

Terms of Reference

PREPARATION GRANT FOR LEBANON DIGITAL ACCELERATION PROJECT

(P181954)

Data Classification Policy

1 Background

Lebanon is facing a protracted, multidimensional crisis that has impaired state institutions and public service delivery. Weak digital foundations and enablers continue to undermine effective service provision and post-crisis recovery. For example, government data hosting remains fragmented, insecure, and unsustainable, while inadequate cybersecurity and data protection measures expose citizens' personal data to significant risks. The absence of a robust digital ID system and trusted data-sharing mechanisms further impedes secure and efficient digital service delivery. In addition, the lack of a whole-of-economy architecture limits coordination among stakeholders, and the policy, legal, regulatory, and institutional frameworks for digital transformation remain underdeveloped.

To address these issues, the Lebanon Digital Acceleration Project (the "Project"), supported by the World Bank, will establish secure, scalable, and resilient digital infrastructure including cloud services, data platforms, and cybersecurity systems that are essential for attracting investment and fostering innovation. By strengthening digital ID, e-signature capabilities, and the legal framework for digital transactions, the Project will improve the ease of doing business and enable trusted, efficient engagement between the public and private sectors. In parallel, the Project will advance key regulatory reforms in telecom, data protection, e-signature, and artificial intelligence (AI), while investing in Lebanon's digital talent pool. Together, these measures will lay the foundation for a more competitive, dynamic, and inclusive economy.

The World Bank's Grant Facility for Project Preparation (GFPP) has been extended to OMSAR to support Project readiness. The GFPP grant is implemented by a Technical Unit (TU) housed within OMSAR.

In an era where data plays a central role in economic growth, innovation, and governance, the Government of Lebanon recognizes the urgent need to establish a robust Data Classification Policy Framework. Currently, Lebanon lacks a standardized framework for classifying, handling, and protecting data leading to inefficiencies, regulatory uncertainty, and heightened security risks.

Global trends show a surge in digital regulations aimed at promoting trust, safeguarding data, and enabling digital transformation. Countries with advanced data classification policies such as the UK, UAE, and Saudi Arabia demonstrate higher digital competitiveness and economic resilience.

Lebanon's policy aims to close existing legal and regulatory gaps and align with internationally recognized best practices and guidance issued by established international standard-setting bodies including the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), National Institute of Standards and Technology (NIST), Organisation for Economic Co-operation and Development (OECD), and the European Union (EU), to ensure secure, interoperable, and trusted data governance across public and private sectors.

2 Assignment and Objectives

This assignment aims to design and develop a comprehensive National Data Classification Policy Framework for Lebanon that provides a structured foundation for data classification and data handling requirements. The consultant undertaking the assignment (the Consultant) will lead a comprehensive policy framework development engagement, including the assessment of the current legal, institutional, and operational context, the development of a national Data Classification Policy for submission to the Council of Ministers (CoM), and the preparation of supporting technical frameworks, roles and responsibility structures, and guidance materials to enable future implementation by public sector entities, and shall be undertaken in alignment with and without prejudice to the applicable national institutional mandates governing digital transformation and data governance.

Core Objectives

- Assess Lebanon's current data governance and classification landscape;
- Benchmark leading national and international good practices;
- Conduct targeted technical consultations with relevant government counterparts and other selected stakeholders to inform and validate policy design; and
- Develop a tailored data classification policy framework with clear implementation guidance.

3 Detailed Scope of Work and Deliverables

Phase 1: Inception and Methodological Alignment

Activities under this phase shall be conducted in alignment with and without prejudice to the applicable national institutional mandates governing digital transformation and data governance.

- Confirm a shared understanding of the project background, objectives, scope, and boundaries in line with these Terms of Reference;
- Define and agree on the methodological approach to be applied across the assignment, including how the current state and international benchmarks will be assessed, how policy design will be structured, and detail the technical frameworks, templates, procedures, and other relevant policy artifacts that will constitute the policy framework;
- Confirm the high-level design principles that will guide the assignment, including a risk-based perspective, consideration of the full data lifecycle, and attention to potential impacts related to confidentiality, integrity, availability, privacy, and societal risk; and
- Present a detailed work plan and timeline, including sequencing of activities, deliverables, expected interactions with stakeholders, and alignment of deliverables with the agreed scope.

Deliverable D1: *Inception Report*

Phase 2: Current State and Benchmark Assessment

Activities under this phase shall be conducted in alignment with and without prejudice to the applicable national institutional mandates governing digital transformation and data governance.

- Review the national digital transformation strategy, existing laws, regulations, and institutional mandates relevant to data classification and handling decisions;
- Evaluate current data classification landscape including a baseline maturity assessment of current data governance and classification practices across a representative sample of selected ministries and public sector entities, including institutional capacity, existing governance roles, SOPs, as well as an overview of representative data types, datasets, metadata, storage and processing environments, and key data flows across the data lifecycle; and
- Use international benchmarks and best practices as design references to inform the identified gaps and the design requirements for the data classification policy framework, including all relevant policy, technical, and procedural artifacts needed for its effective operationalization.

Deliverable D2: *Data Classification Baseline Report*

Phase 3: Policy Drafting

Activities under this phase shall be conducted in alignment with and without prejudice to the applicable national institutional mandates governing digital transformation and data governance.

- Develop a comprehensive Policy Canvas outlining objectives, scope, boundaries, assumptions, risks, and high-level guidance on implementation;
- Articulate core policy principles guiding data classification and use, including a risk-based approach, proportionality, lifecycle awareness, and alignment with privacy, cybersecurity, transparency, interoperability, AI readiness, and broader public-interest considerations;
- Establish policy-level governance, oversight, and accountability principles, clarifying institutional responsibility for public sector data and setting the basis for future designation of accountability and stewardship roles;
- Define the national data classification levels and their definitions, describing the intent, sensitivity, and protection rationale associated with each level, following international good practices;
- Develop the draft Policy and ensure consistency with regional and international benchmarked frameworks while being fully adapted to Lebanon's legal, institutional, and capacity realities; and
- Engage with relevant ministries and technical departments to review, refine, and validate the draft policy.

Deliverable D3: *Draft Data Classification Policy*

Phase 4: Roles, Technical Classification Framework, and Control Matrix (Implementation-enabling)

- Define detailed institutional roles and responsibilities supporting data classification and handling, clarifying operational accountabilities for data stewardship, custody, classification focal points, and oversight functions;
- Develop the technical data classification framework, specifying classification criteria, decision logic, and impact considerations (e.g. confidentiality, integrity, availability, privacy, and societal impact) to guide consistent classification decisions;
- Define data handling expectations by classification level, covering access, storage, transmission, retention, and disposal at a framework level, without system configuration or enforcement;
- Develop a roles and control responsibility matrix, mapping classification levels to minimum control expectations informed by internationally recognized standards (e.g.

ISO/IEC 27002 and relevant NIST guidance), as reference benchmarks rather than compliance requirements; and

- Ensure coherence between the policy and technical framework, confirming that all framework elements directly operationalize the intent and principles set out in the approved policy.

Deliverable D4: *Technical Data Classification Framework and Control Matrix*

Phase 5: Guidance Templates and Procedural Framework

- Develop standardized guidance and templates to support ministries and public entities in applying the Data Classification Policy and technical framework to their own datasets in a consistent and documented manner;
- Design practical classification templates and reference tools, enabling entities to identify datasets, assess sensitivity using the agreed classification criteria, document classification decisions, and record justifications in line with the policy and framework;
- Develop procedural guidance for data classification and reclassification, outlining high-level steps for initial classification, periodic review, and updates over time, without prescribing system-level workflows or tools;
- Define procedures for managing exceptions and deviations, including documentation requirements, approval principles, and oversight considerations, to ensure controlled and transparent handling of non-standard cases;
- Define high-level appeals and escalation mechanisms, providing structured guidance for addressing disagreements or disputes related to classification decisions while maintaining institutional accountability and traceability;
- Develop any other technical, procedural, or operational artifacts needed to ensure effective implementation of the data classification policy framework by line ministries and other public sector entities;
- Ensure alignment between templates, procedures, and the approved policy and technical framework; and
- Validate the Guidance Templates and Procedural Framework and their applicability through relevant stakeholder consultations.

Deliverable D5: *Data Classification Guidance Templates and Procedural Framework*

Phase 6: Final Consultation and Policy Finalization

- Conduct one or more structured consultation sessions with a broader group of relevant stakeholders to validate policy and gather high-level feedback for implementation considerations;
- Document key comments and observations received during the consultation session(s); and
- Prepare the final version for submission to the CoM.

Deliverables D6:

- Final Data Classification Policy Framework
- Summary Consultation and Feedback Note

4 Qualifications

The Consultant must meet the following minimum qualifications:

Education

- Advanced university degree (Master’s or equivalent) in Law, Public Policy, Computer Science, Data Science, Information Management, Information Security, or other equivalent qualification.

Core Professional Experience

- Years of Experience: At least 10 years of professional work in data protection, data governance, data classification, or other field directly relevant to the assignment.
- Policy Drafting: Proven track record of drafting national or institutional regulatory frameworks related to data classification.
- Institutional Assessment: Demonstrated experience assessing legal and institutional mandates related to cybersecurity or digital government in fragile or emerging market contexts.
- Consultation Leadership: Minimum of 7-10 years of experience organizing and leading high-level multi-stakeholder consultations (e.g., with Ministers, political parties, and donors).

Technical Knowledge & Certifications

- International Standards: Profound knowledge of ISO/IEC 27001, 27002, 27701; NIST SP 800-53 and 800-60; and OECD data governance guidelines.

- Regulatory Familiarity: Deep understanding of EU GDPR principles and their adaptation into national laws (specifically the Lebanese Law 81/2018 on Electronic Transactions and Personal Data).
- Certifications (Desirable): CIPP (Certified Information Privacy Professional), CDPSE (Certified Data Privacy Solutions Engineer), or CISM (Certified Information Security Manager).

Language & Behavioural Competencies

- Language: Fluency in Arabic and English (both oral and written) is essential for high-level ministerial consultations and drafting policy for the Council of Ministers.
- Stakeholder Management: Exceptional interpersonal skills to navigate sensitive political environments and achieve consensus among fragmented government entities.

5 Compliance Requirements

The selected Consultant must adhere to all applicable World Bank regulations and guidelines, including but not limited to the *World Bank's Guidelines on Preventing and Combating Fraud and Corruption in Projects Financed by IBRD Loans and IDA Credits and Grants*, and must disclose any actual or potential Conflict of Interest (COI).

In addition, the Consultant must comply with the following Environmental and Social (E&S) requirements aligned with the World Bank Environmental and Social Framework (ESF) and the Lebanon Digital Acceleration Project (LDAP) commitments:

1- Code of Conduct (CoC)

The Consultant must sign and follow a CoC covering data confidentiality, respectful conduct, non-discrimination, and zero tolerance for SEA/SH.

2- Labor and Working Conditions

The Consultant shall perform the assignment in accordance with applicable labor and working condition requirements under the World Bank Environmental and Social Framework (ESS2), including maintaining safe and healthy working practices, professional conduct, and respect for applicable occupational health and safety standards.

The Consultant shall have access to the Project's Grievance Mechanism for raising any work-related concerns or complaints arising during the assignment.

3- Data Security, Privacy, and Cybersecurity

All data handled under this assignment must be securely stored, accessed only by authorized staff, and managed using privacy-by-design and cybersecurity best practices. Any data breach must be immediately reported.

4- Stakeholder Engagement and Grievance Redress

Any targeted technical consultations conducted as part of policy development shall inform participants about the Project’s Grievance Mechanism and how complaints can be submitted.

5- SEA/SH Prevention

The Consultant shall comply with zero-tolerance requirements for SEA/SH and adhere to appropriate professional conduct and reporting procedures when engaging with stakeholders, in line with the Project’s CoC and World Bank requirements.

6- Environmental Considerations for ICT (ESS3)

Any ICT equipment or data storage devices used must be managed responsibly, including secure data wiping and environmentally sound disposal.

6 Deliverables and Payment Schedule

The engagement will be completed in approximately **20 weeks from contract signature date**, with key phases and deliverables structured as follows:

#	Phase	Deliverable	Week of Delivery (from contract signature)	Payment (% of Total)
1	Inception and Methodological Alignment	D1 – Inception Report	4	15%
2	Current State and Benchmark Assessment	D2 – Data Classification Baseline Report	7	15%
3	Policy Drafting	D3 – Draft Data Classification Policy	10	15%
4	Roles, Technical Classification Framework, and Control Matrix (Implementation-enabling)	D4 – Technical Data Classification Framework and Control Matrix	14	20%

5	Guidance Templates and Procedural Framework	D5 – Data Classification Guidance Templates and Procedural Framework	18	20%
6	Final Consultation and Policy Finalization	D6 – Final Data Classification Policy Framework and Summary Consultation and Feedback Note	20	15%
	Total			100%

7 Reporting, Deliverables, and Contract Management

Project Oversight and Management Structure

A Technical Committee (TC) will be established to provide strategic direction, oversight, and effective management of the engagement. Chaired by the Grant Coordinator and composed of members from OMSAR, OMSTAI, and other involved ministries, as applicable, the TC serves as the primary governing body responsible for reviewing the Consultant’s progress and ensuring alignment with national digital transformation goals and applicable institutional mandates.

Reporting Obligations

The Consultant will report directly to the Grant Coordinator. In addition to the contractual deliverables, the Consultant, and upon request, shall participate in progress meetings with the TC team to ensure methodological alignment.

The TC Approval Gate and Deliverable Acceptance

The TC is the sole authority empowered to formally accept and approve project deliverables. The following administrative process applies to every milestone:

- **Submission:** All deliverables listed in the TOR are subject to formal review. The Consultant shall submit each deliverable to the TC Chairperson.
- **Validation:** Payment cannot be processed without written validation or sign-off from the TC.
- **Formal Acceptance:** A "Certificate of Acceptance" or formal written notice signed by the TC Chairperson is a mandatory prerequisite for the release of payment.

Administrative Requirements for Payment Clearance:

- **Certificate of Delivery:** For each milestone, the Consultant must submit a Certificate of Delivery of Services to the Grant Coordinator for TC validation.
- **Invoice Package:** A complete package containing the Official Invoice and evidence of delivery is required to initiate TC validation and issuance of the formal "Certificate of Acceptance" for payment processing.

Currency of Payment

Payments will be processed in U.S. Dollars.

Intellectual Property Rights

All documents, data, analyses, policy drafts, tools, and materials produced under this assignment shall become the exclusive property of Government of Lebanon. The Consultant shall not publish, use, or share any materials without prior written approval from the Government of Lebanon.

Confidentiality Obligation

The Consultant shall maintain strict confidentiality of all information accessed during the assignment and shall ensure that no information is shared, disclosed, or used outside the scope of this contract.

8. Technical Proposal

The consultant shall submit a technical proposal including:

- A curriculum vitae (CV) demonstrating the required qualifications and relevant experience; and
- A brief Methodology and Work Plan (not exceeding 5 pages) outlining the proposed technical approach and logical sequencing of activities to fulfil the 6-phase scope of work.