance with this Guideline. This responsibility applies regardless of the legal form under which the entity is registered.

7.2 Role of Leadership and Boards

Temple presidents, trustees, ministry heads, and boards involved in decision-making are expected to ensure that organisational practices involving personal data are lawful, appropriate, and consistent with this Guideline. While operational tasks may be delegated, overall accountability for decisions affecting personal data cannot be delegated away.

7.3 Governance and Consistency

This Guideline provides a common framework to support consistent data protection practices across ISKCON Europe. Proportionate oversight by leadership and boards helps reduce risk and supports responsible governance.

8. Implementation and Next Steps

This Guideline establishes the minimum expectations for compliance across all entities. Local bodies may need a short local addendum - such as privacy notices or retention rules - to address specific requirements. Training and awareness initiatives are encouraged, provided they remain proportionate to the context. In this way, leaders gain a clear understanding of the steps that follow adoption, without the Guideline itself becoming an operational manual.

Temple Data Protection Compliance Checklist

1. Governance & Responsibility

- Confirm leadership (president, trustees, boards) understand accountability for personal data decisions.
- Ensure each temple/centre/yatra accepts responsibility for compliance with the Guideline.
- Verify whether a Data Protection Officer is legally required; appoint only if mandated.

2. Core Principles (GDPR Article 5)

- Collect and use personal data lawfully, fairly, and transparently.
- Limit data collection to specific, necessary purposes (no excess information).
- Keep records accurate and delete outdated or unnecessary data.
- Protect data with confidentiality and security safeguards (restricted access, secure systems).
- Be able to demonstrate compliance when asked (accountability).

3. Lawful Basis for Processing

- Identify and document the lawful basis for each type of data processing:
    - Legitimate religious/charitable activities (Article 9(2)(d)).
    - Legal obligations (finance, tax, health & safety).
    - Consent (mailing lists, newsletters, fundraising, identifiable images/media).
    - Security (CCTV, property protection).

4. Risk Management

- Assess risks of inadequate practices (legal, reputational, organisational, personal liability).
- Establish clear complaint-handling and incident-response procedures.

5. Local Addenda

- Prepare short local addenda if required (e.g., privacy notices, retention rules).

7. Records & Documentation

- Archive appeals, update mailing lists, and ensure retention schedules are followed.

8. Communications

- Ensure clarity and confidentiality in all official communications.
- Provide contact points for data protection queries.