POWER OVER CODE

Digital Public Law Standard

Institute for Digital Society & Future Public Law

Consultation Draft v1.0 — 28 September 2026

Status of this document

Stage. Consultation draft, version 1.0, dated 28 September 2026. Register entry: to be assigned when the consultation opens.

Issuing body. Issued by the EPLO Institute for Digital Society and Future Public Law.

Legal effect. The Standard is soft law. It is not legally binding unless a competent authority gives it effect through its own instrument.

Consultation. Public consultation of at least sixty (60) days. Comments are invited from public institutions, oversight bodies, courts and ombuds institutions, researchers, civil society and suppliers. Comments are submitted under the author's name and are published with it; anonymous and confidential comments are not accepted.

DRAFT

Introduction

Public authority is now routinely exercised through digital systems: scoring models that select whom an agency investigates, wallets that gate access to cross-border services, and data platforms that shape how hospitals allocate capacity. Sectoral law reviews each system in fragments. Data-protection law asks whether personal data are lawfully processed, AI law asks whether a model meets its risk-based requirements, and cybersecurity law asks whether incidents are managed and reported. No sectoral regime asks the composite question this Standard addresses: does the responsible public institution retain the lawful and practical capacity to understand, direct, inspect, correct and, where necessary, terminate the digital arrangement through which it exercises public authority?

The state does not retain power over code because it owns a contract, a policy or a platform. It retains power over code only where lawful public authority remains demonstrably capable of understanding, directing, inspecting, correcting, remedying, sustaining and, where necessary, exiting the technical and socio-technical arrangements through which a public function is performed. Power over code is demonstrated, not declared.

The Standard is organised in four Parts. Part I (Normative Core) states the core requirement, the eleven principles, the ten retained capabilities and the foundational tests and concepts. Part II (Method) states the Digital Public Law Impact Assessment, the Standard's authoritative method for testing whether the Normative Core is met in each public function. Part III (Application) states how the Standard is used: the modes of use, the Digital Public Function Record, the three Review Levels and their statements of findings, the forms in which a competent authority may give the Standard effect, and its relationship to other instruments. Part IV (Stewardship and Soft-Law Implementation) explains how the Standard is consulted on, adopted, amended, and implemented.

DRAFT

Part I — Normative Core

I.1 Purpose and nature

I.1.1 The Power over Code: Digital Public Law Standard ("the Standard") states the minimum conditions that must remain satisfied whenever a public function is performed, mediated, constrained, prioritised or materially shaped through digital systems.

I.1.2 The Standard is a legal standard: a coherent body of normative requirements, together with an authoritative method for applying them, intended to secure uniform application across institutions and jurisdictions. It draws its content from the constitutional, administrative, human-rights and sectoral law that already governs public authority. It does not create new substantive rights or displace the applicable law, which determines the content and enforceability of each requirement in each jurisdiction.

I.1.3 The Standard applies to digitally mediated public functions that satisfy the Functional Scope Test (I.8.1), whether the function is performed by a public body or by a private actor acting on its behalf.

I.2 Normative language

I.2.1 **"Must"** identifies either a methodological prerequisite for a defensible conclusion under the Standard or an obligation established by applicable law. Every Digital Public Function Record identifies which ground applies. The absence of a "must" requirement blocks the relevant decision category.

I.2.2 **"Should"** expresses a strong expectation of the Standard, from which an institution may depart only with a recorded, reasoned justification.

I.2.3 **"May"** expresses a permitted option.

I.2.4 A methodological failure under the Standard is not in itself a judicial finding of illegality. Equally, a decision not to apply the Standard does not remove any existing legal duty of an institution.

I.3 Definitions

I.3.1 **Digital Public Law** is the field of law concerned with the legal constitution, exercise, mediation and control of public authority in digitally dependent environments.

I.3.2 **Code** means the technically formalised and operationally effective arrangements through which a digital system performs, mediates, constrains, prioritises or otherwise materially shapes a public function. It includes software source code and executable code; algorithms, computational rules, decision models and artificial-intelligence models; system configurations, thresholds, weights, parameters and default settings; data models, schemas, classifications and training, testing, reference or operational datasets; workflow engines, automated decision rules and escalation rules; application programming interfaces and interoperability and data-exchange mechanisms; identity, authentication, authorisation, credential and access-control mechanisms; logging, monitoring, ranking, filtering, matching, recommendation and notification systems; platform architecture, cloud configurations and embedded security controls; technical specifications, procurement requirements, licence conditions and vendor-controlled system

DRAFT

functions; and human–machine interaction protocols where those protocols structure, limit, channel or direct the exercise of public authority.

I.3.3 Law, policy, administrative instructions, contracts and human discretion are not themselves code merely because they are written or formalised. They fall within the definition only to the extent that they are translated into, embedded in, or made operational through a digital system.

I.3.4 Power over code means the legally grounded and institutionally effective capacity of public authorities to understand, direct, constrain, inspect, test, challenge, correct, override, suspend, replace and, where necessary, terminate the technical systems through which public functions are exercised. It requires the responsible institution to retain legal responsibility for the function; sufficient institutional knowledge and technical competence; access to relevant evidence, records, data, models, configurations, logs and audit information; effective control over material system changes; the capacity to give notice, explanations, review, contestation, correction and remedies; operational continuity where a supplier, platform, model or infrastructure component fails or becomes unavailable; and the authority and practical capability to intervene where the system produces unlawful, constitutionally defective, unsafe, discriminatory, unreliable or institutionally unacceptable outcomes.

I.3.5 Power over code does not require a public institution to own or directly develop its own software. Outsourcing, procurement, licensing, cloud dependence, proprietary systems and private-sector participation are compatible with power over code, provided they do not deprive the responsible institution of the practical capacity to discharge its legal duties.

I.3.6 Digital Public Law Impact Assessment (DPLIA) is the Standard's authoritative method, stated in Part II, for identifying, analysing, deciding upon, documenting and reviewing the public-law implications of a digitally mediated public function. DPLIA is part of the Standard, not a separate instrument.

I.3.7 Digital Public Function Record ("the Record") is the single authoritative documentary carrier of an assessment under the Standard (III.2).

I.3.8 Responsible institution means the public institution legally responsible for the public function under assessment.

I.3.9 Competent authority means a public body with legal power to give the Standard effect within its sphere of competence; and **adopting instrument** means the instrument through which it does so (III.5).

I.3.10 Statement of findings against the Standard means the output of an assessment at any Review Level (III.4). It is not a certificate, a conformity mark or a declaration of legality.

I.4 The core requirement

> **Core requirement**
>
> Any institution legally responsible for a digitally mediated public function shall retain the authority, knowledge, access, evidence, capacity, and practical means necessary to understand, direct, constrain, inspect, contest, correct, override, suspend, replace, and, where required, terminate the technical and socio-technical arrangements through which that function is performed.

DRAFT

I.4.1 The core requirement is tested through the ten retained capabilities (I.6) and the Six Gates (II.3). Ownership clauses and policy statements are relevant but are not proof. The question in every case is whether rights, access, authority, evidence and operational capacities exist, are assigned, are usable, and have been tested under realistic conditions.

I.5 Principles

The following eleven principles state the minimum conditions for the lawful, constitutionally continuous, institutionally responsible and resilient digital mediation of public functions.

Principle 1. Public-function identification. Every digitally mediated activity must be assessed according to its function and practical effects, rather than its institutional label, contractual form, ownership model or technological description.

Principle 2. Legal authority and constitutional continuity. Digital transformation must not interrupt the continuing application of legality, competence, procedural fairness, equality, proportionality, reason-giving, accountability, judicial protection and effective remedy.

Principle 3. Non-delegable public responsibility. The responsible public institution must retain legal and institutional responsibility for the public function, including where technical development, operation, infrastructure, data processing or decision support is supplied by a private actor.

Principle 4. Institutional power over code. The responsible institution must retain sufficient legal authority, technical access, knowledge, contractual rights, organisational capacity and operational capability to understand, supervise, test, correct, override, suspend, replace or terminate the relevant system. Evidence of that capacity is organised under the four proof domains (I.7).

Principle 5. Traceability and evidential integrity. The system must generate and preserve adequate evidence of its legal basis, design assumptions, data sources, operational rules, material changes, decisions, interventions, errors and outcomes.

Principle 6. Contestability and remedy. Affected persons must have access to meaningful notice, explanation, review, correction, challenge and remedy appropriate to the nature and consequences of the digitally mediated public function.

Principle 7. Governance across all six layers. Compliance with the applicable law cannot be established solely by examining the algorithm or technical component. Assess the legal, institutional, technical, data, operational, and societal layers together.

Principle 8. Control of private actors and dependencies. Contracts, licences, procurement arrangements, intellectual-property restrictions, cloud dependencies, platform rules and proprietary systems must not prevent the public authority from fulfilling its legal duties or exercising effective control.

Principle 9. Security, resilience and continuity. The digital system must be designed and governed to preserve the continuity, integrity, availability, recoverability and lawful operation of the public function under foreseeable disruption, failure, attack, supplier withdrawal or technological change.

DRAFT

Principle 10. Lifecycle assurance. Assessment must continue after deployment. Material changes to law, purpose, data, models, system configuration, suppliers, infrastructure, risk or institutional capacity must trigger proportionate reassessment.

Principle 11. Integrated institutional judgement. The final decision must not be reduced to a technical score or an automated compliance result. The responsible institution must adopt and record a reasoned public-law judgement based on the Six Gates, the six-layer analysis, the causal synthesis, evidence confidence, residual risks and the conditions of continued operation.

I.6 The ten retained capabilities

I.6.1 The core requirement is given operational content by ten retained capabilities. In canonical order, they are: Understand → Direct → Document → Audit → Explain → Correct → Intervene → Preserve evidence → Continue → Exit.

I.6.2 The capabilities are cumulative, not optional. Strength in one cannot compensate for the absence of another capability necessary to discharge the function's legal obligations, and all ten are considered together.

I.6.3 Source-code ownership is not the determining factor. Depending on the function's constitutional significance and the nature of any private dependency, source-code access may be essential, helpful without being essential, or unnecessary. The question is functional rather than proprietary.

I.6.4 The depth of each capability required scales with the constitutional significance of the function, the severity and reversibility of potential effects, the degree of private dependence, and the difficulty an affected person would face in obtaining evidence of what occurred. The Standard is not strict liability for every system failure and does not require every public authority to maintain an in-house software-engineering capability.

No.	Capability	Required institutional ability	Illustrative evidence	Proof domain
1	Understand	Describe how the arrangement materially affects the function, its operational limits and its known failure modes.	Function map; architecture description; limitations analysis; staff competence record; independent technical explanation.	Know
2	Direct	Control the lawful purposes, governing policy, operative thresholds, affected population and any material change to these.	Decision-rights record; change approval; enforceable supplier change-control terms; approval log.	Govern
3	Document	Reconstruct relevant data, rules, versions, interventions and the pathway by which any decision was reached.	Data lineage; configuration and version history; administrative and technical records.	Know

No.	Capability	Required institutional ability	Illustrative evidence	Proof domain
4	Audit	Enable qualified, appropriately independent scrutiny of performance, logs, controls and supplier-held evidence. Exercise the audit right, not merely hold it.	Exercisable access rights; completed audits; test results; access records.	Answer
5	Explain	Provide intelligible, case-specific reasons sufficient for the affected person to understand a decision and, where appropriate, challenge it.	Explanation tests with users; reasoned decisions; reason templates; disclosure procedures.	Know
6	Correct	Identify and correct errors in data, logic and outcomes, and propagate the correction to every decision the error affected.	Correction and propagation tests; affected-case identification; reopening records.	Answer
7	Intervene	Override, restrict, suspend or safely roll back operation through authorised action.	Tested intervention procedures; trained officials; escalation authority and logs.	Govern
8	Preserve evidence	Keep evidence usable for complaints, review, litigation, inquiry and learning under lawful retention rules.	Retention schedule; legal hold; protected logs; access controls.	Answer
9	Continue	Meet essential legal obligations during an outage, attack or supplier failure.	Tested fallback; alternative channel; recovery exercises; continuity resources.	Sustain
10	Exit	Migrate, replace or terminate a system or supplier while preserving the underlying legal duty.	Costed transition; portability tests; assistance rights; preservation of pending claims; completed exit drill.	Sustain

Table I.1. The ten retained capabilities in canonical order, with the proof domain to which each belongs.

I.6.5 Records must be adequate for reconstruction and remedy while respecting lawful data minimisation, confidentiality and retention limits. Correction must identify every affected decision and provide a lawful route to address it, recording any limits on reopening and their consequences.

I.7 The four proof domains

I.7.1 The four proof domains group the ten capabilities by the kind of evidence each needs. They are an organising aid for evidence, not a second scored set, and they do not alter the canonical order of the capabilities.

Proof domain	Capabilities	Question	Typical evidence
Know	Understand · Document · Explain	Can the institution describe how the function works, where it is limited, and why a given outcome occurred?	Architecture, data lineage, dependency map, staff capability evidence, case-level reasons.
Govern	Direct · Intervene	Can the institution direct material choices and changes and interrupt operation?	Contract and access rights, change-control records, exercised (not merely held) intervention rights.
Answer	Audit · Correct · Preserve evidence	Can the institution submit to scrutiny, correct errors and preserve evidence for review?	Completed audits, correction and propagation records, retention and legal-hold records.
Sustain	Continue · Exit	Can the institution continue its legal duties and exit a dependency?	Exercise results, independent tests, incident response, exit drills.

Table I.2. The four proof domains.

I.8 Foundational tests and concepts

I.8.1 Functional Scope Test

I.8.1.1 The Standard applies where three cumulative conditions are satisfied: (a) public authority is exercised — the matter concerns the exercise, organisation, review or continuity of a constitutionally relevant public function, whether performed directly by a public body or by a private actor acting on its behalf; (b) a digital system materially influences that exercise, shaping its substance, process or outcome in a way that would be different absent the system; and (c) that influence has constitutional significance, affecting legality, accountability, rights, democratic governance or institutional resilience.

I.8.1.2 Material influence may operate through recommendations, defaults, authoritative registries or cumulative service-routing effects. The inquiry concerns actual operation, not the label a system carries: a tool described as decision support may determine outcomes with only nominal human involvement.

I.8.1.3 Failure of any condition places the matter outside the Standard's scope. Routine digital convenience without material public-law significance falls outside scope; a small system can nevertheless qualify where it affects rights or review. Uncertainty does not prove that a function is outside scope: an uncertain boundary requires evidence and a recorded provisional assessment, and the boundary is reopened when the function or its dependencies materially change.

I.8.2 Private Actor Test

I.8.2.1 Where a private actor participates in a function that satisfies the Functional Scope Test, the Private Actor Test asks whether that participation triggers non-delegable public responsibility and enhanced controls. Its limbs are: (a) functional substitution — the actor performs a task the public institution would otherwise have to perform; (b) practical indispensability — assessed through documentation, audit rights, control over change, evidentiary retention and exit capacity; and (c) accountability displacement — ordinary public-law accountability (reasons, review, remedy) cannot reach the actor directly.

I.8.2.2 Where all limbs are satisfied, the actor's conduct is subject to the same rigour as a wholly public body performing the identical function, and enhanced controls are required; a serious individual dependency may justify targeted safeguards. The test identifies governance needs. State attribution, direct supplier liability and amenability to judicial review remain questions of applicable law.

I.8.2.3 The Functional Scope Test and the Private Actor Test answer different questions in sequence and are not merged: the first identifies the public-law matter; the second determines whether a specific private participant within it attracts public-law obligations.

I.8.3 Six-Layer Governance Architecture

Layer	Core question
1. Constitutional and legal-regulatory	What authority, rights, duties and sectoral rules constitute the function, and does the mandate satisfy legality and proportionality?
2. Institutional responsibility	Who owns, funds, operates, supervises and changes the function, and is that responsibility traceable across delegation and supplier relationships?
3. Data and infrastructure	What registries, models, interfaces, cloud services, interoperability arrangements and security architecture does the function depend upon?
4. Decision and service delivery	How is the function performed at the point of decision—through algorithms, automation, or a discretion structure?
5. Accountability and oversight	Do reasons, audit, complaint, appeal and judicial review reach the records the decision layer produced?
6. Resilience and continuity	What happens to the function during an outage, supplier withdrawal, attack, crisis, or transition?

Table I.3. The Six-Layer Governance Architecture.

I.8.3.1 The layers are analytically distinct but institutionally interdependent. A defect at one layer typically surfaces at another: an untraceable responsibility (Layer 2) appears when accountability is tested (Layer 5); an unexamined dependency (Layer 3) becomes a continuity crisis at renewal (Layer 6). The architecture is a causal map, not a seventh Gate or a parallel checklist.

I.8.4 Constitutional infrastructure

I.8.4.1 Constitutional infrastructure means digital systems — identity systems, registries, cloud arrangements, interoperability layers — that have become part of the institutional foundations through which persons exercise rights and public bodies perform constitutional functions, so that their failure interrupts constitutional life rather than causing mere operational inconvenience. Infrastructure is constitutionally critical where failure or loss of control would disable essential rights or the lawful operation of government.

I.8.5 Non-delegable public responsibility

I.8.5.1 A public authority may delegate a task without delegating the answerability attached to it: answerability cannot be handed over with the task itself. Technical outsourcing cannot leave an affected person without

an answerable institution or a usable route to correction. "The supplier is responsible" is not a lawful substitute for institutional answerability.

DRAFT

Part II — Method: Digital Public Law Impact Assessment

II.1 Nature of the method

II.1.1 The Standard states what must remain true; DPLIA is the Standard's authoritative method for testing whether it is true in a given public function. DPLIA does not replace specialised legal, technical, risk or rights assessments where those remain legally required. It reads their outputs together, as evidence, against the Normative Core.

II.1.2 The method must be able to reach a favourable conclusion when the evidence supports it. Its value lies in the quality of reasons, decisions and safeguards, not in the number of adverse findings or the volume of documentation produced.

II.1.3 Gates are findings, not scores. No aggregate score is computed, and legality cannot be established by adding favourable capability ratings or by balancing an unlawful design against expected efficiency.

II.2 The six steps

II.2.1 DPLIA proceeds in six steps. The step numbers organise work; they do not permit a Gate to be finally passed before the evidence it depends on has been tested. Evidence gathered in a later step may change any earlier finding, and a material change may return the assessment to Step 1. Early findings are provisional where they depend on evidence gathered later; the Institutional Decision requires them to be reconciled.

Step	Name	Work	Output in the Record
1	Scope	Open the Record at policy conception, procurement, renewal, material change or incident; identify the owner, intended outcome and decision point; apply the Functional Scope Test; fix the Review Level (III.3).	Screening conclusion; owner; boundary; Review Level; reconsideration trigger.
2	Function Map	Define the function's boundary and dependencies; map the six layers; apply the Private Actor Test; identify affected persons; index imported specialist evidence.	Function Map; dependency and evidence index; affected-person analysis.
3	Six Gates	Test the function against each Gate and rate the ten capabilities, recording evidence source and confidence for each finding.	Gate findings with sub-findings; capability ratings.
4	Causal Synthesis	Read Gate, capability and layer findings together as causal chains; state risk, evidence confidence and implementation integrity separately.	Causal synthesis; residual risks; dissent.
5	Institutional Decision	Adopt a reasoned decision in one of eight categories with conditions, owners, deadlines and consequences.	Signed decision; conditions register; statement of findings.

Step	Name	Work	Output in the Record
6	Lifecycle Review	Monitor operation, notice and redress; reassess on schedule or material change; manage transition or exit.	Review calendar; trigger log; updated findings.

Table II.1. The six DPLIA steps.

Step 1 — Scope

II.2.2 Assessment opens when a function is conceived, procured, renewed, materially changed or implicated in an incident. The responsible institution opens the Record, names the accountable owner and records the intended public outcome and the decision the assessment will inform. It applies the Functional Scope Test (I.8.1) once, before any Gate is assessed; the test is not itself a Gate.

II.2.3 A function found outside scope receives a reasoned screening record naming the owner and a reconsideration trigger. Ordinary legal and administrative obligations continue to apply. For a function within scope, the institution fixes the Review Level under III.3 and records the reasons.

Step 2 — Function Map

II.2.4 The Function Map defines the boundary and dependencies of the function: the actors, data, systems, suppliers, remedies and fallback arrangements it relies upon. It maps the function across the six layers (I.8.3), applies the Private Actor Test (I.8.2) to each material private participant, and identifies affected persons, their vulnerabilities and the interests engaged.

II.2.5 Specialist evidence — a data-protection impact assessment, a fundamental-rights impact assessment, a security test — is indexed by reference, stating its source, version, custodian, legal scope and verification status. A completed specialist report is evidence to appraise, not an authoritative answer on every issue within its subject area. The relevant question is what it establishes about this function and what remains unresolved at the interfaces.

Step 3 — The Six Gates

II.2.6 The Six Public Law Gates ("Six Gates") translate the function's applicable legal and constitutional requirements into explicit findings. Each Gate states a controlling question, the matters it includes, and a blocking rule. A full assessment addresses all six Gates; any sub-question treated as inapplicable requires a recorded reason.

Gate	Controlling question	Includes	Blocking rule
1. Lawful Mandate	Does the institution have specific legal competence and a legitimate public aim for this function?	Competence and jurisdiction; specificity of authority; public purpose and affected population; purpose limitation; consistency between the encoded rule and the legal rule.	The function must not proceed without an identifiable, current and sufficiently specific legal basis for its purpose and population.

DRAFT

Gate	Controlling question	Includes	Blocking rule
2. Rights-Justified Design	Is the design necessary, proportionate, non-discriminatory and accessible, given the available alternatives?	Problem evidence and alternatives; less intrusive means; benefits, burdens and reversibility; group and distributional effects; accessibility; vulnerability.	A design must not proceed where a less intrusive means achieves the same aim, or where group effects are unassessed for a function at Review Level 2 or 3. Reporting cannot remedy unlawful discrimination or disproportionate interference.
3. Public Responsibility	Is one public institution, with a named decision owner, identifiable and answerable for the function?	Lawful allocation of responsibility across public, private and distributed actors; delegation, procurement and data-use arrangements; escalation routes.	The function must have a named public decision owner before committing to procurement.
4. Operational Control	Can the institution lawfully and effectively govern the data, code, suppliers, changes and interventions that materially shape the function?	Lawful data access and correction; contract control over material dependencies; change control, versioning, log access and independent testing; ability to audit, correct, restrict and redirect.	For rights-significant functions, inability to audit, intervene in or correct a material effect must block deployment until control is demonstrated. A contractual promise never exercised is not sufficient on its own.
5. Evidence, Review and Remedy	Can the institution and an affected person reconstruct, understand, challenge and correct a significant outcome or failure?	Administrative and technical evidence; intelligible reasons; meaningful human or institutional review; complaint, appeal, ombuds, regulator and judicial-review readiness; correction of individual and systemic error, including propagation.	For rights-significant functions, absence of sufficient evidence, meaningful challenge or effective correction must block ordinary deployment. A published description or nominal human presence does not establish a remedy.
6. Continuity and Exit	Can the institution continue its legal duties through outage, attack, supplier failure, change, renewal or termination, and exit without abandoning rights, evidence or service?	Tested continuity and non-digital fallback; incident command and safe degradation; portability, switching and transition assistance; preservation of evidence, pending proceedings and corrections through transition.	Continuity and exit must be tested before a renewal or contract-break decision becomes unavoidable, not after dependency has become irreversible.

Table II.2. The Six Public Law Gates

II.2.7 Gate 4 is not a generic cybersecurity score and does not decide whether an affected person has an effective remedy; that is Gate 5's question. Gate 1 establishes authority that no technical capability can supply.

Step 4 — Causal Synthesis

II.2.8 Compliance with the applicable law cannot be established by examining the algorithm or technical component in isolation. Causal synthesis reads Gate, capability and layer findings together as chains, asking of every material finding: (a) what is the initiating condition; (b) through which layer does it propagate; (c) which safeguard is supposed to interrupt the propagation, and has that safeguard actually been exercised or merely documented; and (d) what residual risk remains once the safeguard's real, rather than nominal, effect is taken into account. A favourable assessment of each component separately cannot replace this analysis of their combined operation.

II.2.9 Three evidentiary judgements are recorded separately and are never merged:

- **Risk** — potential harm: severity, likelihood, scale, duration, vulnerability, reversibility and propagation.
- **Evidence confidence** — the support for a finding: high where current evidence is verified and appropriately corroborated; moderate where access or testing is limited; low where evidence is missing, assumed or materially contested.
- **Implementation integrity** — whether safeguards are assigned, resourced, monitored and enforceable in practice.

II.2.10 A low estimated probability cannot cure missing evidence of legal authority or remedy. A contractual entitlement does not demonstrate adequate staffing or effective use.

Step 5 — Institutional Decision

II.2.11 The responsible institution adopts and records a reasoned public-law judgement in one of eight categories.

Decision category	When it applies	Typical trigger
Proceed	All Gates are Pass or Not Engaged; the capabilities are demonstrated with high evidence confidence.	No capability gap identified.
Proceed subject to enforceable conditions	Gates are Pass or Conditional; one or more safeguards are weak but remediable, with a named owner and deadline.	An audit right that exists but is untested.
Pilot under controlled conditions	A novel application where evidence remains prospective.	Capability exists in design but lacks an operational track record.
Redesign and resubmit	A Gate fails but the function remains lawful in principle with redesign.	No data-access or audit rights secured.
Suspend	A capability failure creates ongoing rights exposure while redesign proceeds.	Active harm risk.
Discontinue	The function cannot be operated lawfully within any feasible design.	Irremediable Gate failure.
Seek additional legal authority	The function is sound in design but lacks a sufficient legal basis.	Gate 1 failure unrelated to operational control.

Decision category	When it applies	Typical trigger
Refer for independent determination	Evidence confidence is too low for the assessor to conclude.	Supplier-controlled or inaccessible evidence.

Table II.3. The eight institutional-decision categories.

II.2.12 Every decision records its reasons, any dissent, safeguards, conditions, named owners, deadlines and the consequence that follows automatically if a condition is not met by its deadline. A condition without an owner and a deadline is not a condition. "Continue monitoring" or "to be monitored" is not a sufficient condition.

II.2.13 Conditions may govern improvement during lawful operation, but prerequisites must be verified before the dependent activity begins. A Conditional finding does not authorise ordinary full deployment where a blocking requirement is unmet.

II.2.14 A pilot requires an existing lawful basis, protected participants, a limited scope and a stop mechanism. It cannot serve as an exception to a prohibition or as a substitute for a legal mandate.

II.2.15 The accountable institution signs the decision, identifies who verifies conditions and records the next review. Supplier sign-off cannot replace the public decision. Evidence of active harm requires prompt lawful protective action even while a fuller assessment is completed.

Step 6 — Lifecycle Review

II.2.16 Assessment does not end at authorisation or deployment. Material change to law, purpose, data, models, system configuration, suppliers, infrastructure, risk or institutional capacity reopens the relevant Gates. A function approved as a pilot must not expand its population, purpose, data or institutional reach without a recorded reassessment: there is no silent scaling. A decision remains valid only within its assessed scope and conditions; unmet conditions lead to the consequence specified in the decision, including restriction or suspension where warranted.

II.2.17 At every review the institution confirms that:

- a reassessment calendar and trigger log is maintained and current;
- every Conditional finding has an owner, deadline, verification method and consequence;
- continuity and exit have been tested before a renewal or contract-break decision becomes unavoidable;
- post-deployment review has examined incidents, drift, complaints, corrections and disparate effects.

II.2.18 Exit planning starts during design and procurement, although its execution is recorded in Step 6. Transition or termination preserves service obligations, evidence, pending claims and accountability.

DRAFT

II.3 Gate findings and capability ratings

II.3.1 Gate findings. Each Gate receives one reasoned finding:

Finding	Meaning
Pass	Sufficient authority and safeguards are demonstrated.
Conditional	The requirement can be satisfied through an enforceable, time-bound condition before or during controlled deployment. The condition has an owner, deadline, verification method and consequence of non-compliance.
Fail	The arrangement cannot lawfully proceed without redesign, additional authority or discontinuance.
Indeterminate	Evidence confidence is too low for a responsible conclusion; further evidence or independent determination is required.
Not Engaged	The Gate is not engaged by the function as scoped, for recorded reasons.

Table II.4. The five Gate findings.

II.3.2 Each finding records whether its evidence is direct, imported from a specialist assessment, or inferred. "Partial" is not a Gate finding.

II.3.3 The absence of adequate authority, an accountable institution, essential review evidence or a meaningful remedy blocks ordinary rights-significant deployment. Prohibited or unlawfully discriminatory use cannot be balanced away. An Indeterminate finding on a non-compensable requirement, caused by missing rather than adverse evidence, has the same deployment consequence as a Fail until sufficient evidence is obtained. Critical continuity or exit defects likewise block an arrangement whose failure would disable legal obligations.

II.3.4 Capability ratings. Each of the ten capabilities is rated Yes, Partial or No. For each capability the assessor separates three questions, since a positive answer to the first two is compatible with a negative answer to the third: (a) does the institution hold the legal power or entitlement — a statutory mandate, a contractual audit clause, a documented override authority; (b) does it hold the practical capacity and resources to exercise it — trained staff, technical access, institutional time; and (c) has the capability been demonstrated under realistic conditions? Testing may be simulated or staged where live testing would endanger rights or service continuity.

II.3.5 A supplier assertion without institutional evidence caps a rating at Partial. A contract promising data portability does not, without more, demonstrate Exit; a policy permitting human override does not demonstrate Intervene if the officials empowered to exercise it lack the time, information or standing to do so; a public transparency register does not demonstrate Explain at the level of specificity an individual challenge requires; an audit right is rated Yes only when it has been exercised, not merely held.

II.3.6 Proof levels. Evidence of a safeguard is graded Documented (the safeguard exists on paper), Operational (it has been exercised at least once) or Tested (it has been tested under realistic conditions). The minimum proof level required depends on the Review Level (III.3).

DRAFT

II.4 Indicative links between capabilities and Gates

II.4.1 Every assessment explains which capability ratings support or undermine each Gate finding. The links below are indicative and overlapping; they do not group the capabilities and do not replace the proof domains.

Gate	Capabilities that typically supply evidence
1. Lawful Mandate	None can supply legal authority; Understand and Document evidence the consistency between the encoded rule and the legal rule.
2. Rights-Justified Design	Understand, Direct, Document.
3. Public Responsibility	Direct, Document.
4. Operational Control	Direct, Audit, Correct, Intervene.
5. Evidence, Review and Remedy	Document, Audit, Explain, Correct, Preserve evidence.
6. Continuity and Exit	Intervene, Preserve evidence, Continue, Exit.

Table II.5. Indicative evidential links.

II.5 The system lifecycle

II.5.1 The six steps of DPLIA are distinct from the six phases of the system lifecycle to which DPLIA applies: (1) strategic conception; (2) design and procurement; (3) development and deployment; (4) operational governance; (5) review and adaptation; and (6) termination or transition. DPLIA may be applied, in full or at the depth the Review Level requires, in any phase. The modes of use in III.1 correspond to these phases.

DRAFT

Part III — Application

III.1 Six Modes of Use

III.1.1 The Standard and DPLIA are used in six related modes. The first four are ordinary lifecycle uses; the further two extend the Standard to exceptional events and system-level analysis. In every mode, the Normative Core supplies the benchmark, and DPLIA supplies the method by which deficiency, uncertainty, causal interaction, necessary safeguards and institutional consequences are examined.

Mode	What it tests
1. Prospective assessment	Before design, procurement or legislative authorisation: whether a proposed digitally mediated function can lawfully be built at all.
2. Design and development review	During design and build: whether the emerging architecture satisfies the Gates before commitments become difficult to reverse.
3. Pre-deployment assessment	Before approval, authorisation or go-live: whether the function as built — not as originally proposed — meets the Standard.
4. Operational and lifecycle review	During ordinary operation: whether the function continues to meet the Standard, and whether a material change requires reassessment.
5. Incident, failure, complaint, litigation or controversy review	In response to a specific event: which Gate or layer the event exposes and what correction it requires.
6. Systemic, comparative, legislative or institutional review	Across functions, jurisdictions or a sector: patterns that a single-function assessment cannot see.

Table III.1. The Six Modes of Use.

III.1.2 Each use needs an identified decision consequence and continuing review. Assessing a proposed system may result in redesign or non-deployment; assessing an existing function may require immediate protective action alongside longer-term remediation. Lifecycle review (Step 6) is what makes each mode operative: a review that changes nothing in the Record has not produced an institutional decision.

III.2 The Digital Public Function Record

III.2.1 Every assessment maintains one authoritative Digital Public Function Record. The Record is the institutional memory and evidential spine of the assessment, not an optional annex. It is a coherent decision file, not a document warehouse: it links specialist evidence by reference, stating source, version, custodian and verification status, rather than duplicating underlying contracts, datasets or logs. It is an official administrative record and is retained accordingly.

III.2.2 The Record is organised in six sections:

Record section	Essential contents
1. Screening and Review Level	Function, owner, trigger, scope findings, Review Level and reasons, boundary, review date.
2. Function and legal basis	Mandate, purpose, decision pathway, dependencies, authoritative system description; the responsible institution and accountable decision-maker; systems, suppliers and private actors.
3. Governance and affected persons	Six-layer map; Private Actor Test; responsibility allocation; affected persons, interests and vulnerabilities; participation.
4. Gates and synthesis	Gate findings and sub-findings with evidence source; risk, evidence confidence and implementation integrity; alternatives; causal synthesis; dissent.
5. Capabilities and decision	Ten capability ratings with proof levels; safeguards; the Institutional Decision; conditions, owners, deadlines and consequences; monitoring, redress, continuity and exit arrangements.
6. Public accountability and lifecycle	Statement of findings; public summary; consultation responses; register entry; notice and challenge routes; review dates, triggers, incidents, modifications and subsequent decisions.

Table III.2. The six sections of the Digital Public Function Record.

III.2.3 Procurement documents should require, as conditions precedent to contract award, the audit, evidence, change-control and exit rights that Gates 3, 4 and 6 test. A right asserted for the first time after signature is evidence of a gap in the Record, not a cure for one.

III.3 Review Levels

III.3.1 An assessment is conducted at one of three Review Levels. The Review Level determines who assesses, how much evidence is required, and the independence the review must have. It is a proportionality judgement fixed in Step 1 and revisited whenever the function changes materially; it does not substitute for the substantive findings the Gates produce.

	Level 1 — Self-assessment	Level 2 — Reviewed assessment	Level 3 — Independent assessment
Who assesses	The responsible institution.	The responsible institution, with sign-off by a named reviewer independent of the assessed function.	A party independent of the responsible institution.
Indicative functions	Limited public-law significance; reversible support; no rights-significant automation.	Material effect on rights, services or public trust; moderate irreversibility.	High constitutional significance or irreversibility; high private dependence; vulnerable groups at scale; blocking findings or contested evidence.

	Level 1 — Self-assessment	Level 2 — Reviewed assessment	Level 3 — Independent assessment
Minimum record	Concise Record; named owner; relevant evidence; proportionate monitoring. Gates may be recorded as Pass or Not Engaged on minimal evidence where reasons are stated.	Complete Record; full six-Gate analysis; public summary; specialist annexes triggered by the function.	Full evidence index; affected-person engagement; senior authorisation.
Minimum proof level	Documented.	Operational for each material safeguard.	Tested for capabilities central to legality, remedy, continuity and exit.
Output	Statement of findings against the Standard.	Statement of findings against the Standard.	Statement of findings against the Standard.

Table III.3. The three Review Levels.

III.3.2 Selecting the Level. The Level follows the function's impact, the vulnerability of affected persons, scale, reversibility, private dependence, novelty and evidence asymmetry. Labels such as justice, identity or welfare do not alone determine the Level: the function, its consequences and its dependencies must be analysed.

III.3.3 Constitutional-critical functions. A function that operates constitutionally critical infrastructure (I.8.4) is assessed at Level 3 and additionally requires enhanced continuity and exit testing, incident exercises, periodic independent review, entry in the public register, and senior responsibility for the continuity of essential public obligations.

III.3.4 Assurance context. Donor, cross-border, emergency, security-sensitive or sector-specific conditions may add requirements. They never lower the Review Level or reduce the depth of the substantive assessment. The same function does not receive a lower public-law standard because an assessment is commissioned for funding purposes.

III.3.5 Outside scope. A function that fails the Functional Scope Test is not assigned a Review Level. It receives the screening record described in II.2.3.

III.4 Statement of findings

III.4.1 At every Review Level the output of an assessment is a statement of findings against the Standard. It states: the function and responsible institution; the Review Level and the identity and independence of the assessor or reviewer; the scope, criteria and evidence relied on, and the date at which evidence was verified; each Gate finding; the ten capability ratings and proof levels; the evidence confidence; the Institutional Decision adopted by the responsible institution, where one has been adopted; and the next review date.

III.4.2 A statement of findings is not a certificate, a conformity mark, a declaration of legality or a declaration that a system is compliant. Its findings support, and do not replace, the decision of the competent institution. Completion of an assessment never creates a presumption of legality. A statement is valid only for the

scope, version and date recorded in it; the Standard does not recognise a statement resting on an assessment that was never recorded in a current Record.

III.5 Forms of adoption and legal effect

III.5.1 A competent authority may give the Standard effect as a statutory duty; a ministerial or administrative instruction; a public-service or judicial-administration standard; a procurement requirement; a regulator's method; an ombuds or audit benchmark; a donor safeguard; or a voluntary policy. Its legal effect depends on the adopting instrument.

III.5.2 An adopting instrument should identify the adopting body and its competence, the version of the Standard adopted, the functions covered and the internal consequences of non-compliance. It distinguishes existing legal obligations from additional commitments adopted as institutional policy.

III.5.3 At a minimum, an adopting instrument should provide that:

- every proposed or materially changed digitally mediated public function is screened before procurement, deployment or irreversible design commitment;
- the responsible public authority is named and may not transfer final public-law responsibility by contract;
- functions at Review Level 3, and constitutional-critical functions, receive independent assessment;
- Gate findings are kept separate from risk scores and benefits;
- specialist assessments are incorporated by reference and reconciled in one composite conclusion;
- the institution maintains the ten retained capabilities proportionate to impact;
- public summaries and individual reasons are provided, subject to lawful exemptions;
- monitoring, reassessment, incident response and exit are mandatory lifecycle elements;
- the Digital Public Function Record is an official administrative record and is retained accordingly.

III.5.4 Procurement should secure the audit, documentation, change-control, intervention, continuity and exit arrangements the capabilities require. Smaller institutions may use shared expertise or combine roles, with conflicts disclosed and independent challenge preserved. An institution should document how it will fund staff, review, participation and testing rather than adopt obligations it has no capacity to carry out.

III.5.5 An adopting institution should maintain a public register identifying, for each assessed function, the responsible institution, the assessment date, the version of the Standard applied, the Review Level, the decision, the next review and an accessible challenge route. A two-level publication structure may protect sensitive material while supporting accountability; any restriction on disclosure requires a lawful, reasoned basis and appropriate access for competent independent reviewers.

III.5.6 DPLIA should be integrated with existing governance rather than assigned to a detached ethics office. The coordinating function may sit within a ministry of justice, cabinet office, government digital service, supreme audit institution or cross-government assurance unit; operational responsibility remains with the authority exercising the function.

DRAFT

III.6 Participation and transparency

III.6.1 Participation begins before significant choices close. The Record states who was heard, whose experience remains missing, what changed as a result and why alternatives were rejected. Public summaries support discovery; case-specific reasons and usable complaint routes support remedy. Transparency operates at three levels — register, system and case — and a register-level record does not by itself satisfy case-level reasons or remedy.

III.7 Relationship to other instruments

III.7.1 A public body can satisfy each sectoral obligation individually while the composite function they jointly touch remains unassessed. The Standard is designed to close that gap, not to compete with the instruments that supply it evidence. Use it alongside them as follows.

Instrument	Evidence it supplies	What the Standard adds
Council of Europe Framework Convention on AI and HUDERIA	Context, participation, human rights, democracy and rule-of-law effects and mitigation across the AI lifecycle.	The constitutional-legality and institutional-control layer: jurisdiction-specific Gate findings, retained capabilities and the accountable institutional decision, including for non-AI components.
EU AI Act fundamental-rights impact assessment (art 27)	Affected groups, specific harms, oversight, governance and complaints within its legal scope.	Responsibilities and dependencies across the full public function. The Standard does not replace the FRIA.
EU AI Act requirements for high-risk systems	Evidence on the AI system's own technical and organisational requirements.	Assessment of the composite public function rather than the system in isolation.
GDPR data-protection impact assessment (art 35)	Processing purposes, necessity, risks, safeguards and review.	Institutional authority, non-processing dependencies, overall remedy, continuity and exit.
ISO/IEC 42001	Evidence of organisational AI governance.	The two answer different questions. 42001 certification is relevant evidence, not proof of lawfulness.
NIS2 cybersecurity risk management	Resilience of network and information systems.	Legality, rights and accountability of the function the systems support.
Interoperable Europe Act assessment	Legal, organisational, semantic and technical effects on cross-border interoperability.	Whether an affected person can exercise an equal right once systems exchange data; composite responsibility and continuity.
Canada Directive on Automated Decision-Making and AIA	Impact levels, legal consultation, testing, review and recourse.	Function-wide evidence where digital mediation extends beyond the Directive's institutional or system scope.

Instrument	Evidence it supplies	What the Standard adds
NIST AI RMF	Voluntary AI risk-management evidence and practices.	Applicable public-law obligations and their consequences for the institutional decision.

Table III.4. Relationship to other instruments.

III.7.2 Existing instruments already support integration: a DPIA may address a set of similar processing operations, and the AI Act's fundamental-rights assessment expressly provides for complementarity with a DPIA.

III.7.3 HUDERIA's broad rights and rule-of-law approach is a substantive source of compatible analysis, and its non-binding status does not diminish the value of its methodology. Canada's AIA already incorporates review through the system lifecycle. DPLIA uses such work rather than claiming lifecycle analysis as an exclusive contribution.

DRAFT

Part IV — Stewardship and Soft-Law Implementation

IV.1 Steward and label

IV.1.1 The Standard is stewarded by the Institute for Digital Society and Future Public Law ("the Institute") under the Regulation of the Institute. Until the endorsement described in IV.1.2, it is described as "the Institute's Power over Code: Digital Public Law Standard", with the words "consultation draft" until its adoption.

IV.1.2 The Standard may be described as an EPLO Standard or a Provisional EPLO Standard, or as endorsed by EPLO, only after its endorsement by the EPLO Executive Committee under the Regulation on EPLO Standards. Endorsement does not amend the Standard's text.

IV.2 Consultation, adoption and amendment

IV.2.1 Adoption and amendment follow Article IV.3(f) of the Regulation of the Institute, under which the Scientific Council adopts the Institute's standards and methodologies on the proposal of the Director, and the Scientific Council's Decision on the Procedure for the Development and Adoption of Institute Standards; the Regulation on EPLO Standards also applies. Under those provisions:

- a new version is submitted to public consultation of at least sixty (60) days, and any other substantive amendment to public consultation of at least thirty (30) days, and every comment receives a published disposition;
- the Standard, and any amendment to it, is adopted by the Scientific Council on the proposal of the Director, without the participation of members who have an interest in it, including its authors;
- each adopted version carries a version number and date and is entered in a public register maintained by the Institute.

IV.2.2 Each amendment is published with its reasons and a record of changed requirements. It states its effect on assessments already completed or in progress and any transitional arrangement. Statements of findings state the version of the Standard applied.

IV.2.3 Stewardship publishes its responsibilities, participation procedures, conflict-of-interest rules and version history. It includes public institutions, legal and technical specialists, affected communities and independent researchers.

IV.3 Soft-law implementation tools

IV.3.1 The Standard is implemented through soft-law tools: guiding principles; model clauses and model regulatory provisions; advisory opinions of the Institute; requests for comments; commentaries and interpretive notes; training and practice guides; and interoperability statements with instruments of intergovernmental organisations.

DRAFT

IV.4 Assessment, audit and compliance validation

IV.4.1 Assessment, audit and compliance validation carried out by or for the Institute rest on an agreed scope, identified criteria and verifiable evidence. The Institute issues its findings as statements against the Standard (III.4). They support, but do not replace, the competent institution's decision.

IV.4.2 Any public attestation of results on the Institute's own initiative requires a separate decision of the EPLO Executive Committee.

IV.5 Legal effect and public status

IV.5.1 The Standard is not legally binding unless a competent authority gives it effect through its own instrument (III.5). Neither the Standard nor any statement of findings confers legal power, creates a presumption of legality, or gives the Institute or any assessor a reserved public status.

IV.6 Personnel certification

IV.6.1 When a certification body for the competence of persons is established, certification will operate behind an impartiality firewall between training, assessment and certification laid down in the decision establishing it.

DRAFT