

- Organise workshops and meetings to engage relevant stakeholders, including government officials, legal experts, private sector entities and civil society representatives.
- Facilitate discussions to gather input and feedback on the development of the integrated legislative framework, focusing on cybersecurity, and cybercrime and Personal Data Protection.

## 2. Legal and Policy Analysis:

- Conduct in-depth analysis of existing national legal and strategic frameworks related to cybersecurity and data protection, to ensure clarity, coherence, and legal soundness.
- Solicit feedback from legal experts, government officials, and relevant stakeholders to identify areas for refinement and revision in legislation and policies (current and in preparation).
- Research EU best practices and standards in cybersecurity and data protection to inform the development of the legislative framework.

## 3. Drafting Legislative Documents:

- Provide technical assistance and expertise to support the drafting of legislative documents, including bills, regulations, and policy guidelines and strategies, including in cybersecurity, cybercrime and in data protection.
- Collaborate with legal experts and government officials to ensure the alignment of proposed draft legislation with international standards and EU best practices.
- Incorporate feedback and recommendations from stakeholder consultations into the draft documents.

## **Activities relating to Output 2.4.:**

### 1. Capacity Building:

- Conduct training sessions and capacity-building workshops for government officials and relevant stakeholders on cybersecurity, data protection, and legislative drafting.
- Provide guidance on the interpretation and implementation of the proposed legislative framework.
- Empower stakeholders with the knowledge and skills necessary to support the adoption and enforcement of cybersecurity and data protection measures.

### 2. Awareness Raising Campaign:

- Develop and implement an awareness-raising campaign to inform the public about the importance of cybersecurity and data protection through CSOs and private sector organizations. These campaigns will use various communication channels, such as social media, workshops, and community events, and will aim to raise awareness and promote understanding of the legislative framework.

### 3. Training Needs Assessment:

- Conduct a comprehensive assessment of the digital skills and training needs of civil servants across government agencies.
- Identify gaps in knowledge and expertise related to digital tools, platforms, and technologies.
- Use the assessment findings to tailor training programs and initiatives to address specific skill gaps and requirements.

### 4. Design and Development of Training Programs:

- Develop targeted training programs and skill development initiatives focused on building digital literacy and competence aimed to foster training capacity within the public administration.
- Design training modules and materials covering topics such as digital tools and platforms, data management, cybersecurity awareness, and e-government practices.
- Customise training content to align with the diverse roles and responsibilities of civil servants across different departments and sectors.