# ICMPD Job Profile

## Information Security & Data Protection Officer[1]

### Functional Overview

The Information Security & Data Protection Officer (IP2), under the guidance of the Head of Security & General Services / Resilience & Services, supports the implementation and day-to-day operation of ICMPD's information security governance and data protection framework. The role contributes to ensuring compliance with GDPR and internal policies by applying established procedures, providing technical and regulatory support, and coordinating with relevant internal stakeholders. The position serves as an operational focal point for data protection supporting alignment of business processes with ICT-security measures under established guidance and in close coordination with the ICT unit in charge of IT security.

As part of its functional scope, the role ensures the consistent application of ICMPD data protection and information security policies and procedures, and the accurate maintenance of related documentation, including data protection registers and records. The position provides timely operational support to Data Protection Impact Assessments (DPIAs), privacy notices, and data subject rights processes in line with established guidance.

The role contributes to increasing staff awareness of secure information handling and data protection obligations through the provision of practical guidance and support materials, and ensures effective coordination with IT, Legal, Human Resources, and operational units within the assigned scope of responsibilities.

### Key Results

**Data Protection Support:** The incumbent supports the implementation of ICMPD's data protection framework in line with GDPR and internal policies. This includes maintaining data processing records and providing structured support to Data Protection Impact Assessments (DPIAs) under guidance. The role also assists in the handling of data subject rights requests and ensures that related documentation is prepared and maintained accurately.

**Information Security Governance Support:** The position supports the application of non-technical information security policies, procedures, and standards across ICMPD. It contributes to the development of awareness materials and practical guidance to promote secure information handling and compliance with organisational requirements.

**Risk & Incident Support:** The incumbent supports the identification and documentation of information security and data protection risks within the assigned scope of work. Under supervision, the role assists in the

[1] This profile is classified at IP2.

coordination of responses to data breaches and information security incidents, including the preparation of records and follow-up actions.

**Coordination & Reporting:** The role coordinates with Legal, Human Resources, IT, and operational units on assigned information security and data protection tasks. It prepares inputs for reports, dashboards, and briefings to support monitoring, oversight, and decision-making.

## Required Expertise

- Capability to support the implementation of information security and data protection activities within an international organizational context, in line with established frameworks, policies, and procedures.
- Ability to apply GDPR and data protection principles in operational processes, including supporting documentation, assessments, and compliance-related tasks under guidance.
- Ability to analyze information security and data protection issues within defined parameters and contribute to the identification of appropriate solutions in coordination with relevant stakeholders.
- Capability to coordinate effectively with internal counterparts, including ICT, Legal, Human Resources, and operational units, to support the consistent application of information security and data protection requirements within the assigned scope of work.
- Strong organizational, drafting, and communication skills, including the ability to prepare clear documentation, guidance materials, and inputs for reporting and monitoring purposes.

## Qualifications, Experience and Language Skills

- Experience in international or multicultural environments is an asset.
- Master's degree in law, data protection, information security, IT governance, or a closely related field.
- Minimum of 3 years of experience in data protection, compliance, or information governance or relevant related field, at the international level.
- Good organisational, drafting and communication skills.
- Proficiency in (verbal/written) English, proficiency in the language of the duty station is an asset.
- Proficiency in the use of standard IT tools and ICT user skills.