LUMARA – Transparency and Data Protection Policy

Purpose:

Establish principles, mechanisms, and responsibilities to ensure organizational transparency and the secure protection of information, especially in sensitive contexts related to the defense of human rights in totalitarian regimes.

I. Transparency Principles
Access to institutional information:

LUMARA will periodically publish its reports, financial statements, activities, institutional donors (when safe), and impact results.

Public access to the founding documents, statutes, and institutional policies will be facilitated.

Active communication:

Digital and physical communication channels will be maintained open with members, allies, and the public.

Legitimate inquiries about the organization's operations will be answered clearly, ethically, and without manipulation.

Accountability:

The organization will file annual financial reports with its members and regulatory authorities (including the IRS).

Periodic internal and/or external audits will be conducted depending on the availability of funds.

II. Protection of Personal and Sensitive Data
Confidentiality of information:

All personal, medical, legal, or security information collected about victims, witnesses, advocates, or LUMARA staff will be treated as confidential.

Only authorized persons will have access based on principles of minimum exposure and operational necessity.

Informed consent:

Any person who provides personal data must do so with free, prior, and informed consent, with the right to withdraw it.

Safe storage:

Encryption and secure storage systems, both digital and physical, will be implemented.

Platforms protected by strong passwords and two-factor authentication systems will be used.

Risk management:

A digital security protocol will be implemented to prevent cyberattacks, leaks, and external or internal threats.

Data deletion:

Personal data will be stored only for as long as necessary and permanently deleted after fulfilling its legal or humanitarian purpose.

III. Responsibilities
Digital Security Coordinator: will be responsible for implementing and supervising technical compliance with this policy.

Legal Director and Director of Research and Documentation: will work together to ensure ethical and legal compliance with information protocols.

Every person affiliated with LUMARA must sign a confidentiality and compliance agreement upon joining.

IV. Violations and Sanctions
Any leak, misuse, or improper exposure of data will be subject to internal investigation.

Violations of this policy may result in disciplinary action, including termination of employment with LUMARA and legal action, if appropriate.

Final Provision
This policy is part of LUMARA's ethical framework and is regularly updated in response to legal, technological, or strategic changes, ensuring that privacy and information rights are respected at all levels of operation.