# VOLUNTEER AGREEMENT

*and Confidentiality Deed (including BYOD & Cybersecurity Policy)*

| | |
|---|---|
| **Document ID:** | VOL-AGR-2026-V4.0 |
| **Effective Date:** | [to be completed on execution] |
| **The Organization:** | **RBTF - Environmental Protection - Medical Rescue and Global Defense MTÜ**<br>Järvevana tee 9, EE-11314 Tallinn, Estonia (a non-profit association, MTÜ, registered under Estonian law)<br>(Hereinafter referred to as 'the Organization' or 'emgprd.org') |
| **The Volunteer:** | First and Last Name: _____<br>Street + Nr: _____<br>Town + Zip: _____<br>Country: _____<br>(Hereinafter referred to as 'the Volunteer') |

## Document Version Control & History

| Version | Date | Author | Changes / Update Description |
|---|---|---|---|
| 1.0 | 01.03.2025 | Legal Team | Initial Volunteer Agreement Framework and Confidentiality Agreement. |
| 2.0 | 05.06.2026 | Management | Revised Framework: Implementation of dynamic Advancement Paths (Community Member to Core Member), standard enterprise BYOD & Cybersecurity IT Policies, and explicit Munich (Germany) judicial forum alignment. |
| *3.0* | *18.07.2026* | *Management* | *Consolidated the two separate €25,000 liquidated-damages clauses into a single, unified damages clause; limited fixed liquidated damages to intentional (vorsätzlich) violations; introduced an ordinary-damages standard (no fixed penalty) for grossly negligent violations; clarified that good-faith errors and phishing victimization despite training do not constitute gross negligence.* |
| *4.0* | *18.07.2026* | *Management* | *Added a whistleblower / statutory-reporting carve-out to the confidentiality clause; tiered confidentiality duration (indefinite only for genuine trade secrets, 5 years for other non-public information); softened 'Advancement Path' / 'Core Member' career language to reduce misclassification risk as an employment relationship; made the Organization's own commitments binding rather than best-efforts; added a data-protection (GDPR) obligation for the Volunteer; replaced mandatory full-device endpoint client with a segregated work-profile option and a reference to a separate privacy notice; added an offboarding / access-revocation clause; noted that Estonian association law may govern volunteer-liability privileges regardless of the chosen contract law. Munich jurisdiction retained unchanged at the Volunteer's request.* |

*The Volunteer and the Organization collectively agree to the terms and obligations detailed in this multi-part legal framework:*

# Part I – Terms of Engagement & Extended Responsibilities

## 1. Nature of Agreement & Role Development

The Volunteer joins the Organization strictly as an official Community Member. This operational collaboration is executed entirely on a voluntary, non-compensated basis. Both parties explicitly covenant and agree that:

- This relationship does not constitute, imply, or establish an employment contract, independent contractor agreement, partnership, commercial consultancy, or agency under any international, regional, or domestic law.
- The Volunteer performs all operational tasks voluntarily, waiving any rights to financial compensation, regular wages, overtime salary, severance, or corporate employee benefit programs.
- Role Development: The scope of tasks a Volunteer takes on may broaden over time, based on reliability, experience, and the Organization's operational needs, as reflected through the Volunteer's activity logs in the Organization's systems. This is an informal, non-contractual description of how tasks may evolve and creates no entitlement, timeline, or guaranteed role change, and does not itself alter the non-employment nature of this relationship.
- Future Status Modifications: Should the legal framework of this operational alignment shift toward a compensated structure at any point in the future, such a progression will necessitate independent, formal negotiations culminating in the execution of a separate, written corporate employment agreement.

### 2. Mutual Operational Expectations

To ensure systemic efficiency across a global ecosystem, both parties adhere to the following baseline standards:

- The Organization's Commitments: emgprd.org will provide distinct task parameters, functional role definitions, accessible digital e-learning paths, essential remote infrastructure access, a safe digital ecosystem, and inclusion in the weekly 30-to-60-minute 'Coffee Talk' for community alignment, feedback, and strategic growth.
- The Volunteer's Commitments: The Volunteer pledges to vigorously support the humanitarian, non-profit, and environmental mandates of emgprd.org; execute assigned workloads carefully; complete specialized e-learning security or task models; and meticulously track and log all operational progress natively inside the tracking systems utilized by the organization.

### 3. Agreement Duration and Separation Rules

- This operational agreement takes effect immediately upon the electronic execution of signatures by both parties and remains active for an indefinite term.
- Initial Collaboration Phase: The inaugural three (3) months of active engagement are structurally classified as an Initial Collaboration Phase. During this specific term, either the Volunteer or the Organization may immediately terminate this agreement without notice, without penalty, and without a statement of cause.
- Subsequent Separation: Following the Initial Collaboration Phase, either party may terminate the volunteer relationship at any moment via written notification delivered through official Slack communications or enterprise email. This separation takes effect immediately upon receipt.

### 4. Offboarding & Return of Assets

- Upon termination of this agreement for any reason, the Organization will revoke the Volunteer's access to all organizational accounts, systems, and communication channels (Google Workspace, Slack, GitLab, Odoo, and any other tools) within 24 hours of the termination taking effect.
- Within 7 days of termination, the Volunteer must, to the extent technically possible, delete all local copies of confidential Organization data from personal devices and confirm this in writing, and must return or destroy any Organization-provided hardware or access credentials.
- Obligations under Part III (Confidentiality) survive offboarding as set out in that Part.

## Part II – Enterprise IT, BYOD & Cybersecurity Policy

### 1. Purpose & Scope of the IT Security Framework

Because emgprd.org operates as a highly decentralized, digitally-driven global non-profit infrastructure, our digital workspace, infrastructure integrity, and donor privacy rely heavily on localized device security. This Bring Your Own Device (BYOD) and Cybersecurity framework governs any personal technology (computers, tablets, smartphones) used by the Volunteer to access corporate networks, Google Workspace accounts, Odoo ERP architectures, or internal communication nodes.

## 2. Hardened Device Security & Access Protocols

The Volunteer explicitly agrees to institute and preserve the following cybersecurity controls on all hardware assets interacting with Organization data:

- Mandatory Multi-Factor Authentication (MFA): The Volunteer must activate MFA on all organizational accounts (Google Workspace, Slack, GitLab, Odoo) utilizing approved authenticator apps. Password reuse across internal and personal channels is strictly prohibited.
- System Patching and Endpoint Health: Host operating systems (Windows, macOS, Linux, iOS, Android) and critical applications must remain updated with active vendor security patches. Devices running obsolete, 'end-of-life' (EOL), or jailbroken/rooted operating systems are permanently banned from network interactions.
- **Malware Mitigation & Corporate Endpoint Audits:** Where the Organization determines that additional endpoint protection is necessary for access to high-security infrastructure, the Volunteer will be offered a **segregated work profile or containerized workspace** (e.g., a separate managed browser profile, virtual desktop, or mobile work-profile) rather than a full-device security client, wherever the underlying systems make this technically possible. Any endpoint software that is installed operates purely to block malicious payloads and detect cross-network attacks; it does not monitor private user data, log personal activities, or track non-corporate browsing profiles. The specific technical scope of any such tool will be described in a separate, plain-language privacy notice provided to the Volunteer before installation.
- Prohibition of High-Risk Digital Activities: The Volunteer must not use devices actively connected to emgprd.org environments to visit unverified file-sharing networks, execute illegal streaming platforms, download pirated data, or engage in behavior that exposes the parallel enterprise environment to digital infection.

## 3. Liability, Cyber Incidents, and Confidentiality Breaches — Unified Liquidated Damages

- Reporting Mandate: The Volunteer must notify the IT Security Department immediately (within a maximum of 2 hours) upon suspecting or discovering any cyber anomaly, active data leak, credential compromise, or device theft involving assets configured with organization profiles.
- **Intentional Violations (Vorsatz):** If the Volunteer intentionally breaches the cybersecurity protocols set out in this Part II or the confidentiality obligations set out in Part III — including deliberate deployment of malicious software, deliberate circumvention of firewall policies, deliberate unauthorized disclosure of confidential information, or deliberate use of unauthorized network scanning utilities — the Organization may terminate this agreement with immediate effect and claim liquidated damages of **up to €5,000 per proven intentional incident, capped at a combined total of €15,000** for all such incidents arising from the volunteer relationship. This is a single, unified claim covering cybersecurity and confidentiality violations together; it does not apply twice to the same underlying conduct. Where the Organization's actual, independently proven loss exceeds this amount, the additional loss remains claimable through ordinary judicial channels.
- **Grossly Negligent Violations:** If the Volunteer, through gross negligence — meaning a serious and obvious disregard of the care that could reasonably be expected in the circumstances — causes verified operational disruption, financial loss, or architectural damage to emgprd.org, the Organization may terminate this agreement and seek compensation limited to the actual, proven direct damages caused. The fixed liquidated damages amount above does not apply to merely negligent conduct. **For the avoidance of doubt,** gross negligence does not include good-faith errors, isolated oversights, or falling victim to a sophisticated phishing or social-engineering attack despite having completed the required security training.
- Ordinary Negligence: Isolated, non-repeated lapses that do not amount to gross negligence or intentional misconduct do not give rise to liability under this section.

### 4. Data Protection (GDPR) Obligations

- The Volunteer must process any personal data encountered in the course of volunteer activities (including donor, partner, or beneficiary data) only for the purposes assigned by the Organization, in line with the GDPR and the Organization's data protection policy, and must not copy, export, or share such data outside approved Organization systems.
- The Volunteer must report any suspected personal data breach to the Organization within the same 2-hour window set out in Section 3 above, to allow the Organization to meet its own regulatory notification deadlines.

## Part III – Restrictive Covenants & Confidentiality Deed

### 1. Non-Disclosure of Corporate Trade Secrets

The Volunteer acknowledges that during their tenure, they will gain access to proprietary information, digital architectural methodologies, and secure databases owned by emgprd.org. The Volunteer binds themselves to the following restrictive terms:

- **Core Trade Secrets (indefinite):** The Volunteer shall maintain strict, indefinite secrecy regarding the Organization's genuine trade secrets — proprietary codebases, customized Odoo ERP system maps, database infrastructure configurations, donor registries, and tactical operational methodologies for medical or environmental emergency deployments.
- **Other Non-Public Information (5 years):** Other non-public technical, economic, structural, or strategic information encountered during or adjacent to volunteer execution — including partner contracts and internal development visions not covered above — remains confidential for five (5) years following termination of this agreement.
- Exceptions: This confidentiality mandate ceases to apply to information that has legally passed into the public domain through no fault or breach of the Volunteer, or information explicitly authorized for public release via formal management declaration. In case of localized ambiguity, the Volunteer is legally bound to obtain definitive written clearance from an official supervisor prior to any data dissemination.
- **Statutory & Whistleblower Reporting:** Nothing in this Agreement restricts the Volunteer's right to report suspected unlawful conduct to a competent public authority, regulator, or law-enforcement body, or otherwise exercise statutory whistleblower protections, and no liability or penalty under this Agreement attaches to such a report made in good faith.
- Post-Termination Survival: The confidentiality requirements outlined within this deed survive the expiration, termination, or formal cancellation of this volunteer relationship for the durations set out above.

### 2. Public Relations, Media Protocols, and Social Asset Protections

- Authorized Public Relations: The Volunteer agrees to clearly credit emgprd.org in external public presentations, professional research portfolios, or academic publications detailing project work. However, the Volunteer is strictly barred from conducting formal interviews, releasing statements to journalists, or acting as an organizational spokesperson across print, broadcast, or digital media platforms unless possessing an explicit, prior written mandate issued by the Management Team.
- Social Media Boundaries: To ensure systemic operational security, the Volunteer must never publish internal software interfaces, non-public operational visuals, unreleased project designs, or internal administration layouts on personal social media channels, personal blogs, or open web forums. Amplifying, sharing, or linking to content officially published by authorized emgprd.org channels is warmly encouraged.

### 3. Enforcement & Choice of Law / Jurisdiction

- **Contractual Enforcement:** A culpable, verified violation of this Confidentiality Deed is addressed exclusively under the unified liquidated damages provision set out in Part II, Section 3 above (intentional violations up to €5,000 per incident, capped at €15,000 combined; grossly negligent violations limited to proven actual damages). No additional or separate fixed penalty applies under this Part III. Standard criminal or civil exposure under applicable trade secret protection statutes remains unaffected.

- Choice of Law and Legal Forum: This Volunteer Agreement, including its appended IT Security Policies and Confidentiality Deed, shall be exclusively governed by, construed under, and enforced via the laws of Germany. The parties explicitly covenant to submit all civil, administrative, or operational disputes arising out of this relationship to the exclusive jurisdiction of the courts located in Munich, Germany (Europe).

---

*This is a working draft prepared for internal review. It has not been reviewed by a lawyer qualified in German and Estonian law and should be checked by one before it is put back into use — in particular the enforceability of the liquidated-damages cap under §307 BGB, the whistleblower carve-out's alignment with the Hinweisgeberschutzgesetz, and whether Estonian association law affects any assumed volunteer-liability privileges.*

**--- SIGNATURE PAGE & EXECUTION OF DEED ---**

| **FOR THE VOLUNTEER:** | **FOR THE ORGANIZATION (emgprd.org):** |
|---|---|
| Signature of the Volunteer<br><br>Date: _____<br>Place: _____ | Authorized Management Signature<br><br>Name: _____<br>Position: _____<br>Date & Place: _____ |