

Privacy, Data and Image Consent

Collect only necessary information, protect it, use it for the stated purpose and respect people's choices about images and publicity.

MN-DP-01 | Version 1.0 • Published 15 October 2026

Registration status: Registration in progress.

Adopted by authorised management on 15 October 2026 as internal commitments and procedures during registration. This adoption does not imply completed registration or statutory effectiveness of the internal bylaws.

1. Information and purpose

Programme records may include names, contact details, eligibility criteria, functional needs and follow-up services. Before collection, explain the purpose, required information, access, retention and individual rights in an understandable format. Do not collect identity numbers, detailed health information or precise locations merely because they are available. Document necessity for sensitive collection and disclosure.

2. Choice and individual rights

Separate service consent from photography or publicity consent. Individuals can request access, correction, deletion or withdrawal of optional consent through the published email. Where legal or contractual duties or necessary evidence prevent deletion, explain why and minimise retained data and access. Disability does not imply lack of capacity; provide appropriate support to understand and express decisions.

3. Children and images

Explain image use, audience, platforms and possible redistribution outside organisational control. Obtain consent from a safe caregiver and the child's agreement suited to age and capacity, respecting refusal. Depict people with dignity and avoid exposing home locations, health details or a child at risk. Stop future optional use after withdrawal and make reasonable removal efforts, explaining that all internet copies may not be recoverable.

4. Access, storage and sharing

Assign and periodically review role-based access, using appropriate security, backups and recovery. Separate complaint records from general service files. Do not transfer member or participant data to another entity or commercial or political activity for an unrelated purpose. Prefer aggregate reporting. Identifiable sharing with a partner requires necessity, authority and written safeguards, including cross-border transfers where these occur.

5. Retention and incidents

Set retention periods by record type, purpose, law and agreement; do not retain every record indefinitely. Financial records follow their specific requirements and case records undergo continuing-need review. On loss or disclosure, contain the incident, assess risk, preserve evidence and notify affected people and relevant bodies where required without increasing harm. Document corrective action.

6. Website and contact

Netlify hosts this website and may process technical logs needed for delivery and security. Some pages use Google Fonts and external assets, which may contact their providers when loaded. Do not enter safeguarding case details into third-party services or public forms; use the complaints routes and request a safe way to share details. Send privacy requests to muntalaq-alnahda@greatiraq.com, with escalation through the alternate listed on the complaints page.

Governance and document control

Policy owner: Board of Directors, under Article 53 of the approved internal bylaws. Review at least annually and after significant incidents or changed requirements. Arabic and English versions are published together; any ambiguity must be resolved without weakening protection. No past training, screening or donor certification is asserted by this document.

DFAT guidance on images and social media: [Official reference](#)

Web version: greatiraq.com/policies/privacy/en/