IFOR INTERNATIONAL FELLOWSHIP OF RECONCILIATION

DATA PROTECTION GUIDELINES

As a global movement committed to working for peace and nonviolent social change, IFOR seeks to maintain the security of all personal data in its possession. The trust and safety of our members, donors, and partners is of critical importance to us. While we do not have the resources to ensure state of the art protections, we do follow the following guidelines to ensure the protection of all personal data at IFOR.

- Any and all personal data collected is collected with explicit consent. If sensitive data is stored by IFOR then all sensitive data will require additional consent.
- Any requests to remove ones personal data are complied with immediately.
- All IFOR employees, consultants, interns, and volunteers sign an agreement as a part of their contracts requiring them to protect IFOR data and not share that data with any party external to IFOR.
- All data is stored securely and is only accessible to IFOR employees and authorized consultants, interns and volunteers.
- Because IFOR uses cloud-based software enabling our team to work remotely, we work to ensure that the software used has security standards that meet or exceed industry standards. Most if not all programs engaged by IFOR use two-step identification for access.
- IFOR also seeks to use encryption methods to protect the identity of human rights defenders, members, donors, and others.

Updated 18 May 2018

IFOR International Secretariat
Postbus 1528 ✻ 3500 BM Utrecht ✻ The Netherlands
+31.30.303.9930
www.ifor.org