14.07.2022

# Enterprise Risk Management and GDPR documentation platform

## Background

The Danish Refugee Council (DRC) assists refugees and internally displaced persons across the globe. DRC provide emergency aid, fight for their rights, and strengthen their opportunity for a brighter future.

With its headquarters (HQ) in Copenhagen, a network of regional offices (RO) and country offices (CO), DRC oversees risk, compliance and governance in more than 45 countries.

In a large, decentralized, and global organization with a high focus on Data Protection in general, it entails and requires DRC to live up to Data Privacy principles in day-to-day work. The ongoing effort of protection not only beneficiaries, but also partners and employee’s personal data it has been recognized by the management that a common GDPR & Data Privacy platform is needed to benefit from the unified approach and documentation standards.

DRC is therefore, searching for a platform that would enable an integrated and structured approach to these matters.

1. Enterprise Risk management. A robust, agile, and friendly user tool to manage, ensure relevance and progress in the treatment of risks across the organisation.
2. A platform to accommodate “Documentation of Compliance” (DoC) for General Data Protection Regulation (GDPR) and Data Privacy.

## Platform requirements

**Risk management**

Overall, the platform helps ensure that risk management is in line with the organisations’ strategic and operational goals.

More specifically DRC seeks to achieve this objective through the following outcomes:

1. Enable risk information to be recorded in a systematic and simple manner to help the first and second lines of defense to monitor and report risks and to capture relevant risks for escalation to the attention of senior management.
2. Increases oversight and accountability.
3. Increases digitalisation and enables more effective workflows.
4. Reduces administration time and bureaucracy.
5. Enable a more proactive risk management activity and better handled recommendations.
6. Provides customised reports and visualization of data.
7. Contribute to eliminating risk siloed information.

**General Data Protection Regulation (GDPR) and Data Privacy**

Overall, the platform needs to provide a guided approach and a blueprint for DoC that fits into DRC’s global operating model for reaching a satisfactory level of GDPR and Data Privacy compliance defined by DRC. The platform should establish an overview of current compliance gaps, risks towards data subjects, and a process for annual review.

More specifically DRC seeks to achieve this objective through the following outcomes:

1. A platform that is ease of use to support day-to-day operation regarding Data Privacy documentation and follow-up activities via a guided approach (user-friendly and intuitive)
2. A mapping of Data Privacy related processes, systems, and data objects enabling art. 30 in GDPR
3. A risk-assessment of the Record of Processing Activities (RoPA)
4. An overview of the current Data Privacy compliance level visualized via dashboard or other reporting functionalities
5. Additionally, but not exhaustive or limiting, covering following features:
   1. Handling of policies and procedures
   2. Handling of Data Processor Agreements (DPA)
   3. Risk and control management of threats and vulnerabilities (e.g., incl. other risk frameworks)
   4. Incident management (e.g., data breaches)

In short, the DRC seeks to operationalize and centralize the GDPR and Data Privacy effort in a shared platform.

## Scope of the assignment

DRC operates globally in more than 45 countries; however, the focus and scope of the implementation is HQ in Denmark, and two to four country operations. The goal is to gradually expand to all countries where DRC operates.

**Risk management**

Currently, the risks assessments are being managed in excel spreadsheets at the entity level, which will be a starting point for creating a baseline in the new platform.

Thus, the criteria for implementations are:

* The implementation should cover one to four countries selected by DRC for migration from the excel to the new platform.
* Recommend and implement role-based platform governance (admin, super-users, users etc.)
* Based on best practice, setup relevant annual review activities to be conducted on monthly, quarterly, bi-annually, or yearly basis
* Configure relevant reporting mechanisms and dashboards (if not out-of-the-box feature)
* Relevant training and guidance enabling the users to be self-sufficient in terms of i.e., train-the-trainer, guidelines, best practices, and platform communities among others.

**General Data Protection Regulation (GDPR) and Data Privacy**

Today, some of the data privacy processing activities in HQ have been documented in a SaaS-based compliance software, which will be a starting point for creating a baseline in the new platform.

Thus, the criteria for implementations are:

* The implementation should cover three to four business units in HQ selected by DRC to document their data privacy processing activities
* Data from the SaaS-based compliance software to be exported to Excel or similar and documented into the new platform, if applicable
  + For business units without previous data available, the platform provider should document the data privacy processing activities directly in the platform
* Review with business units and update with additional information needed to complete the assessment/overview in the new platform
* Recommend and implement role-based platform governance (admin, super-users, users etc.)
* Based on best practice, setup relevant annual review activities to be conducted on monthly, quarterly, bi-annually, or yearly basis
* Configure relevant reporting dashboards (if not out-of-the-box)
* Relevant training and guidance enabling the users to be self-sufficient in terms of i.e., train-the-trainer, guidelines, best practices, and platform communities among others.
* Present the result to the management team from the documentation of data privacy processing activities, including article 30 report with risks identified, and appropriately, recommendations for a global implementation approach based on best practices

## Timeline and renumeration

The scope of work to start on October 1st, 2022, or shortly thereafter and completed by November 15th, 2022.

The price for conducting the assignment will be paid 30 days after the receipt of the final presentation, reporting, project sign-off and invoice.

## Purchase agreement

The purchase agreement needs to assign for 24 months with the possibility of 2 x 12 months extension on licenses.

DRC expects following financial information provided:

* Total Cost of Ownership (TCO) for 24 months, including but not limited to:
  + Any initial start-up cost
  + Annual running costs (monthly/yearly)
  + Implementation costs (see attachment: A.2 Financial Offer Bid Form)
  + Other cost

Additionally, before extension of contract after 24 months, a negotiation process is required minimum 3 months prior to original contract termination.

## Qualifications

**Platform**

* Proven Enterprise risk management and GDPR and Data Privacy platform, ideally recognized by peers, Governance, Risk & Compliance (GRC) or Privacy Enhancing Technology (PET) community (e.g., Gartner Magic Quadrant, GRC software ranking lists etc.)

**Implementation**

* Proven experience in advising NGOs or international organizations in achieving desired risk management and GDPR and Data Privacy compliance via platform implementation
* Proven experience in training end-user and ensuring adoption of platform in day-to-day operations

## Proposal Evaluation

For the award of this project, the evaluation criteria below will govern the selection of offers received. The evaluation is made on a technical and financial basis.

The proposed offers by bidders will be evaluated using the following criteria, and points will be allocated in a scale from 1 to 10 for each of the criteria stipulated below, whereas the weighting is as follows:

|  |  |
| --- | --- |
| 1. **Proposed services**   (Documented with the technical proposal (max 2 pages) and technical specification list) | * Content of the proposal suitable for the requirements * Demonstration of required features (65%) |
| 1. **Prior experience**   (Documented with list of relevant references) | * Experience of implementation at NGOs * Experience of global implementation (15%) |
| 1. **Proposed methodology**   (Documented with deliverables and benefits) | * Recommended implementation plan with milestones and deliverables (10%) |
| 1. **After Sales Services**   (In Denmark and other countries of operations) | * Describe how the implementation partner will support the after sales process regarding support, consultancy, SLA’s etc. (10%) |
| **Total** | **100%** |

The five technically best scoring candidates will be invited to an interview to assess the candidates’ qualifications. The interviewers will be further evaluated against:

* Other platform capabilities and future possibilities
* Licensing & financials
* Organizational fit

## Confidentiality

All information presented, obtained, and produced is to be treated as DRC’s property and is considered as confidential for all other purposes than what is outlined in the Terms of Reference. The material prepared by the supplier cannot be sold, used, or reproduced in any manner (partially or in full) by the consultant without prior permission from DRC.

## How to apply

The deadline for submissions is **31.08.2022, 23:59 CEST= 22:59 GMT**. Please find the bid submission instructions in the RFP template.

## Additional Information

For additional information regarding these terms of reference or submission instructions, please send your questions to: Mobeen Arif at [mobeen.arif@drc.ngo](mailto:mobeen.arif@drc.ngo). **Any questions will only be answered in the period between August 9 – 26, 2022 due to summer holidays.**