European Union Network for the Implementation and Enforcement of Environmental Law

REQUEST FOR PROPOSAL
FOR IT COMPLIANCE AND SECURITY CHECK
INVITATION TO TENDER

The **European Union Network for the Implementation and Enforcement of Environmental Law (IMPEL)** is an international non-profit association of the environmental authorities of the European Union Member States, acceding and candidate countries of the EU, EEA and EFTA countries. The association is registered in Belgium and its legal seat is in Brussels. Currently, IMPEL has 58 members from 38 countries and its working language is English.

The Network's **objective** is to create the necessary impetus in the European Community to make progress on ensuring a more effective application of environmental legislation, by ensuring the consistent implementation and enforcement of environmental legislation across Europe. It promotes the exchange of information and experience and the development of environmental legislation. IMPEL has developed into a widely known organisation in the environment field and is mentioned in several EU legislative and policy documents. The Network functions as a collective association of environmental law enforcement authorities, dedicated to elevating the legal framework designed to safeguard our environment beyond a mere set of regulations.

The IMPEL network has seen a growing emphasis on dissemination of its information, best practices and project results exchange among expert colleagues, especially with the rise of virtual communication during the COVID-19 pandemic and in consideration of environmental factors. Many team and project meetings now occur virtually or in a hybrid format. Additionally, recent years have witnessed some IMPEL members experiencing significant cyberattacks, resulting in the loss of inspection data, prolonged downtime, and email correspondence loss. This has prompted heightened security measures and a more critical perspective on GDPR and IT security within the IMPEL network and its member authorities due to the increased electronic data exchange and associated security risks.

To support the secure ex-change of environmental enforcement authorities and increase the safety of these forms of communication, the IMPEL Board has decided to have an IT security check carried out by a competent external European provider. In order to protect the network and its member agencies, IMPEL wants to comprehensively assess relevant risks and take professional measures to mitigate the risks.

Current IT Structure

Our organization currently relies on multiple key IT components:

- Microsoft 365 (Outlook, Teams, Sharepoint) & Zoom: These platforms serve as the backbone of our communication and collaboration.

- Website: Our website is a vital digital presence that interacts with clients, partners, and stakeholder. The website contains and collects a wide range of sensitive data (from personal to classified) that runs on our managed server located in Germany. The system is based on PHP with Laravel as framework. It includes a newsletter and a member area with different tools that have access restrictions and right management.
- Basecamp: We use Basecamp as a project management and team collaboration tool to streamline our project workflows and enhance communication.
- Nemovote

Service specification

The Service required includes the following key services & deliverables:

1. Comprehensive IT security assessment, including vulnerability scanning.
    1) Data Encryption Assessment
    2) Incident Response Planning
    3) Security Policy and Procedure Review
    4) Security Architecture Review
2. GDPR compliance assessment.
3. Recommendations for improving IT security and GDPR compliance.
4. Recommendation of security measures and compliance practices, especially for regular security monitoring and reporting.
5. Optional Security Awareness Training for our IT and non-IT staff on security and compliance best practices.
6. Report results twice before the final report is approved through an online meeting with the IMPEL representatives

Essential Requirements & Skills

1. A proven track record in international IT security assessments and GDPR compliance audits.
2. A team of experienced professionals with relevant certifications (CISSP, CISM, CISA)
3. Knowledge of EU wide industry standards, GRPR laws, rules and regulations and best practices in IT security and GDPR compliance, including the ability to navigate evolving data protection laws.
4. The ability to tailor practical recommendations.
5. Optional training for our IT and non-IT staff.

Desirable & Goals

1. Obtain a valid security and GDPR compliance assessment for our organization.
2. Strengthen our IT security posture to protect against current and emerging threats.

3. Ensure that all IT processes and data handling procedures align with GDPR regulations.
4. Deliver actionable and tailored recommendations on specific issues found in the assessment. Prioritize them and put a focus on practicality.

Conditions

It is imperative that the selected service provider completes the project and submits all invoices by the end of December 2023, in accordance with the project timeline and our organizational needs.

Application

Proposals must be submitted by the 26th of October 2023.

Please include the following in your proposal:

- Company background and experience.
- Proposed methodology for IT security and GDPR compliance assessments.
- Detailed pricing structure.
- References from past clients.
- Any additional relevant information.

All proposals should be submitted in the English language to:

- info@impel.eu;
- johannes.ortler@impel.eu

Evaluation of proposals will be based on criteria including experience, expertise, proposed methodology, and cost.

Shortlisted service providers will be informed till October 30th.

Teleconference (TEAMs) interviews with those shortlisted will be conducted in the following days.

For more information on the tendered service, please contact Johannes Ortler at johannes.ortler@impel.eu.

04.10.2023