JESUIT REFUGEE SERVICE

Request for Proposals (RFP)

FOR

DATA PROTECTION AND SECURITY

Procurement Reference Nr.	JRSIO/RFP2025/DP
Closing Date	15/06/2025

Contents

1. **Purpose/Background/Context of the role:** 4

a. **Organizational Context:** 4

b. **Operational Context:** 4

2. **Scope of work:** 6

3. **Methodology** 6

4. **Expected Deliverables:** 7

5. **Timeline** 8

6. **Expected outcome** 8

7. **Qualifications** 8

8. **Remuneration** 9

9. **Contact Person** 9

10. **Confidentiality** 9

11. **Application submission and selection criteria** 9

Introduction 9

Clarification on RFP Documents 9

Submission of proposal 10

Applicants should submit the following documentation: 10

Technical Proposal: 10

• A proposed action plan outlining the approach and methodology to deliver the requested service. 10

• A CV demonstrating compliance with the stated requirements, or a company profile that illustrates relevant expertise. 10

• A sample of previous work related to data protection policy development, if available. 10

Financial Proposal: 10

• A comprehensive price quotation, clearly detailing the cost breakdown, including all applicable taxes and VAT. 10

• 10

Submission and receipt of Proposals 10

Award Criteria 10

Due Diligence 11

Award of Contract 11

Confidentiality 11

Corrupt or fraudulent practices, conflict of Interest 11

Appendices.. 11

1. Purpose/Background/Context of the role:

Organizational Context:

The Jesuit Refugee Service (JRS) is an international non-governmental organization whose mission is to accompany, serve, and advocate for the rights of refugees and forcibly displaced people. The organization was founded in November 1980 and now has a presence in over 58 countries, divided into 9 Regions. JRS undertakes services at national and regional levels with the support and guidance of an International Office (IO) in Rome. JRS service is human and spiritual, working in situations of greatest need, seeking the long-term well-being of refugees and displaced people while not neglecting their immediate or urgent needs. The main services provided are in the fields of economic inclusions and livelihood, education, MHSPP, reconciliation, global advocacy and effects of climate change on displacement. Currently, 1.2 million individuals are beneficiaries of JRS project worldwide.

For further information on JRS, its mandate, and operations, please visit our website: http://www.jrs.net.

Operational Context:

In compliance with evolving data protection regulations and to ensure the highest standards of data security, we are seeking the expertise of a Data Protection Consultant.

On achieving his mission different data are processed and collected and JRS operates a globally distributed IT infrastructure designed to support operational and administrative activities across 58 countries and regional offices.

The infrastructure is cloud-based and centrally managed by the JRS International Office, ensuring a standardized approach to data management, security, and user support.

Current IT Infrastructure:

1. **Data Management:**
   - Centralized databases hosted in Europe, offering scalable and easily accessible storage for several types of data.
   - Key systems include:
     - **SQL Server** for handling transactional data, payroll systems, IMS (GMT, HRM, PME)
     - **Cloud storage solutions** like **Microsoft Azure** for backups and data archiving. Data is stored on European servers
     - Networking monitoring services
     - **Unifi** internet and Local Area Network management platform
2. **Microsoft Account Services:**
   - **Microsoft Exchange** Email services.
   - Document collaboration tools through **SharePoint, OneDrive, Azure Blob Storage**.
   - Financial and operational tools such as **Microsoft Dynamics NAV** and **Business Central**.
   - Productivity applications like **Word**, **Excel**, and **PowerPoint**.

3. **Management and Maintenance:**
    - The IT infrastructure is maintained via the **Microsoft 365** platform, with user management (creation and password policies) handled centrally.
    - The platform supports approximately **1000 E3 licenses** and **2000 E1 licenses**, with all tenant data stored on European servers

JRS handles a variety of sensitive data across its global operations, reflecting the diverse nature of its work and stakeholders. The primary categories of data managed by JRS include:

1. **Beneficiary Data**: At the heart of JRS's mission are the individuals and communities it serves. Data collected from these beneficiaries can range from demographic information to personal details necessary for delivering targeted assistance programs, such as:

    - **Personal Information** (Name, Date of Birth, Gender, Nationality, Address)
    - **Health & Medical Records** (if providing medical aid)
    - **Socioeconomic Information** (Income, Education, Vulnerability status)
    - **Case Management Records** (Services provided, follow-up history)
    - **Personal images** (Photo, Video)

    Beneficiary data are mainly stored on PME, Excel, Kobo, Local databases etc.

2. **Staff and Volunteers Data:** The organization manages comprehensive personal data related to its employees and contractors across the 58 offices. This includes information such as
    - **Employer and Volunteers records** (identifications details)
    - **HR Records** (Contracts, Salary, Performance reviews)
    - **Background Checks** (Security clearance, References)
        - **Training & Certifications**

    The current storage is hosted in separate SharePoint sites, but not all regions are using this platform to store data.
    Staff data are mainly stored on HRM, NAV, Payroll, DocuSign etc.

3. **Donor Data and Fundraising Data:** JRS collects and maintains personal and financial information from its donors, who provide the essential support needed to sustain the organization's mission. This data includes not only contact details but also financial records that are crucial for processing donations and ensuring transparency in how funds are allocated, such as:

    - **Donor Information** (Name, Contact details, Organization details)
    - **Donation Records** (Amount, Frequency, Payment Method)
        - **Grant Agreements & Contracts**
        - **Restricted vs. Unrestricted Funds Allocation**

    Donor and FR data are mainly stored on GMT, NAV, Salesforce etc.

4. **Key JRS stakeholders**

    JRS collaborates with many stakeholders and collect or share sensitive information about joint projects, research or initiatives

    - Partner and consultant information
    - JRS Governance body members (Board members, Administrative Council, and other stakeholders involved in JRS governance that may have access to strategic or financial data).

5. **Financial and Accountability data:**

   - **Budgets & Expenses**
   - **Bank Account Details**
   - **Payroll & Tax Information**
   - **Procurement & Vendor Information:** As JRS engages with numerous external service providers and vendors worldwide, it collects relevant business information from these entities. This data is used to manage agreements and process payments

6. **Communication & Advocacy Data**

   - **Email Communications**
   - **Meeting Records & Reports**
   - **Social Media & Public Relations Data**

7. **IT & System Security Data**

   - **User Login Credentials & Access Permissions**
   - **Encrypted Files & Backup Data**
   - **Incident Reports** (Cybersecurity threats, breaches)

The procedures and the minimum requirements relating to the processing, collection, and storage of data according to the GDPR are currently not unified at a global level and no data protection policy and data exchange agreement has been officially adopted and implemented at a global level, while some Regions have an internal DPP or other policies with similarities with the DPP that covers the COs managed by the region.

2. Scope of work:

The primary objective of this consultancy is to assess JRS' current data protection practices, identify areas for improvement, and develop a comprehensive global policy to enhance data security and compliance with relevant regulations.

3. Methodology

The consultant will have to work by his/her own means to develop the required activities.

An initial **desk review** for JRS assessment to be carried out, in consultation with a global JRS task force team composed by

- **Organizational Development and Financial Planning Advisor,** as JRS Task Force Manager
- **Leadership Coordination Officer**
- **IO Head of Finance**
- **HR Officer**
- **HR Director**
- **IT Director**
- **IMS System Engineer**
- **Communication Representative**

- **IT Field Representatives**

The desk review and assessment phase must include

- interviews and meetings with the different JRS Regional Directors (five regions) to contextualize the global policy at various levels,
- meetings with key staff from the different JRS operational areas at various levels (International Office, Regional Office, Country Office)

Meetings with the Data protection cluster of UNHCR are also recommended.

4. Expected Deliverables:

The consultant is expected to deliver the following products in English within 6 months of the beginning of the consultancy:

- **Organizational privacy model (roles and responsibilities) and processes (e.g., privacy by design & by default, extra-EU data transfer)**
- **Global data protection policies - organizational privacy model and processes: draft / review for global adoption:**
    - Creation and revision of privacy organizational models, procedures, and policies.
    - Identification of the 'privacy roles and responsibilities' of those involved in the processing of personal data.
    - Verification, preparation or updating of legal privacy-data protection documentation (register of data processing) ensuring compliance with principles of privacy by design and by default.
    - Policy must identify the following processes:
        - **Data lifecycle and information lifecycle management** to create the framework to manage data (from creation to storage to archiving to destruction).
        - **Data loss and data breach prevention:** Revising activities (such as storing, archiving, and securing data with encryption technologies) in place to ensure prevention of data loss and data breach.
        - **Data storage management; data backup and recovery:** identify all activities associated with securely moving production data into a secure storage repository -- whether on-site, off-site in a cloud or managed service provider environment, or a hybrid of these options.
        - **Protecting data sovereignty; confidentiality, integrity, and availability**
        - **Cybersecurity management and ransomware protection**: access management software, perimeter security software and hardware, antivirus software and anti-phishing software, endpoint protection platforms, and endpoint detection and recovery systems.
        - **Data access management controls and password management**
        - **Extra-EU data transfer**
    - Define procedures; standards and regulations compliance: policies establish the "what" associated with data protection activities, while procedures define the "how" activities. Both are essential in a data management program and are typically examined as part of the audit process. A data

protection policy can be a standalone document or be embedded within a larger data management policy.

- **Protocols of data exchange between offices**
  Mapping of international data flows and preparation of necessary documentation to regulate privacy roles between legal entities and manage transfers from a privacy perspective:
    - Appointment of data controller/co-ownership agreement.
    - Standard contractual clauses/binding corporate rules; Data transfer impact assessment.
    - Drafting and negotiation of data processing/exchange agreements between data controllers and data processors

upon completion of these first two streams, a further consultancy phase may be considered, involving training & awareness for the implementation of the organizational model outlined in stream 1 and support in the selection of data management tools.

5. Timeline

The consultant is expected to deliver the following products within 6 months of the beginning of the consultancy. If the applicant considers that more time is needed, please provide evidence to help the assessment at the selection stage.

- **Inception report** due within 4 weeks of the contract start date.
- **Draft Data Protection Policy** due within 12 weeks of contract start.
- **Final Data Protection Policy** and Implementation Plan due within 20 weeks of contract start

6. Expected outcome

- **Inception report:** A detailed plan outlining the methodology, timelines, and key stakeholders to be consulted.
- **Comprehensive Global JRS DPP (Data Protection Policy)** with clear guidelines and procedures to data Protection.
- **At least 2 Regional JRS DPP finalized**
- **1 Data Exchange Protocol model/template developed**
- **1 Report of conclusions,** which should include: recommendations on standard operating procedures, and accountability and supervision structure

7. Qualifications

- Technical skills and experience:
    - Solid experience in managing and implementing data protection programmes
    - Experience with Record of Processing Activities (RoPA) or Data Privacy Impact Assessments (DPIA)
    - Knowledge of any Data Security Solution tools
    - Knowledge of Microsoft 365 application is an advantage (Share point, One drive, Teams, and Outlook app.)

    - Familiar with Data Management and Privacy, e.g. One Trust, TrustArc, Collibra, BigID
    - Have a proven record of accomplishment of analyzing workflows/ processes/system and effectively documenting them
    - Considerable experience in the internation data protection contest and legislation (EU-GDPR)
    - Previous experience working with international non-profit organizations is strongly recommended but not mandatory.
    - Previous experience working with special categories of data such as refugee data, forced displaced and/or data issued from conflicts areas.
    - The possession of a certification by the international Association of Privacy Professionals (IAAP) is considered an asset. (i.e., certification in Information Privacy Association and certified Information Privacy Professional etc.)
- Legal knowledge:
    - Strong knowledge of domestic and global Data Protection laws, regulations, and standards including European GDPR and the Data Protection Act 2018

8. Remuneration

Payments will be made in accordance with the Consultant/Firm's proposed offer and signed contract, in different installments based on the agreed deliverables and timeline, by bank transfer 30 days from the date of receipt of the invoice, which must be addressed to: JRS Jesuit Refugee Service Borgo Santo Spirito 4 00193 Rome - CF. 97229380585

9. Contact Person

The Task Force Manager will be the primary point of contact at JRS, providing guidance and feedback throughout the consultancy.

10. Confidentiality

The consultant will sign a confidentiality agreement/NDA to ensure all data and information shared during the consultancy remain strictly confidential.

11. Application submission and selection criteria

Introduction

The Applicant is invited to submit a technical proposal and a financial proposal for the services required in the assignment outlined in the request for proposal.

A sample of previous work related to data protection policy development (If available).

Clarification on RFP Documents

Applicant may request clarifications regarding the RFP in writing via email to io.procurement@jrs.net, using in the subject the Procurement Reference Number: JRSIO/RFP2025/DP. JRS will provide responses via email.

Submission of proposal

Applicants should submit the following documentation:

- **Technical Proposal:**

A proposed action plan outlining the approach and methodology to deliver the requested service.

A CV demonstrating compliance with the stated requirements, or a company profile that illustrates relevant expertise.

A sample of previous work related to data protection policy development, if available.

- **Financial Proposal:**

A comprehensive price quotation, clearly detailing the cost breakdown, including all applicable taxes and VAT.

Submission and receipt of Proposals

- The proposal (Technical Proposal and Financial Proposal) shall be submitted in PDF format and as an email attachment. Proposals submitted as links will not be considered.
- Proposals must be submitted electronically to: io.procurement@jrs.net , referencing in the subject the Procurement Reference Number and the name of the Firm/Consultant.
- Late submissions will not be considered. Any bid received by JRS after the deadline for submission of bids shall be rejected and not considered.
- The Proposal must remain valid for 180 days from the submission date. During this period, the Bidder is required to ensure availability of the proposed professional staff for the assignment. JRS will make every effort to complete negotiations within this timeframe.

Award Criteria

All submissions received will be reviewed and evaluated according to the following criteria:

- **Technical proposal:** 60%

The selection criteria will include the following:

i. Experience of the consultant/firm in relation to the scope of the assignment.
ii. Proposed methodology to deliver the required services:
iii. Estimated Timeframe

- **Financial proposal:** 40%

The selection criteria will include the following:

i. Cost competitiveness
ii. Alignment with the technical proposal

A procurement committee will review the proposals and decide on the successful bidder before June 15, 2025.

Due Diligence

- JRS shall conduct due diligence to confirm and verify the qualifications and suitability of the selected bidder before awarding the contract.

Award of Contract

- The Contract will be awarded following successful negotiations.
- The parties must sign the contract within 30 days of the award notification unless there is a request for administrative review.
- JRS may at any time terminate the procurement process before awarding the contract without any further liability.

Confidentiality

Information related to the evaluation of proposals and award recommendations shall not be disclosed to the Bidders or to other persons not officially concerned with the process, until the evaluation is completed, and the report is approved.

Corrupt or fraudulent practices, conflict of Interest

- JRS requires that the Applicant adhere to the highest ethical standards during the selection and execution of the consultancy contract.
- The Applicant must submit a signed declaration (appendix 1) confirming that they have not been, and will not be, involved in any corrupt or fraudulent practices.
- The Applicant must also submit a signed declaration confirming the absence of any conflicts of interest. It must promptly disclose any potential conflicts that arise during the procurement process.
- JRS will reject the proposal and reserve the right to terminate the contract if it determines that the Bidder has engaged in corrupt or fraudulent practices or has a conflict of interest.

Appendices

Appendix 1: Declaration of Non-involvement in Corrupt or Fraudulent Practices

absence of conflict of interest

GDPR: General Data Protection Regulation, n.d.

Protection of Personal Data of Persons of Concern to UNHCR, n.d.

WFP (World Food Programme) Guide to Personal Data Protection and Privacy, n.d.