

TEISOND

Civic Infrastructure for Continuous Legitimacy Monitoring

WHITE PAPER

Version 4.0 (Public)

August 2026

MISSION STATEMENT

Teisond provides citizens with permanent infrastructure to render judgment on any official exercising governmental authority – making public legitimacy visible, continuous, and comprehensive – for every official, every day.

DOCUMENT STATUS

This White Paper presents the conceptual framework, methodology, governance principles, and implementation approach for Teisond – a civic technology platform for continuous legitimacy monitoring of government officials, operated by AGPT Ltd (UK).

This document is published for general informational purposes. It is intended for citizens, media organisations, researchers, civic organisations, and public officials interested in the Platform's mission and methodology. For partnership inquiries: hello@teisond.com. Website: teisond.com.

Language Versions

This White Paper is published in English as the canonical version. Official translations of the Executive Summary and Section 1 into national languages are available on the respective national platform pages ({{country}}.teisond.com/whitepaper); the remaining sections are published in English. In the event of any discrepancy between a translation and the English original, the English version shall prevail. Translation dates and update status are indicated on each language version.

COPYRIGHT AND USAGE

© 2026 AGPT Ltd. All rights reserved.

This document may be shared for informational purposes. Reproduction, distribution, or derivative works require written permission from AGPT Ltd. This document is published in its entirety for public access.

DISCLAIMER

This White Paper contains forward-looking statements regarding anticipated platform development, jurisdiction activation, and operational capabilities. Actual outcomes may differ due to technical, regulatory, and other factors. The information provided is for informational purposes only and does not constitute legal advice or an offer to sell securities. Readers with specific legal or compliance questions are encouraged to seek qualified professional advice in their jurisdiction.

READER'S GUIDE

Document Scope

This is the complete public edition of the Teisond White Paper. It covers all ten sections plus five appendices. Some implementation details (anti-manipulation algorithm specifications, pricing schedules, vendor-specific configurations) are omitted by design to prevent gaming, not because they are restricted.

Document Structure

Section 1 – Introduction. What problem we solve, why existing instruments fall short, what Teisond is and is not, and why now.

Section 2 – Concept and Methodology. Core concept (legitimacy as a continuous signal), objects of monitoring, judgment mechanism, legitimacy index calculation, citizen value proposition, anti-manipulation safeguards, methodological transparency, limitations and biases.

Section 3 – Technical Architecture. Design philosophy, multi-tenant architecture, identity verification, data separation, publication controls, infrastructure resilience.

Section 4 – Revenue Model and Economics. Two-tier data access architecture (public and subscriber), subscription model, primary and secondary revenue sources, cost structure, permanent exclusions.

Section 5 – Legal Structure and Jurisdictional Framework. Bands of jurisdiction, GDPR as baseline, data governance and publication policy, liability and dispute resolution, operational resilience, verification independence, jurisdictions beyond the single legal space.

Section 6 – Governance and Ethics. Governing principles, roles and jurisdictions passport, ethical commitments and boundaries, stakeholder relationships, ethical dilemmas and resolution frameworks, governance evolution.

Section 7 – Roadmap and Implementation. Simultaneous presence, activation as readiness permits, phased functionality, election sensitivity protocols, long-term vision, infrastructure and partner ecosystem, security and compliance roadmap.

Section 8 – Team and Organisation. Organisational philosophy, founder and leadership, team development, advisory board, governance and succession, community as institutional foundation.

Section 9 – Civic Ownership. The principle of citizen ownership, distributed infrastructure, token model and ownership pathway, governance distribution, transition from community formation to citizen ownership.

Section 10 – Conclusion. The case for continuous legitimacy monitoring, what the Platform achieves and does not, business model as mission alignment, governance as ongoing practice.

Appendices A–E. Theoretical and philosophical foundations; glossary; frequently asked questions; bibliography and references; governmental authority position estimates by level.

Navigation by Reader Type

Public officials: Executive Summary, Sections 1, 2 (overview), 4, 10. Time: 1-2 hours. Focus: what the Platform measures, how indices work, subscription services.

Civic organisations and partners: Executive Summary, Sections 1, 2, 5, 6, 7, 9, 10. Time: 3-5 hours. Focus: methodology, legal framework, governance principles, civic ownership architecture, deployment approach, partnership opportunities.

Academics and researchers: Sections 1, 2, 6, 9, 10, Appendix A. Time: 4-5 hours. Focus: theoretical grounding, methodology rigour, legitimacy concepts, civic ownership model, research opportunities.

Media and journalists: Executive Summary, Sections 1, 2 (overview), 6, 9, 10. Time: 1-2 hours. Focus: democratic innovation angle, citizen ownership model, governance principles, credibility indicators.

Strategic partners: Executive Summary, Sections 4, 5, 7, 8, 9, 10. Time: 3-4 hours. Focus: revenue model, legal structure, roadmap, team, civic ownership trajectory.

General public: Executive Summary, Section 1, Sections 9–10. Time: 30-60 minutes. Focus: what problem this solves, how it works, who owns it, why it matters.

Reading Time Estimates

Quick orientation: 30 minutes (Executive Summary only). Basic understanding: 1-2 hours (Executive Summary, Sections 1 and 10). Comprehensive grasp: 3-5 hours (all ten sections). Full reading: 6-8 hours (complete document including appendices). Academic study: 8-12 hours (with detailed attention to Appendix A).

Feedback Welcome

This White Paper will evolve through engagement with readers. If you find sections unclear, redundant, or insufficient, please provide feedback: hello@teisond.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

SECTION 1: INTRODUCTION

- 1.1 The Democratic Accountability Deficit
- 1.2 Existing Mechanisms and Their Limits
- 1.3 Attempted Remedies and Institutional Barriers
- 1.4 The Teisond Solution
- 1.5 Why Now: Technological and Social Readiness
- 1.6 Public Legitimacy Analytics as a New Category of Data and a Business Model
- 1.7 A Universal Mission, a Disciplined Execution

SECTION 2: CONCEPT AND METHODOLOGY

- 2.1 Core Concept: Legitimacy as Continuous Variable
- 2.2 Objects of Monitoring
- 2.3 Judgment Mechanism
- 2.4 Legitimacy Index Calculation
- 2.5 Citizen Value Proposition: The Psychology of Participation
- 2.6 Anti-Manipulation Safeguards
- 2.7 Methodological Transparency and Auditability
- 2.8 Limitations, Biases and Ethical Considerations
- 2.9 From Unidirectional Authority to Mutual Accountability

SECTION 3: TECHNICAL ARCHITECTURE

- 3.1 Design Philosophy: Single Engine, Multiple Configurations
- 3.2 Identity Verification: One Citizen, One Account
- 3.3 Data Architecture: Separation and Minimisation
- 3.4 Publication and Access Controls
- 3.5 Anti-Manipulation Safeguards
- 3.6 Infrastructure Resilience

SECTION 4: REVENUE MODEL AND ECONOMICS

- 4.1 Data Access Architecture: Public and Subscriber
- 4.2 Primary Revenue: Officials Monitoring Themselves

- 4.3 Secondary Revenue Sources
- 4.4 Cost Structure: Automation-First Operations
- 4.5 What the Revenue Model Excludes

SECTION 5: LEGAL STRUCTURE AND JURISDICTIONAL FRAMEWORK

- 5.1 Operational Structure Within the Single Legal Space
- 5.2 Jurisdictional Home
- 5.3 National Data Governance
- 5.4 Data Governance and Compliance
- 5.5 Liability and Risk Allocation
- 5.6 Dispute Resolution
- 5.7 Operational Resilience and Contingency
- 5.8 Verification Independence
- 5.9 Legal Structure Evolution
- 5.10 Jurisdictions Beyond the Single Legal Space
- 5.11 Conclusion: Legal Framework as Mission Enabler

SECTION 6: GOVERNANCE AND ETHICS

- 6.1 Governing Principles
- 6.2 Roles and Jurisdictions Passport
- 6.3 Ethical Commitments and Boundaries
- 6.4 Stakeholder Relationships and Accountability
- 6.5 Ethical Dilemmas and Resolution Frameworks
- 6.6 Governance Evolution and Future Considerations

SECTION 7: ROADMAP AND IMPLEMENTATION

- 7.1 Simultaneous Presence
- 7.2 Activation as Readiness Permits
- 7.3 Phased Functionality
- 7.4 Election Sensitivity
- 7.5 Long-Term Vision
- 7.6 Infrastructure and Partner Ecosystem
- 7.7 Security and Compliance Roadmap

SECTION 8: TEAM AND ORGANISATION

- 8.1 Organisational Philosophy
- 8.2 Founder and Leadership
- 8.3 Team Development
- 8.4 Advisory Board

8.5 Governance and Succession

8.6 Community as Institutional Foundation

SECTION 9: CIVIC OWNERSHIP

9.1 The Principle: Value Belongs to Those Who Create It

9.2 Distributed Infrastructure

9.3 Token Model and Ownership Pathway

9.4 Governance Distribution

9.5 From Community Formation to Citizen Ownership

SECTION 10: CONCLUSION

10.1 The Case for Continuous Legitimacy Monitoring

10.2 Why the Teisond Solution is Viable Now

10.3 Stakeholder Value Proposition

10.4 What the Platform Does Not Provide

10.5 Long-Term Governance Vision

10.6 Why Centralised Multi-Tenant Architecture

10.7 Business Model Aligned with Mission

10.8 Governance as Continuous Practice

10.9 Realistic Expectations

10.10 Acknowledged Risks

10.11 Call to Action

10.12 Final Reflections: Democracy as Continuous Practice

APPENDIX A: THEORETICAL AND PHILOSOPHICAL FOUNDATIONS

A.1 Introduction: Why Theory Matters

A.2 Legitimacy: Conceptual Framework

A.3 Electoral Legitimacy: Two Fundamental Lacunae

A.4 Social Control Reconceptualised

A.5 Crisis of Civic Cohesion

A.6 Synthesis: How Teisond Addresses Theoretical Gaps

A.7 DAO and Tokenisation: Civic Ownership Philosophy

A.8 Conclusion: Theory Informs Practice

APPENDIX B: GLOSSARY OF TERMS

APPENDIX C: FREQUENTLY ASKED QUESTIONS

C.1 General

C.2 For Citizens

- C.3 Method & Privacy
- C.4 Reading and Using the Index
- C.5 Product & Access
- C.6 Officials, Media & Civil Society
- C.7 Compliance & Operations
- C.8 Governance Evolution

APPENDIX D: BIBLIOGRAPHY AND REFERENCES

- D.1 Core Theory of Legitimacy and Democratic Accountability
- D.2 Measurement and Statistical Guardrails
- D.3 Privacy by Design and Publication Thresholds
- D.4 Human Rights and Public Interest Basis
- D.5 Neutrality, Transparency and Media Use
- D.6 Governance, Tokens and DAO (Non-Financial, Scoped)
- D.7 How to Cite this White Paper
- D.8 Versioning Note

APPENDIX E: GOVERNMENTAL AUTHORITY – DETAILED POSITION ESTIMATES BY LEVEL

- E.1 Level 1: National Authority
- E.2 Level 2: Regional Authority
- E.3 Level 3: Municipal Authority
- E.4 Level 4: Local Officials and Appointed Administrators

EXECUTIVE SUMMARY

Every citizen of a democratically governed country holds a body of internationally recognised civil and political rights: rights that shield the individual from injustice at the hands of the state, and that secure a place in the civic and political life of society. Some of them, however, remain declarations. They are written into treaties, constitutions and statutes, and left without any mechanism through which an ordinary person might actually exercise them.

Modern democracies operate no mechanism by which the judgment of citizens might bear upon the quality of the authority exercised over them – neither across the long intervals between elections, nor in respect of the authority of the ungranted mandate, the countless officials who are appointed rather than chosen. This absence is not an oversight awaiting correction. It has hardened into a permanent structural feature of the democratic order, and it preserves, undisturbed, a latent social conflict as old as government itself: the conflict inherent in the compulsion exercised by some members of society over others, and in the inequality of their positions with respect to the distribution of power.

Teisond is a universal digital platform, capable of independent and autonomous operation in any democratic jurisdiction as an economically self-sufficient nationwide infrastructure of civic judgment.

Its purpose is to extend the familiar repertoire of democratic practice by one further mechanism: an institution of civic monitoring of the public legitimacy of officials at every level of public authority. Such monitoring consists in the continuous collection and aggregation of the personal attitudes of citizens towards serving holders of power – judgments rendered by verified citizens of the country, users of the Teisond Platform, of their own will and by their own choice, freely and at no cost, in a simple binary form, trust or distrust, and open to change or withdrawal at any moment.

From these judgments the Platform produces public indices of the legitimacy of each object of monitoring, released once a minimally sufficient body of judgment has accumulated. Beyond the indices themselves, a distinct specialisation of the Platform is the continuous generation of analytical derivatives of monitoring: data intended for use by every participant in public information exchange, for personal, civic and commercial ends.

What separates Teisond from the many existing channels of communication and information exchange is architectural. It resolves the old dilemma of authenticity and anonymity: irreversible cryptographic hashing joins, for the first time, the verifiability of the participant with the anonymity of the judgment.

One consequence of an institution of this kind is the appearance of a category of data that did not exist before: Public Legitimacy Analytics (PLA). The scientific soundness of the methodology by which the Teisond platform gathers these data is what makes them trustworthy; the market value of the Platform's information products is what makes the infrastructure of civic judgment economically self-sufficient.

SECTION 1: INTRODUCTION

1.1 The Democratic Accountability Deficit

Classical constitutional theory proclaims the people the sole source of power. On that logic representative democracy is the legitimate frame, and the system of public administration the instrument that gives effect to the sovereign's will. The practice of modern government reveals a persistent divergence between the declaration and the social reality. Democracies have come up against an accountability deficit that is turning public governance, by degrees, into a closed and self-reproducing process. The deficit is systemic in character, and it appears in two connected circuits, each of which weakens the capacity of citizens to influence those who govern them.

1.1.1 The First Circuit: The Deficit of Extra-Electoral Influence

The first circuit is laid down in the nature of the representative model itself, which may be reduced to a formula: continuous power, episodic oversight.

On polling day the citizen is the supreme subject of politics, delegating through the ballot the right to govern. But the act is a single one, a conditional blank cheque written years in advance. Once the polling stations close, power becomes continuous, autonomous and monopolistic, while public control over it contracts to the nominal. The citizen moves from the centre of the system of public administration to its periphery, and turns from a subject of politics into an object of its effects.

Formal elections remain the principal mechanism for renewing and revoking mandates of power, yet they occur discretely, ordinarily once in four or five years. Between electoral events citizens live through a long period of practical disenfranchisement, deprived of any accessible structured instrument of influence. The legalised forms of political interaction – public hearings, assemblies, petitions – are received by the population as rituals without consequence. Digital initiatives of the gov tech kind and deliberative practices erect no more than a participatory façade, since they are pointedly advisory in character and easily disregarded by the officials to whom they are addressed. Power remains continuous; oversight of it remains sporadic.

1.1.2 The Second Circuit: The Authority of The Ungranted Mandate

Where the first circuit concerns elected power alone, the second, and the deeper of the two, covers the whole apparatus of state public administration.

Modern governance is legally layered: elected representatives concentrate on framework norms of nationwide application, while real everyday power – the right to issue instructions and licences, to allocate budgets, to inspect and to impose sanctions – passes to appointees.

Beyond the offices of political power there operates an immense administrative and bureaucratic apparatus which governs the public space day by day and holds direct and immediate authority

over the population. These are the directors of healthcare and education establishments, the heads of social services, the chiefs of inspectorates, the commanders and functionaries of law enforcement. All of them take decisions, general and individual, which citizens are compelled to obey under threat of state compulsion.

When such an official proves incompetent, partial, contemptuous or corruptly motivated, the ordinary citizen stands in a position of effective absence of legitimate defence. Appeal procedures are for the most part internal to the department and directed at protecting the interests of the institution; judicial protection is either disproportionate in cost to the weight of the matter or out of reach for most citizens; the media respond only to isolated cases loud enough to become news. Electoral levers are powerless here: this category of officials is by definition not elected and faces no electoral risk. The citizen, in short, holds no real lever over their conduct or over the quality of their administration.

This actual absence of feedback between the governed and those who govern is what constitutes the deficit of legitimate public influence.

1.1.3 The Scale of Power Beyond Oversight

The scale of the administrative blind spot formed by the two circuits is striking. What is meant here by permanent public oversight is not specialist political analysis, and not visibility in the media, but regular, verified and systematic measurement of the level of public trust. By that criterion, in any modern democracy the overwhelming majority of the apparatus of power stands outside oversight altogether.

In an average European country of thirty to fifty million people, some tens of senior political figures at most are covered by any form of sociological monitoring. Real powers of authority, meanwhile – the disposal of society's resources, decisions of permission and prohibition, the exercise of functions of compulsion – are held by more than a hundred thousand appointed administrators.

The figures below show the ratio between those who actually exercise state power and those whose standing with the public is at least sporadically tracked between elections:

- a small democracy (3–5 million people): some 10,000–20,000 officials exercising power, against some 5–15 under sporadic observation;
- a modest state (10–30 million): some 30,000–100,000 against 10–30;
- a mid-sized state (30–50 million): some 100,000–150,000 against 15–50;
- a large state (50–100 million): some 150,000–500,000 against 30–80.

Put another way, for every official whose level of public trust is periodically published there are several thousand who act in conditions of complete public invisibility.

1.1.4 The First Systemic Premise: The Presumption of an Incompetent Demos

The persistence of both circuits rests on two deep premises built into the modern architecture of power.

The first is the presumption of an incompetent demos. Political institutions and electoral technique proceed on the thinly concealed assumption that the ordinary citizen is incapable of forming an independent rational assessment of complex administrative decisions. Citizens are taken to delegate power to representatives while remaining permanently without the competences that oversight of those representatives would require. From this follows the settled practice of managing

the voter's behaviour through media narratives and information campaigns, justified by a crudely generalised public good.

The opposing position, less popular among governing elites, holds that civic competence is a real and widely distributed capacity of society. It does not idealise citizens as well informed or immune to manipulation, but it rejects outright the idea of an innate inability of the population to recognise its own interest or that of society. That people are able to observe the actions of institutions, to set them against their own expectations and to form a relevant judgment about the quality of public administration is not in doubt. The question is only whether there exists a system of information exchange capable of turning that capacity into a sustained public signal.

1.1.5 The Second Systemic Premise: The Protective Coalition

The second premise concerns the internal logic of the state apparatus. In theory the executive vertical of officialdom is accountable to elected politicians, and they in turn to the people. In practice the scheme is eroded by the politicisation of the civil service and by nepotism.

Since the bureaucratic apparatus is ordinarily the creation of the political group in power, that group loses any motive to exercise real control over its own appointees. The effect is one of mutual cover: the apparatus supplies politicians with administrative resource and financial stability, and politicians in return guarantee the apparatus immunity from the law and from public anger [O'Donnell, 1998]. The declared hierarchical accountability within the state apparatus becomes an instrument by which the system defends itself against external influence from its own constitutional source. This feature of the system should not be attributed to any conspiratorial inclination on the part of its individual participants; it is a consequence of its operating without any independent external oversight.

1.1.6 Two Deficits, One Problem

The deficit of extra-electoral influence and the deficit of legitimate public influence share a single root cause: the absence of an organised system of mutual accountability between citizens and power, existing as a social institution in its own right.

Officials exercise continuous power as a matter of system; citizens lack any systematic continuous mechanism bearing on the quality of that power. The consequence is a structurally one-directional relationship: authority flows downward without interruption, while the response of its source rises upward only episodically, and in respect of the most numerous segment of that authority does not rise at all. The modern architecture of public governance displays a deep asymmetry. The system of state administration holds robust institutional barriers, elaborate procedures and legal immunities that protect administrators from public discontent, while the citizen, under the continuous pressure of bureaucratic decisions, is left without defence.

Above all, the problem is not a speculative one. The evidently declarative quality of the people's celebrated status as the source of power carries critical practical significance, above all through the standing threat of a crisis of legitimacy. When citizens begin, in numbers, to see that status as a formula on paper, trust in state institutions as such gives way. Political practice testifies that once a constitutional principle ceases to work, what follows is not theoretical dispute but real social upheaval, from revolutionary rupture to the slide back into authoritarianism.

The deficit of mutual accountability between power and citizens is no more speculative than this. Accountability in an institutionalised form, recognised by society, is very nearly the only real

safeguard holding a population back from the loss of any sense of influence over power, and with it from the destructive consequences described.

1.1.7 The Roots of the Deficits

Several structural factors explain why an infrastructure of mutual accountability between citizens and power never arose of its own accord.

The most obvious is the technological limitation of earlier ages. Until now there existed no instrument for the mass collection, aggregation and publication of the individual judgments of citizens in real time. The inherited instruments – petitions, surveys, rallies – were shaped by the communication capacities of their time, and were never conceived as a means of continuous information exchange between a population and its government.

The second factor is the inherent rejection by bureaucracy, in every age, of any external attempt at oversight that it cannot administer itself. Any system resists ideas, phenomena or foreign elements incompatible with its own deep nature. Internal control mechanisms, meanwhile, are created to protect institutional cohesion rather than to widen the scope for intervention from outside.

To this belongs political opportunism, and the political advantage that flows from the existence of grey zones and inter-electoral vacuums of accountability, and hence the absence of any incentive to build an infrastructure that would fill them.

All of this is reinforced by the barriers to collective action: the dispersion of citizens and the lack of resources to build independent systems of monitoring. Where organised groups do arise, they mostly serve narrow interests rather than the idea of systematic civic oversight at every level of power, an idea that has always laboured under the assumption of a demos incapable of forming judgments worth having on matters of politics and administration.

Finally, a decisive part was played by the neglect, in scholarship, of any vision of public legitimacy as a continuous, quantified and dynamic variable, one that can and should be subject to permanent public measurement. The absence of a conceptual frame in turn prevented the term from forming and the paradigm from being recognised; and so the corresponding social construct generated no demand for an infrastructure to serve it. It is this omission, conceptual and technological at once, that Teisond exists to fill.

1.2 Existing Mechanisms and Their Limits

Over centuries the democratic world has produced instruments directed, in one way or another, at ordering the relationship between society and power, and among them the inequality of the parties' positions with respect to influence over the decisions of power. None of these instruments, singly or together, has proved capable of closing the deficits described above. The reason lies not in any defect or inefficiency of the instruments themselves, but in the fact that none of them corrects the structural asymmetry of influence: power is exercised continuously, while influence upon it remains episodic and unevenly distributed. In earlier times this asymmetry was taken for an innate property of the order of things. In the modern world it increasingly threatens both social stability and the effectiveness of society, since accumulated distrust and discontent find no legitimate channel of release.

1.2.1 Traditional Democratic Mechanisms

Elections remain the cornerstone of accountability, since they carry a direct sanctioning mechanism: the replacement of those in power. Yet elections operate only on macro-cycles, confining the citizen's right of political intervention to rigidly periodic access. In respect of the multitude of appointed administrators, no form of that right is provided at all. Elections also yield a binary result, retain or replace, compressing thousands of impressions and judgments into a single bipolar choice.

The alternative instruments of direct expression – referendums, recall procedures on the principle of the imperative mandate, and their like – carry an exceptionally high threshold of mobilisation and cost. They are therefore used only in situations of crisis, and only where the law expressly provides for them.

1.2.2 Internal Mechanisms of Control

Institutions of parliamentary and intra-state control, such as audit offices, supervisory inspectorates and the offices of ombudsmen, are a characteristic expression of democracy's attempt to build mechanisms of accountability directly into the machinery of the state.

Each is intended to secure the performance of some function important to the state, but to count them as part of a civic infrastructure of oversight would be naive. In practice they concentrate either on high-level policy or on manifest legal deviations, leaving aside administrative ineffectiveness, bureaucratic obstruction and the institutional arrogance of officials in their dealings with the population. Situated inside the state apparatus, such bodies are inevitably drawn into vertical protective coalitions, where preserving the stability of the system always prevails over allaying public discontent.

In these conditions the complaint of an individual is bound to remain solitary within a closed bureaucratic system. It does not accumulate with others like it, does not become a transparent public signal, and leaves the real scale of the problem invisible to society.

1.2.3 Instruments of Civic Participation

Instruments of civic participation display limitations of another kind. Petition campaigns, even where they lapse the moment a formal bureaucratic reply is issued, do generate a sporadic public signal. Their overall effectiveness is nonetheless negligible, owing to the legal non-binding quality of the demands and the discretionary character of the response. An illustration of the latter is the existence of formal signature thresholds: ten thousand may trigger a reaction, nine thousand nine hundred and ninety-nine will not. The principal weakness of the petition as an instrument of civic influence, however, is that neither the fact of its submission nor the content of its demands creates, in itself, any incentive for those in power to respond. As instruments of civic influence or of oversight over power, therefore, petitions cannot serve.

Street protest signals the outer limit of tension in public feeling, but carries a high cost of participation, risks to the personal safety of those involved, and the raising of conflict to the stage of open confrontation. For building any durable social equilibrium it is by definition unsuited.

Collective forms of engagement such as public hearings and consultations suffer from a systematic error of sampling, since those who take part are an unrepresentative and often interested minority. Beyond that, proceedings of this kind are markedly declarative in character, which allows officials to simulate dialogue without incurring any obligation to change their conduct.

1.2.4 Opinion Polling

Sociological polling is a relatively effective instrument for studying the state of public feeling, but is unsuited to the role of a public infrastructure of accountability by reason of purely structural limits, alongside a series of systemic defects.

The defects of current polling practice with regard to attitudes towards public politicians arise from methodological problems, from political context and from the psychology of respondents, and may be grouped under four heads. Among the methodological and procedural flaws are the effects of the imposed list – a restricted roster of names, and the artificial modelling of a rating through the inclusion or exclusion of a given politician from it – manipulative wording of questions, and the difficulty of assembling a representative sample. Among psychological factors and respondent behaviour are the effect of social desirability, whereby respondents conceal their real political preferences; the fear of voicing a critical opinion during telephone or door-to-door surveys; and the superficiality of assessments, which fix a momentary emotion in place of a settled attitude.

A separate group of problems concerns manipulation in the publication of results and the activity of pseudo-sociological services: commissioned and invented ratings, fragmentary presentation of data in the media, disregard of a margin of error that may exceed the distance between candidates, and disregard of the share of respondents who are undecided or who declined contact. Last comes the problem of the dynamism of the data, the short-life effect: figures that have lost their currency, and whose publication often misinforms society rather than reflecting reality.

1.2.5 Social Networks and Digital Platforms

Social networks give citizens unprecedented scope to voice any judgment whatever, including their attitude towards any holder of power, but as an infrastructure of accountability they carry fundamental defects of construction. They require no verification: an account may be created by anyone. They lack structure: a critical post and the output of a bot farm are indistinguishable as a data format. And they perform no aggregation: individual expressions of discontent do not compose a credible public signal.

The consequence is that social networks and digital platforms of general purpose generate unstructured emotional noise and suffer from endemic unreliability through the prevalence of bots. Alongside this, a substantial defect of social networks remains the deficit of privacy: in criticising power, the citizen is exposed to the risks of profiling, of persecution and of personal retaliation, given the ease of deanonymisation.

1.2.6 The Missing Mechanism

To summarise, not one of the existing instruments possesses the critically necessary set of properties that a hypothetical infrastructure of democratic accountability would have to hold simultaneously: continuity of operation, universality of coverage, cryptographic verification to eliminate distortion, mathematical aggregation of judgments, unimpeded civic participation, and architectural protection of privacy.

This set of properties, or anything approaching it, has never belonged to any instrument of civic participation devised to date. Before turning to the modelling of a proper alternative, however, it is worth considering why the many attempts to modify the existing instruments, in the sense of overcoming the democratic accountability deficit, met with no success.

1.3 Attempted Remedies and Institutional Barriers

The deficits described did not pass unnoticed. Political theory has proposed ways of overcoming them more than once, yet each attempt ran into the structural resistance of the very system it set out to reform. These attempts matter here not as historical reference but as evidence: the gap does not close through the refinement of existing instruments. It requires an instrument of a different nature. What follows examines the attempts to reform both circuits, together with the reasons why each of them came up, without fail, against hard institutional barriers.

1.3.1 Reforms of the First Circuit: Deliberative and Electronic Democracy

Attempts to overcome the accountability deficits of the first circuit took the form of two progressive formats of political order. The first is deliberative democracy, in which the condition of an administrative decision is the prior achievement of public consensus through the participation of citizens in framing it. The second is electronic democracy, which provides for civic participation in governance through the means of information and communication technology [Habermas, 1975; Fishkin, 2011].

Both formats duly revealed defects of their own. The most conspicuous is the participatory façade, arising from the advisory character of decisions taken through such procedures and from the unqualified freedom of their addressees to disregard them. The second is the elitism of participation: deliberative practice always draws in a small self-selected group whose composition does not represent society. The third, particular to the digital formats, is the risk of populism – emotional voting without deep analysis, where the speed and mass reach of the channel reward reaction rather than judgment [Coleman & Moss, 2012]. In sum, formats of this kind widen the space for expression, but create no mechanism whose consequences power would be unable to ignore.

1.3.2 Reforms of the Second Circuit: Making Appointees Elective

The most radical attempt to revive the second circuit lay in the idea of making appointed administrators elective, on the model of the election of sheriffs and judges in some states of the USA. The logic is attractive: if the source of the problem is the absence of electoral responsibility, then electoral responsibility should be introduced.

The principal defect of this route was found to be the politicisation of professional offices. Once law-enforcement or judicial bodies begin to take decisions with an eye to electoral ratings rather than to the law, the very function for which those offices exist is impaired. Beyond that, the voter objectively possesses no instrument for assessing narrowly specialised competences: the procedural quality of a judge's or an investigator's work can no more be assessed through a ballot paper than a surgeon can be chosen by vote [Schumpeter, 1942]. Making a professional office elective substitutes electoral logic for the principle of criteria, and leaves citizens without any means of judging the substance.

1.3.3 Reforms of the Second Circuit: Quasi-Independent Controllers'

The next approach was realised in the form of quasi-independent supervisory bodies: specialised anti-corruption structures, inspectorates, institutions of the ombudsman and the like. The intention was to place control outside the traditional vertical of administration and endow it with institutional autonomy.

The principal and fairly obvious defect proved to be the speed with which such bodies acquired closed procedures of their own and turned into a new mega-bureaucracy, isolated from civil society [Pollitt & Bouckaert, 2011]. Created as a remedy for the closedness of the apparatus, a body of this kind inevitably reproduced that same closedness at a new level. As a result, in place of an independent arbiter the citizen receives one more institution, to be approached under its own rules and awaited upon for its own discretion. More than that, a controller external by design comes in time to be integrated, in fact, into the very structure of mutual protection it was meant to counterbalance.

1.3.4 Reforms of the Second Circuit: New Public Management

The third approach, founded on the concept of new public management, introduced market and service mechanisms, under which the state is transformed into a digital platform and the official into a provider of services with automated KPIs [Osborne, 2010].

Notably, this model proved its worth at the lower, routine level of administration, where interaction with the citizen reduces to a simple service such as the issue of a certificate or a licence. At the higher levels of regulatory decision, however, market criteria prove untenable: the function of state compulsion is by its nature at odds with the logic of market service. The effectiveness of an inspector imposing a sanction, or of an investigator restricting liberty, is not the effectiveness of a service provider to be assessed on service indicators. Where authority is compulsion rather than service, the metric of customer satisfaction loses its meaning.

1.3.5 The Common Barrier: Information Asymmetry

For all their variety of conception, every one of these attempts ran into a single common barrier, most conspicuous in the second circuit. It is information asymmetry – the Weberian phenomenon of power through a monopoly on knowledge, where complex legal jargon and departmental instructions reliably preserve the deficit of public influence [Weber, 1978]. So long as the apparatus remains the only party that understands its own procedures and controls its own data, any attempt at oversight from outside is obliged to rely on information supplied by the object of that oversight.

From this follows a conclusion that narrows the field of possible solutions: no reform of the vertical of power itself, and no reform functionally dependent on that vertical, is capable of overcoming this barrier, since it inherits the barrier's origins.

1.4 The Teisond Solution

The empirically demonstrated institutional weakness of traditional models of public administration establishes the point: neither isolated acts of civic activism, nor quasi-independent safeguards built

into the vertical of power, nor the various gov tech services created by the state itself are objectively capable of defending the public interest against a system that protects its own closedness from outside influence, and the private interest of its functionaries. The existing instruments of civic participation in public governance do not close the accountability deficits, and the modernisation of those instruments holds no prospect, given that they are embedded in the vertical of power, dependent upon it, or both.

The social counterweight to an institutionalised system of state compulsion governed by the logic of self-preservation can only be another system, institutionalised in the same measure: a distinct social institution, independent of power, operating at the level where the social and psychological needs of the individual citizen are met.

1.4.1 Teisond as a New Social Institution

The Teisond solution is a system of continuous civic monitoring of the legitimacy of power, whose purpose is to structure, regulate and legitimise sustained oversight of the manner in which the powers delegated by citizens are exercised in the period between elections.

The practical embodiment of that system is a public digital infrastructure of non-compulsory, extra-formal, sustained feedback, which continuously generates data bearing on the personal career and reputational consequences for holders of power, and so transforms the judgments of citizens into visible signals and into incentives that officials can feel.

That such a system answers to the classical marks of a social institution is evident. The principal purpose of social institutions is to lend stability, order and predictability to social relations, and their form of existence is a durable public infrastructure securing the free and unimpeded participation of citizens in their operation. At the same time, the democratic accountability deficit is a phenomenon that is systemic, all-encompassing and politically sensitive, and therefore capable of being overcome only by another system on the scale of a social institution, rather than by a one-off initiative or a passive instrument. Continuous civic oversight of the public legitimacy of power can and should become a generally recognised social practice, institutionalised in time as an autonomous institution independent of the state.

The founding principle of Teisond is not without precedent. The open data movements and transparency legislation have already established the right of citizens to structured information from the sphere of public administration, from open budgets to transparent procurement. Until now, however, that principle has covered only the institutional dimension of power. Teisond takes the next step and extends it to the personal dimension: the public visibility of the legitimacy of each individual official.

The significance of this frame becomes clearer set against the classical institution of elections. Both systems are social institutions, and in sustaining the viability of democracy they perform different but complementary functions. The institution of elections structures, regulates and legitimises the discrete delegation of powers from the sovereign to its representatives on macro-cycles. The institution of continuous civic monitoring of the legitimacy of power structures, regulates and legitimises sustained oversight of how those powers are exercised in the period between elections. The first answers the question of whom the people entrust with power; the second, the question of how that power is exercised day by day once it has been delegated.

The purpose of this new social institution is accordingly neither to supplant the institutions that already exist, political ones above all, nor to improve them. Its task is not intervention in the work of power or in electoral procedure, but the securing of a durable equilibrium within the system of governance, by balancing the compulsion of power with the continuous reputational signal of society. It confers on the citizen no right to take decisions in place of an official. It returns to the

citizen the right to a judgment of one's own and to its public visibility: basic democratic rights lost since antiquity.

1.4.2 Why an Institution of Civic Monitoring Requires an Independent Infrastructure

Any social institution with the ambition of amounting to more than a set of declarations requires a material and technical skeleton: an infrastructure of its own. The institution of elections rests on an extensive state infrastructure of electoral commissions, polling stations and systems of counting. But the particular nature of an institution monitoring the legitimacy of power does not allow it to depend on the state or on the state's material base, since the object of its oversight is the state itself. An infrastructure administered by the party it is meant to observe loses its meaning at the moment of creation.

In modern conditions, meanwhile, the viability of this institution can be secured by an independent digital infrastructure arising directly within civil society: a civic technology platform with a verifiable data architecture and algorithms open to independent audit. The resilience of such an infrastructure rests neither on rights of ownership, nor on technological means, nor on the physical protection of servers, but on legal legitimation: on basic constitutional norms, and on Article 25 of the International Covenant on Civil and Political Rights, which guarantees to everyone the right to take part in the conduct of public affairs directly. In respect of its own institutional standing, likewise, civic monitoring of public legitimacy is an instrument giving effect to the citizens' right of political expression: the possibility, provided by law, of freely expressing one's will, thoughts and intentions, entailing consequences including legal ones, and founded on freedom of speech and belief.

Ultimately, however, the resilience of an institution of public monitoring is secured neither by law nor by technology, but by scale. Such an institution comes into being and endures for as long as a critical mass of society shares its aims and its motives. When the instruments of monitoring legitimacy are used by millions of verified citizens, the practice of oversight becomes a social phenomenon that cannot be countered administratively without entering into conflict with the source of power itself.

It is on these foundations – institution, independent infrastructure, scale – that the substantive architecture of the Teisond Platform, presented in this White Paper, is built.

1.4.3 The Functional Logic: A Two-Level Ecosystem

The practical embodiment of the Platform requires an environment that converts a dispersed social signal into structured data with low friction and high security.

The architecture of Teisond unfolds on two levels. The civic level provides verified citizens with access to participation in the monitoring of the public legitimacy of holders of power, and with the means of rendering judgment. The Platform level is responsible for the collection, storage and aggregation of those judgments into public indices of legitimacy, protected by a threshold of representativeness and by the principle of privacy by design, and for the preparation of the accompanying analytics. The consumers of the Platform's information products do not form a separate architectural level: officials, media, NGOs and researchers differ only in their procedures of access. Among the advantages of this arrangement, two are of the first importance: it overcomes the asymmetry of information exchange between citizens and power that is inherent in traditional means of mass communication, and it denies the parties to that exchange any means of direct influence upon each other.

1.4.4 The Civic Level: Verification, Anonymity, Binary Judgment

The Platform's interface is designed on the logic of an accessible mass digital product. Anyone may view the current indices of legitimacy of officials freely and without registration; these data are open to all. Identification of citizen users is required only at the moment of rendering a first judgment, which introduces, as a matter of procedure, the democratic standard of one citizen, one account. Thereafter no repeat identification is needed: access to the account is secured by a cryptographic access key bound to the citizen's device, and rendering or changing judgments in respect of any officials takes a few seconds and requires no further checks. Verification is a single event of entry into the application, not a recurring barrier to participation.

Verification takes place through national digital identification services and protects the system against artificial manipulation, coordinated inauthentic behaviour and bot farms. What passes into the system, however, is not the person but only an irreversible cryptographic hash of the identifier. This makes political profiling and deanonymisation technically impossible even for the Platform's own developers: the system is able to confirm that a judgment belongs to a real and unique citizen, but is unable to establish who that citizen is or what the judgment was. Anonymity here is not a technical option of security but a fundamental institutional guarantee of freedom of expression. Without it, a citizen in a small community would never render distrust in a local official.

The act of registering a judgment itself is reduced to a binary choice between trust and distrust, with no further justification required. This binary form shortens a single interaction with the Platform to a minute or two, while the minimisation of thresholds of participation and the absence of any charge encourage the widest possible circle of citizen users towards constant participation in monitoring, as the precondition of network scaling and of the viability of the system. These factors were built into the architecture of the Platform not merely for the convenience of the participants in this information exchange, but above all with a view to forming a distinct space of social communication and to institutionalising the corresponding practice.

1.4.5 The Platform Level: Aggregation, the Publication Threshold, Privacy by Design

The second and final architectural level is the Platform itself: the collection, storage and aggregation of judgments, and their conversion into public indices, being measures of the public legitimacy of a person exercising power in the eyes of those subject to it. Every judgment is rendered in respect of an official identified through the office that person holds. The index is computed as a snapshot of all standing judgments concerning that official at the moment of calculation, and is then published. Calculation occurs at a set periodicity, and so the published index remains unchanged until its next recalculation. The sequence of such snapshots forms the dynamics of public trust in the official over time.

The anonymity of participation and the citizen user's protection against deanonymisation are integrated directly into the Platform's code on the principle of privacy by design. The first safeguard is laid down at the level of verification: since the system stores only an irreversible cryptographic hash, a judgment cannot be linked to the person who rendered it, neither by outsiders nor by the Platform's developers. The second safeguard concerns the data themselves: the system does not, as a matter of principle, retain any history of judgments or of changes of mind, and records only their current status. Even in the event of unauthorised access to the system, an intruder would obtain no more than a body of depersonalised current judgments, without names behind them and without history before them.

A distinct element of the methodology is the statistical publication threshold. An official's index is released once a set number of verified judgments has accumulated; until then the profile shows the progress of accumulation, how many judgments have been recorded and how many remain before the index opens. This is not a technical formality but a standard of quality in measurement: an indicator of legitimacy drawn from too small a body of judgment would be distorted by chance, and

the Platform does not present such values as a measured level of public trust. Thresholds are differentiated by the scale of the office, from several hundred judgments for officials of national rank to several dozen for local ones. The publication of an index accordingly means that a sufficient body of judgment always stands behind it, and the moment an index opens becomes a public event.

1.4.6 The Publicity of the Index

The accumulated body of individual citizens' judgments the Platform converts into a public signal: the index of legitimacy of the official under monitoring. That index is released in an open reputational profile, and in this the Platform gives effect to a principle – that the public nature of power should be matched by the publicity of society's assessment of the legitimacy of the person who holds it. Here the civic signal completes its journey and becomes a social fact.

Officials do not form a separate architectural level of the Platform; they are consumers of its information products. An official's public profile is open to every visitor. A subscription adds analytical depth to the data concerning the level of that official's own public legitimacy, and a verified profile adds the right of reply: a channel of official presence alongside one's own index, in the same plane of public visibility in which the reputational signal is formed.

1.4.7 How Monitoring Legitimacy Produces Accountability

The sceptical question put to an institution of legitimacy monitoring, as to any form of social observation without a separate system of sanction or mechanism of compulsion, is an obvious one: if the publication of an index of legitimacy entails no legal consequence, why should the official under monitoring take any notice of it? The answer is that changes of behaviour outside formalised procedure are brought about not by the threat of sanction but by the force of visibility. Publishing the index of public legitimacy of a holder of power sets in motion several distinct mechanisms of independent action, which in turn compose a set of incentives and motivations that matter to the official.

The first mechanism is electoral anticipation. For holders of elected power, instability or decline in the index signals vulnerability long before the electoral contest reaches its close, and allows public conduct to be corrected. Settled electoral cycles open the feedback channel only at the moment when a response has ceased to mean anything, whereas access to continuously updated data turns a distant threat of defeat into a current parameter of management. The incentive to keep watch on electoral sentiment accordingly operates not only in the pre-election period but throughout a term of office.

The second mechanism is the vulnerability of reputational capital. The index is public and persistent: it exists as common knowledge in the official's relations with voters, party, colleagues and the media. An official whose index declines steadily is bound to face uncomfortable questions from journalists, from fellow party members and from opponents, without any formal consequence, but with consequences that are informally quite palpable. The bearing of reputation on career prospects has counted in every age; the existence of a verified public source multiplies it.

The third mechanism is media amplification: indices carry the potential to become standard reference indicators for the media. Any movement in such an indicator becomes news, which widens the space of interest in civic participation and of motivation towards it; a wider circle of participants in monitoring refines the index and deepens the picture. The feedback loop between the publicity of monitoring data and the intensification of civic participation fills the information space and makes the suppression of an inconvenient index impossible: everyone with an interest can see it.

The fourth mechanism is the response of the competitive environment. Political and administrative rivals acquire the means to cite an opponent's unconvincing indicators of legitimacy as an argument for personnel change, and the opposition quotes them in public. The position of the official under monitoring within the institution becomes vulnerable in matters of career prospects, powers and preferment. In theory an official may ignore the data of public monitoring of one's own legitimacy for as long as one likes; in conditions where those around are showing close interest in it, this is unlikely.

None of these mechanisms formally sanctions or compels; together, however, they radically alter the environment in which a holder of power operates, an environment that thereby loses its principal historical advantages: invisibility and freedom from answering.

1.4.8 What Teisond Is and Is Not

The nature of a social institution lies in structuring the disorder of some sphere of social relations by standardising it. At the same time, an understanding of the social need such an institution exists to satisfy becomes clear in the distinction between what it is and, particularly, what it is not.

Teisond is neither a body controlling deviation through a system of sanctions, nor even a form of association of individuals into groups or structures for the performance of social functions. Its tasks nonetheless answer fully to the marks of satisfying certain basic needs of society, among them security, socialisation and development, and lend themselves to being built by a democratic society into its existing processes.

Teisond is an infrastructure for measuring the attitude of society towards power, which makes civic judgment visible. Its functions end there, but its social value does not: that value lies in the possibility of softening the consequences of the permanent latent social conflict bound up with the compulsion exercised by some members of society over others, and with the inequality of their positions with respect to the distribution of power.

The Platform takes no decisions of its own, creates no obligations, imposes no sanctions, dismisses no one and appoints no one. What its operation produces is a continuous structured flow of data, available for use by a wide range of parties, from organs of state power and political parties to business, the media, scholars and civic organisations, each pursuing pragmatic ends and needs of its own. At the same time, the Platform's operation as a means of social interaction gives rise to a distinct spectrum of social and political consequences: from the use by citizens of open data in reaching their own electoral decisions, and the emergence of an institution of reputation, to the institutional cohesion of society as a form of bridging social capital.

Teisond monitors not the quality of public administration but the attitude of the governed towards those in power who administer it. An index of legitimacy shows the level of citizens' agreement with the performance of particular functions of power by a particular person, not how well, objectively, that person performs them. These are fundamentally different objects of monitoring, and the Platform does not conflate them: a competent official may hold low public legitimacy, and a popular one high legitimacy on middling competence. Telling the one from the other is the work of society, exercised through the media, expert analysis, institutional checks and the judgment of voters; the Platform supplies a signal, and reading it requires the whole ecosystem of democratic institutions.

Teisond is neutral as to political affiliation. It monitors the public legitimacy of all officials without exception, at all levels of power without exception, irrespective of their ideological colouring. The Platform holds no political preferences of its own and no position of its own on who deserves trust and who does not: its function is confined to publishing the actual state of public opinion.

Teisond is neither a social network nor a forum. The Platform provides no facility for comments, messages or the creation of content of any kind, only the structured binary judgment. Nor is the

Platform a system of surveillance in respect of any category of its users, in any form: the object of monitoring is exclusively the public perception of officials' public activity, not their private life or conduct; the participation of citizens is anonymised; and the public character of officials is a legal principle of every democratic state.

The Platform's information data are distributed in the form of market products, which meet the needs of various groups of consumers, social and psychological as well as purely commercial. In relation to citizen users, the Platform is not an instrument for the performance of civic duty: it neither exhorts nor obliges. It renders the citizen a service, unimpeded and free of charge, in satisfying personal social and psychological needs, among them the needs for recognition, for social standing, and for a sense of dignity, of one's own significance and of personal influence.

The overcoming of the democratic accountability deficit, mutual recognition, and the lowering of the level of conflict in society arise as a consequence of the citizen user's pursuit of those needs, and not as the discharge of a task set before that citizen.

Teisond monitors not the quality of public administration but the attitude of the governed towards those in power who administer it. An index of legitimacy shows the level of citizens' agreement with the performance of particular functions of power by a particular person, not how well, objectively, that person performs them. These are fundamentally different objects of monitoring, and the Platform does not conflate them: a competent official may hold low public legitimacy, and a popular one high legitimacy on middling competence. Telling the one from the other is the work of society, exercised through the media, expert analysis, institutional checks and the judgment of voters; the Platform supplies a signal, and reading it requires the whole ecosystem of democratic institutions.

1.4.9 Limits and Honest Expectations

Intellectual honesty requires a clear statement not only of what the Platform does and does not do, but of what it does not promise.

An index of legitimacy records public perception, which is by definition subjective, dependent on prevailing sentiment and open to influence and manipulation of various kinds. It is a measure of trust, not a certification of competence, and should be read as such.

The Platform draws no samples and resorts to no extrapolation: it works with rendered judgments, whose voluntary character is the guarantee of their candour. The threshold of judgments required protects against random noise, but is no safeguard against disproportionate participation: some groups of citizens, for reasons of their own or in respect of particular objects of judgment, speak up more readily than others. Each individual index is accordingly aggregated from a circle of judgments unique to it. By the same token, movement in an index does not always mean a change of attitude; it may reflect a change in the circle of those who have chosen to speak.

1.5 Why Now: Technological and Social Readiness

If the structural deficits of accountability and the untouchability of appointed bureaucracy have existed for centuries, it is necessary to explain what objective factors make the deployment of Teisond both possible and needed at this particular moment. The answer lies at the intersection of two parallel processes: the maturing of an acute social need, and the maturing of technologies capable of meeting it. The first creates demand; the second, for the first time, makes supply possible.

1.5.1 An Infrastructure of Emotion Without an Infrastructure of Judgment

The digital order has already produced a highly effective, all-embracing and universally accessible infrastructure for the discharge of human emotion. Social networks and communication platforms are optimised for holding attention and spreading content, and both of these tactics reward emotional arousal rather than considered judgment. In an infrastructure of that kind, only emotion moves instantly and without impediment.

Yet for all the colossal infrastructure of emotion that has arisen, humanity has still acquired no infrastructure of sober judgment. The available instruments can mobilise people in an instant for a destructive surge, but offer no sustained institutionalised channel for recording and publishing a measured, everyday assessment of the effectiveness of public governance. Emotion is observed immediately and by everyone; considered judgment leaves no trace.

An entire generation has grown up in this environment. The inhabitants of digital platforms constitute ever weightier demographic cohorts in every settled democracy: multilateral interaction within an ecosystem is natural to them, and feedback in real time is their standard of communication. In consequence, the confinement of civic participation in public life, governance and rule-making to a polling booth once in several years admits of no intelligible explanation. For this generation the question is not why one should use such a thing, but why it does not yet exist.

The infrastructural imbalance described contributes to the erosion of the capacity for rational judgment, to the fragmentation of attention, to the coarsening of public discourse and to a fall in trust towards basic models of governance, and ultimately to the atomisation of society. It is precisely these phenomena that form an acute civic demand for an instrument of direct but non-forcible influence: for a way of being heard that requires neither taking to the streets nor an emotional rupture.

1.5.2 Why This Was Impossible Before

Until recently that demand could not be met, for want of technological maturity: the instruments of the previous generation carried two fundamental vulnerabilities.

The first was the absence of any means of remote identification. Without them, any independent survey is defenceless against coordinated inauthentic behaviour: counterfeit participation cannot be told apart from genuine participation. A system in which that distinction is out of reach cannot be received as a legitimate source of a public signal.

The second was that the database architectures of past decades could not guarantee anonymity of participation. Any centralised authentication of a person left a digital trace linking the user of a resource to the message that user sent, and thereby created risks of deanonymisation in conditions offering no protection against influence exercised outside the law.

Even in a mature democracy the citizen depends on power daily and in many dimensions, which is to say that the citizen lives under the continuous operation of compulsion, applied with varying degrees of justice. Decisions to apply that compulsion, moreover, are taken by people, at their discretion and with all the flaws that people have, while instruments of protection such as the courts or the ombudsman are engaged at best after the fact. In such conditions personal participation in any practice of social observation, even an informal one, remains hazardous for the citizen, and the only guarantee against that hazard is the absolute anonymity of the judgment.

The requirements for overcoming these two vulnerabilities are mutually contradictory: a credible signal requires a confirmed identity, and safe participation requires that identity to be absolutely concealed. So long as technology could not join the one to the other, mass independent monitoring of the legitimacy of power remained impossible.

1.5.3 The Change in Technological Preconditions

The situation has changed fundamentally only now, when digital ecosystems have advanced to the necessary infrastructural maturity and closed both of the vulnerabilities named above.

The first precondition is the mass introduction and legal recognition of national systems of digital identification. For the first time these allow the user of an online resource to be identified, authenticated or verified instantly, unconditionally and at no cost to that user, as, among other things, a citizen of the jurisdiction concerned. At the same time no state system is a single point of entry for the Teisond Platform: a parallel channel of authorised independent providers guarantees that an infrastructure of civic monitoring does not depend on decisions taken by those it monitors.

The second precondition, and the decisive one, is the maturity of irreversible cryptographic hashing. Modern digital engineering makes it possible to separate the result of authenticating a person from the storage of that person's judgment, converting personal data into a depersonalised code. As a result, any outside observer may see that the right of judgment has been exercised by one of the verified citizens, and may see the judgment itself, yet no one in the world is technically able to establish who rendered it. The verifiability of the participant and the anonymity of the judgment coexist for the first time within a single system, without contradicting one another.

It is this convergence of two new qualities – the maturity of a social need and the maturity of technology – that determines the historical singularity of the moment for the introduction of a new social practice. An acute demand for the overcoming of the accountability deficits has for the first time acquired an adequate technological foundation, which makes the attempt not premature but timely.

1.6 Public Legitimacy Analytics as a New Category of Data and a Business Model

Supplementing the familiar practices of democracy with an institution of monitoring public legitimacy carries Teisond beyond the bounds both of human rights activism and of a purely technological project. It founds a fundamentally new social category, scientific and commercial at once: Public Legitimacy Analytics (PLA). The joining of these two properties gives the institution a double footing: the scientific character of the methodology secures trust in the data it generates, and the market value of those data as an information product secures its economic self-sufficiency.

1.6.1 PLA as a New Category of Data

The sociology of public opinion records the opinion of society in occasional isolated snapshots, concerning the summit of the political class, from one poll to the next. Digital services, state and commercial alike, generate colossal volumes of data without interruption, but the attitude of society towards power is the subject of interest of none of them, appearing in those volumes at most as an

incidental trace: by accident, dispersed and unstructured. The function of continuous public monitoring of the legitimacy of power remains vacant.

It is this function that the category of PLA assumes, presenting to society and to the market, for the first time, the current state of the legitimacy of power – a quantity until now merely presumed from the fact of election or appointment – across the whole vertical of governance, in the form of quantified and continuously updated bodies of data.

The substantive core of the category is the structuring of civic judgment. The Platform aggregates the attitudes of citizens towards a particular official, the object of monitoring within that person's exercise of official powers, relating each judgment to the office and each computed indicator to the moment of its computation. Individual binary judgments of verified citizens are thereby converted into living indices, computed under a single methodology, and from those into derivative mathematical trends and comparisons: between individual officials of equal standing, between levels of governance, and between periods of time.

The resulting analytical products are indices of differing depth of detail: the national officials' legitimacy index (NOLI), detailed scorecards of individual officials (OPLS), and indicators of reputational anomaly. These metrics yield a statistical snapshot of the legitimacy of the administrative apparatus at any depth, from the head of government to the head of a district inspectorate, making visible the attitude of society towards power where until now no one has measured it, neither for the highest leadership of the state nor for municipal bodies.

Teisond's information products open a distinct segment within a long-established market, that of sociological polling: a segment of new demand and of new consumer value, as yet without competition. This market space has had no opportunity to form until now, and not through anyone's oversight: what was missing was the conceptual frame in which the legitimacy of power might be conceived as a measurable quantity. Without the frame there was no category of data; without the data their value remained invisible; without visible value no demand could arise. The Platform breaks this circle from the side of supply: first the frame, then the data, and only then the market. Positioning within the polling market is, however, no more than the commercial projection of the social values the Platform creates. In parallel, as an emergent consequence of the operation of a newly created information channel, an additional form of social capital takes shape: mutual visibility, recognition, and a lowering of the tension of conflict between society and power.

1.6.2 The Value Proposition for Citizens

The Teisond Platform does not urge citizens to the discharge of civic duties of one kind or another, and does not rely on any inherent social conscience on their part. What makes the Platform viable is a proposition of value that meets a set of personal psychological needs of the individual user: the needs for recognition, for self-respect, for a rise in social standing and self-esteem, but above all for the restoration of dignity and of capacity to act in dealings with the holders of power.

When officials at the higher levels of power act at variance with citizens' notions of the common good, of public benefit or of justice, and when the representatives of the lower circles of public administration display self-interest, incompetence, legal ignorance or contempt, the citizen is seized by a particular mixture of feelings: frustration, helplessness and humiliation.

When every means of response, resistance or defence known to a person is either unavailable or ineffective, that mixture of feelings destroys psychological stability while at the same time provoking an acute need to find some means of compensation. It is on the notional market of products meeting needs of this character, in a segment of it that has not existed until now, that the consumer finds the Teisond proposition: an immediate, free and anonymous opportunity to act, to respond with a judgment that becomes part of a public signal.

The need is thereby met through a mechanism that allows a citizen's personal experience not to remain invisible. Capacity to act is restored without confrontation, without organisation, without public deanonymisation, and the psychological reward is specific and immediate: I was not helpless.

1.6.3 The Value Proposition for Officials

The resilience and self-sufficiency of an infrastructure of democratic accountability, and of the corresponding social institution, rest on every category of participant deriving value from taking part in its operation, whatever social stratum they come from and whatever role they occupy. For the participant who holds office, that value likewise makes no appeal to virtue – to openness, to accountability, to service – but addresses the concrete professional and psychological needs of an individual exercising public power.

The motivation of an official as a potential user of the Platform operates first of all at a purely psychological level. For any person vested with political or administrative authority it is an imperative to keep watch over the state of the environment subject to that authority, over one's own sphere of electoral interest, and over current sentiment and the events that shape it. Beyond that, the awareness on the part of a holder of power that something is taking place in the public space outside that person's attention, something with the potential to bear upon their standing yet not under their control, makes indifference to such a situation psychologically untenable. The motivating effect of watching the indicators of one's own public position arises almost automatically, whatever the details of the argument.

As to the particular needs of a holder of power that the Platform meets, the first of them is the need for reliable feedback. An official at any level operates in a deep information vacuum as to the actual attitude of those subject to their authority: opinion polling is not practised beyond a few dozen leading politicians; internal departmental channels of feedback filter the civic signal, carrying upward for the most part what those above wish to hear; and social networks produce unstructured emotional noise of little informational content, whose relevance is negligible or nil. Civic monitoring of legitimacy is very nearly the only information channel that delivers to an official an unfiltered, verified and continuous signal about how their authority is perceived by those over whom it is exercised.

The second is the need for a public representation of one's own. The right of reply gives an official a channel of official presence alongside their own index: official explanations placed without the mediation of the media, in the same plane of public visibility in which their reputational capital is formed.

The third need arises from challenges of a professional character. The competitiveness of the environment described above turns ignorance of one's own indicator into administrative blindness by choice: an official who does not watch their index is left uninformed of circumstances known to every professional observer, opponents, colleagues and journalists included.

A particular mark of this set of value propositions is its universality across the whole vertical of governance. The motivations of a prime minister and of the head of a secondary school are identical here: both hold public office, both carry a personal reputation on which their careers depend, and both have until now had access to no source of information whatever as to the actual state of that reputation.

The existence of the Platform creates a new risk for an official: what could previously only be guessed at becomes publicly manifest. At first sight this is a pure threat, yet the source of the risk is not the appearance of public judgment – that has always existed – but only its acquiring a visible and measurable form. In these circumstances the value of the Teisond proposition is plain: an unstructured threat, dispersed and unmeasurable, cannot be managed in principle, whereas a

measurable parameter can; and the Platform's function in relation to an official becomes not an instrument of pressure but an instrument of professional self-management.

1.6.4 The Business Model

Participation in monitoring is free for citizens by definition, since the exchange of value between the Platform and its user takes place in the plane of meeting that user's personal social and psychological needs. The commercial potential of the Teisond model lies outside that exchange: the Platform's revenue is formed where the results of processing the body of civic judgment acquire professional value for other categories of user.

The business model of Teisond is built on the foundation of a Crowdsourced Measurement Platform. The Platform does not connect users, affords the parties to the exchange no means of direct interaction with one another, and does not act as an intermediary in that exchange. Using the information data received from one category of user, it instead creates value in the sphere of public communication by processing those data, analytically and synthetically, into structured and useful information. The judgments of individual citizen users do not reach users of other categories in their original form: they dissolve into aggregates, and what becomes the consumer product is an index computed under a single methodology and authored by the Platform itself. The participant in monitoring and the object of monitoring do not meet in this construction, do not come to terms and do not choose one another; the anonymity of participation excludes it architecturally.

The Platform's information products are distributed at two levels of access. The first, the public level, discharges the Platform's mission as the embodiment of an institution monitoring the public legitimacy of power. At this level the information is open to all visitors without any need to register, and comprises the current index of legitimacy of every official who has passed the publication threshold, notice of the threshold where judgments are as yet insufficient, and the full methodology of monitoring. The second, the analytical level, is paid, and contains the absolute indicators of trust and distrust, metrics of consensus, the dynamics and direction of movement of indicators over time, confidence intervals, historical series, comparisons between officials at the same level of governance, and indicators of reputational anomaly. The boundary between the levels follows from the principle that public information is self-sufficient and carries a social value of its own, and that everything relating public data to detailed indicators concerning objects of monitoring belongs to the analytical level, that is, to the results of the analytical and synthetic processing of primary data as the Platform's commercial product.

The Platform's primary source of revenue is officials' subscriptions to data at the analytical level, generated continuously by the Platform from the body of citizens' judgments concerning the subscription holder. In the subscription relationship the official is a client of the Platform, but what is purchased is neither presence in the system nor an opportunity for self-positioning: it is detailed current information about one's own public position. The price of a subscription is fixed by level of authority, from the lowest for officials of local rank to the highest for the leading officers of the state, and depends neither on the number of judgments recorded by the Platform nor on the level of the indicators of legitimacy; within each level it is calibrated to the economic conditions of the jurisdiction. This structure of pricing removes any connection between the activity of citizens in rendering judgments and the economic advantage of the Platform, while keeping the price of access acceptable to an official of any rank.

Secondary revenue the Platform generates from several further categories of subscriber, each guided by motivations of its own for obtaining access to data at the same analytical level, but concerning all serving officials of the country, for professional purposes (Data Access). The value proposition for the media is a saving on sources and a standing editorial resource. Academic institutions and policy development organisations obtain access to aggregated data sets for research, and in doing so constitute PLA as a field of study in its own right. Political consultancies, public relations agencies and the analytical divisions of institutions and corporations use indices of

legitimacy as inputs to their own advisory work: the development of strategy, the mapping of stakeholders, the assessment of institutional risk. Revenue from this segment of users grows to the extent that the Platform's data become a standard point of reference in the ecosystem of political analytics.

A distinct feature of the Teisond Platform is a high potential for network growth in the value of the proposition, for each new user and each current one, as the total number of users increases. Each category of user consumes the result of the activity of another, and value accordingly grows on both sides, though in somewhat different ways: a wider circle of participants in monitoring raises the statistical weight of the data, while the attention of power increases the point of civic participation. The wider the circle of citizens rendering judgments, the more precise the index and the deeper the analytics received by the client segments. And conversely: the more officials who watch their own public position and make use of the right of reply, the more palpable to the citizen is the thing for which that citizen is in the system – the addressee of the judgment observes and responds. The first flow of data feeds the commercial value of the product, the second the social value of participation. No transactions take place between the parties, yet each of them contributes to raising the value of the Platform for its counterpart.

The global Teisond project is deployed on a model of multi-tenant centralised architecture: all jurisdictions are served by a single body of software code, and national specificity is set by a separate configuration package of data. Launching a national Teisond platform in a new country requires neither local infrastructure nor local personnel; all that is needed is integration with one or more existing local systems of verification. The marginal cost of each successive country in the Teisond network – the additional outlay on its launch over and above the common base – accordingly reduces for the most part to the one-off population of a national database of officials, the creation of a configuration file, and the activation of identity verification for the jurisdiction concerned. Aggregate costs grow substantially more slowly than coverage, and unit economics improve with every expansion.

A number of common sources of revenue are excluded from the Teisond model deliberately, not as a declaration of intent open to later revision but as a structural constraint of architecture and governance. Advertising in any form is excluded, since it generates incentives to maximise engagement at the expense of adherence to methodology. The transfer of user data to third parties is excluded architecturally: data that could be transferred the Platform neither accumulates nor stores – neither citizen profiles nor individual judgments in any form fit for export. Political consultancy and campaign support services are not permitted, as incompatible with the imperative of neutrality that secures the worth of the core information product. Nor does the model provide for dependence on public budgets or grant programmes: financial self-sufficiency is built into its foundation.

The common denominator of the whole model is the independence of the measurement of legitimacy from the commercial side of relations between the Platform and its participants: neither an official's subscription nor the purchase of a Data Access package has any effect whatever on the Platform's methodology, and neither carries any right to intervene in the collection, computation or publication of data.

1.6.5 Mission and Model as One

Every link of the construction described composes a single circuit. The deficit of feedback between power and society gives rise to a social need; the need is met through mass participation; participation generates data of a new category; the market value of the data funds the infrastructure of collection, storage and processing; and the infrastructure sustains the existence of the institution that meets the need. Social mission and business model do not here coexist in compromise – they constitute a single mechanism, examined above from different sides.

1.7 A Universal Mission, a Disciplined Execution

The social disproportion that Teisond removes is not unique to any one country: wherever officials exercise continuous power without being burdened by mechanisms of continuous accountability, the same structural gap exists, and with it the same space for an institution to fill it. The model of the Teisond Platform is accordingly suited to any consolidated democracy in the world, and adapts readily to national specificity by virtue of a single methodology, a single architecture, and the software configuration of local parameters.

The universality of the mission does not, however, imply indiscriminacy in the directions of the Teisond network's expansion. The set of jurisdictions in which the Platform may be deployed is not determined by any settled list, nor established at anyone's administrative discretion: the stated criterion is the mark of a consolidated democracy under the classification of the independent international institutions Freedom House and V-Dem. It is this criterion that answers the question of any given country's prospects of joining the Teisond network, and that makes the geography of its expansion transparently predictable. The current composition of the network's jurisdictions is shown directly on teisond.com; the White Paper deliberately does not fix it, given the dynamics of the network's development.

The Teisond project is not announced – it operates. Every jurisdiction of the current set has a national presence; full activation of the national platform is complete in some and, in others, at the stage of assembling the local databases of the objects of monitoring, the one component of deployment that takes time. The multi-tenant architecture of the Teisond network radically simplifies the connection of a new country at the entry level, and the period for a further jurisdiction to join the operating network amounts to a matter of days. The pace of expansion is limited solely by the operational readiness of the national databases, and not by technical capacity, financial cycles or any need to assess consumer demand: a social institution of this kind forms its environment by the very fact of its presence in the public space.

A single network under a single operator is the base model for realising the Teisond mission, but not the only possible one. For jurisdictions whose interested representatives seek full autonomy, the Teisond standard may be reproduced in the form of a self-standing national platform, with the same architecture, the same software code and the same methodology, but under local management of its own. This form of national realisation of the project is possible on franchise terms, in compliance with the Teisond standards, which guarantee the comparability of indices and the inviolability of the methodology irrespective of the form of management. For either of the two models named, one and the same formula holds: the mission is universal, the execution disciplined.

The sections that follow set out how the construction of the Platform is arranged: the conceptual and methodological foundations of measuring the level of legitimacy, the technical architecture of the Platform, the operational model of deployment, the legal structure, governance, and the long-term vision of the acquisition of ownership rights over the infrastructure by its users.

SECTION 2: CONCEPT AND METHODOLOGY

2.1 Core Concept: Legitimacy as Continuous Variable

2.1.1 Rethinking Political Legitimacy

Political legitimacy – the recognition by citizens that those exercising governmental authority do so rightfully – has traditionally been treated as a binary attribute: a government either possesses legitimacy or it does not. Elections serve as the mechanism for conferring this status, and between elections, legitimacy is presumed until the next electoral test.

This binary treatment misrepresents the phenomenon it describes. Legitimacy is not a fixed status conferred at a moment in time but a state that is acquired, maintained and lost: a continuous, dynamic relationship between the governed and those who govern. Every dealing between a citizen and an official either reinforces trust or erodes it. A mayor who responds openly to a local crisis strengthens legitimacy; one who evades accountability weakens it. These micro-interactions accumulate into a collective sentiment that shifts without interruption, while traditional measurement reaches it only at long intervals, and only at the summit of the political class.

Teisond reconceives legitimacy along three axes. First, legitimacy is subjective and personal: it exists in the judgment of individual citizens, not as an objective property of an institution. There is no legitimacy by definition; there is only the aggregate of individual judgments of trust. Second, legitimacy is continuously variable: it moves in response to the actions of officials, to the outcomes of policy, to personal experience and to exposure to information. Third, legitimacy is measurable: defined as the aggregated trust of citizens towards particular officials, it can be captured, quantified and published through the appropriate infrastructure.

This reconceptualisation has practical consequences. If legitimacy is binary, measurement is unnecessary – elections suffice. If legitimacy is continuous, measurement becomes essential – societies need instruments tracking how legitimacy evolves continuously, across the full spectrum of officials exercising authority – including the vast majority who never face elections at all. The Platform provides this instrument.

2.1.2 Legitimacy as "Currency of Expectations"

Legitimacy functions as a currency of expectations between citizens and officials. Citizens "invest" expectations in officials through the act of delegating authority. Officials "spend" this currency through their decisions and conduct. Fair, competent governance maintains or increases the balance. Corruption, incompetence, or dismissiveness depletes it.

Unlike financial currency, legitimacy currency has no central bank controlling supply. Each citizen holds their own reserve of expectations and distributes trust independently. The Platform makes this distributed currency visible by aggregating individual assessments into public indices –

creating, for the first time, a transparent "exchange rate" between citizen expectations and their acceptance of how authority is exercised.

This framing has practical implications for officials: legitimacy is not an inexhaustible resource. Officials who consistently deplete citizen trust face declining indices visible to voters, supervisors, media, and peers. The Platform does not create this dynamic – it makes it measurable and visible.

2.1.3 From Episodic Sampling to Continuous Census

Traditional political measurement relies on episodic sampling: polling organisations survey 1,000–2,000 respondents at intervals of weeks or months, extrapolating to populations of millions. This captures roughly 0.001–0.01% of the population per survey and covers only a few dozen high-profile figures.

Teisond inverts this model. Rather than sampling a fraction of citizens about a fraction of officials, the Platform enables the entire verified citizenry to judge any official at any time. If participation reaches even a fraction of the voting population, the resulting dataset dwarfs any polling sample – and covers tens of thousands of officials across all levels of authority rather than a few dozen high-profile figures. Updates are continuous rather than periodic, identity verification ensures data integrity impossible in anonymous polling, and the marginal cost of additional participants and officials approaches zero once infrastructure exists.

This is not an incremental improvement upon the methodology of polling but a categorical shift: from episodic sampling to a continuous census of expressed civic judgment.

2.1.4 Early Warning System and Accountability Between Elections

Continuous legitimacy measurement creates an early warning system for democratic governance. Gradual erosion of an official's legitimacy index signals emerging problems before they escalate into crises. A mayor whose trust index declines steadily over several months receives a clear signal that citizen confidence is eroding – providing opportunity for course correction rather than discovering the problem only at the next election.

For appointed officials who never face elections, this early warning function is even more critical. A regional administrator whose legitimacy index shows persistent decline generates a signal visible to supervisors, media, and the public – creating accountability pressure where no structured mechanism existed before.

The Platform thus addresses a structural absence in democratic accountability: elected officials govern without structured feedback between elections, and appointed officials – the vast majority of those exercising governmental authority – operate without any such feedback at all.

2.1.5 Limitations and What Legitimacy Indices Don't Measure

Legitimacy indices measure expressed citizen trust, not objective governance quality. High legitimacy does not guarantee competent governance; low legitimacy does not prove incompetence. Popular officials may implement destructive policies while maintaining public support; competent officials making difficult decisions may face low indices.

Indices reflect participating citizens, not the entire population. If participation is unevenly distributed, indices may overrepresent certain demographics. The Platform mitigates this through transparency: every index is published only above a minimum threshold, and its sample size and confidence interval are available in the subscriber analytical layer, so that readers can assess the statistical reliability of the data they are interpreting.

Indices capture direction (trust/distrust) but not reasoning. A citizen distrusting an official due to corruption and one distrusting due to policy disagreement register identically. The Platform measures what citizens express, not why – leaving interpretation to the democratic ecosystem of media, researchers, and public discourse.

These limitations are inherent in any measurement system and are disclosed transparently rather than concealed. The Platform provides information; democratic institutions and citizens determine its significance.

2.2 Objects of Monitoring

2.2.1 Inclusion Principle and Definition

Teisond monitors individuals holding governmental authority – those making decisions that affect citizens' lives and claiming to act on citizens' behalf. The inclusion principle is universal: any person authorised to make decisions obligatory for others to implement in governmental capacity. This definition captures the essence of governmental authority: the power to impose binding decisions on others. Whether that authority derives from election, appointment, professional qualification, or administrative hierarchy, if an individual exercises it on behalf of government, they become an appropriate subject for citizen judgment. This principle is the Platform's core criterion, distinguishing it from all existing accountability mechanisms.

The definition excludes individuals who do not exercise governmental authority regardless of their public influence. Business leaders, activists, and public figures may shape public discourse but do not make decisions binding on others in a governmental capacity. Career civil servants who implement policies established by others – without discretionary decision-making authority of their own – fall outside the scope for the same reason.

Certain categories of official who do hold governmental authority require additional safeguards to protect institutional independence. Judicial officers, for example, fall within the monitoring framework because they exercise binding authority over citizens, but the Platform draws a clear boundary between measuring the confidence of citizens in the person holding a mandate and creating pressure upon particular rulings. The safeguards applicable to judicial and other independence-sensitive positions are described in the Note on judicial monitoring (§2.2).

2.2.2 Four Levels of Governmental Authority

Every jurisdiction has an institutional structure of its own, federal or unitary, centralised or devolved, with differing numbers of administrative tiers, but the underlying pattern of governmental authority is universal. The Platform accommodates this diversity through configuration specific to each country (§5.3.1) rather than through structural redesign: the same methodology, the same architecture of privacy and the same standards of publication apply to every political system.

The Platform identifies four levels of governmental authority, each containing officials whose decisions bind citizens. The levels reflect organisational structure and jurisdictional scope, not importance or any hierarchy of accountability. A municipal planning officer exercises authority over the lives of citizens just as surely as a cabinet minister: the scope differs, individual permits against national policy, but the principle of accountability applies equally.

In a democracy of average size the number of officials exercising governmental authority across all four levels runs to the hundreds of thousands. Traditional political monitoring typically reaches a few dozen high-profile elected figures per country. The Platform extends the infrastructure of accountability to officials operating at every level of governmental administration. Network-wide totals are a function of the current composition of jurisdictions and are published on teisond.com. The revenue implications of this scope, and why officials at every level become natural subscribers, are described in Section 4.

2.2.3 Level 1: National Authority

National-level officials exercise authority affecting the entire country's population – broad policy, national legislation, executive action, and institutional direction. This level encompasses heads of state and government, cabinet ministers and junior ministers, members of national legislatures, senior political appointees heading major agencies, and – where appointments are political – supreme or constitutional court justices and heads of regulatory bodies.

A typical consolidated democracy has between 250 and 800 officials at national level. These are the political actors of the highest visibility, and the only tier covered by national polling, by the major media and by traditional political monitoring. The Platform supplements that existing ecosystem with continuous rather than episodic measurement. A detailed breakdown of Level 1 positions and estimated counts is provided in Appendix E.

2.2.4 Level 2: Regional Authority

Regional officials exercise authority over provinces, states, autonomous regions or other first-tier administrative subdivisions. The scope of regional authority varies considerably from one jurisdiction to another. Federal systems have strong regional governments with substantial legislative and executive powers; quasi-federal systems grant significant devolved autonomy; unitary centralised systems maintain a regional administration that principally implements national policy. This level takes in regional heads of government, regional legislators, and senior administrators at the provincial or intermediate tier where such a tier exists.

A typical consolidated democracy has 400–2,500 regional officials, with federal systems at the higher end. Regional officials occupy a middle visibility tier – they receive coverage in regional media and face some polling before elections, but systematic continuous monitoring rarely extends comprehensively to this level. The Platform closes this gap. A detailed breakdown is provided in Appendix E.

2.2.5 Level 3: Municipal Authority

Municipal officials exercise authority over cities, towns and local administrative units. This level shows the greatest structural variation of all, ranging from jurisdictions with fewer than a hundred consolidated municipalities to those with tens of thousands of communes, but the principle is

uniform: mayors, municipal councillors and senior municipal administrators take binding decisions affecting the daily lives of citizens.

The accountability deficit is sharpest at this level. Media coverage and political analysis typically reach perhaps 50 to 200 prominent mayors nationally. For the remaining thousands of municipal leaders, and the tens of thousands of councillors, no continuous mechanism of accountability exists between elections. They exercise governmental authority while operating outside any structured public scrutiny. A typical mid-sized democracy has between 25,000 and 80,000 municipal officials. The Platform adapts to the municipal structure of each country through configuration, not through changes of code. A detailed breakdown is provided in Appendix E.

2.2.6 Level 4: Local Officials and Appointed Administrators

This level represents the Platform's most significant innovation: creating accountability infrastructure for officials who previously operated with virtually none beyond internal institutional processes. Level 4 encompasses officials exercising direct authority over citizens in daily life – school principals, police chiefs, building inspectors, hospital directors, social services supervisors, tax office directors, court judges, and administrators across every sector where governmental decisions affect individual citizens more immediately than abstract policy debates.

The scale is substantial: a typical mid-sized democracy has between 50,000 and 150,000 officials at Level 4, by a wide margin the largest category. These officials are largely invisible to traditional mechanisms of accountability. No polling organisation surveys the trust of citizens in a local building inspector; no media outlet tracks the legitimacy of a regional hospital director. Yet these are the officials whose decisions citizens experience most directly and most often.

Judicial officers are included at this level because they exercise governmental authority, but the Platform draws a clear boundary. An index of legitimacy for a judicial mandate measures the confidence of citizens in the person holding it, not agreement or disagreement with particular rulings. The Platform publishes no data at the level of individual cases and provides no mechanism for citizens to respond to individual decisions. Judicial independence remains paramount; monitoring measures public acceptance without creating instruments capable of influencing outcomes.

Database population for Level 4 begins with the operational team identifying officials from public records and government rosters, prioritising the most common citizen touchpoints: schools, police, building inspections, social services, hospitals, and tax offices. AI agents progressively expand coverage as the Platform scales. A detailed breakdown by sector is provided in Appendix E.

2.2.7 Implementation Approach

The scope of the MVP is defined by completeness at a given level of authority rather than by partial coverage across all of them. Teisond opens with a fully populated database of Level 1 officials (§2.2.3) in every active jurisdiction. This ensures that citizens in every country can begin rendering judgments on the officials of highest public visibility from the first day of operation. The database is populated in advance by the Platform's operational team from official government registries, parliamentary rosters and publicly available institutional records. Expansion to Levels 2 to 4 follows as national deployments mature and operational capacity allows, each level added only once the database for it meets the standards of completeness and accuracy across the jurisdiction concerned.

Once launched, the database is maintained through continuous monitoring of official sources: electoral results, government reshuffles, term expirations, and organisational changes are tracked and reflected in the database as they occur. Expansion toward comprehensive Level 2–4 coverage – potentially encompassing hundreds of thousands of officials per country – is driven by AI agents that systematically identify and catalogue office-holders from public records, government rosters, and institutional directories. This automation is what makes coverage at all four authority levels across every jurisdiction operationally feasible without proportional growth in team size.

2.2.8 Exclusions and Boundary Cases

The exclusion of private citizens and career civil servants without decision-making authority is described in §2.2.1. Two further categories are clearly excluded: monarchs and ceremonial heads of state whose functions are constitutionally symbolic, and officials of international organisations who do not exercise authority within a national governmental framework.

Several boundary cases require case-by-case assessment. Semi-autonomous agencies are included where they exercise binding authority over citizens – a national energy regulator issuing mandatory compliance orders qualifies; a purely advisory economic council does not. Public university leaders are included because they administer publicly funded institutions with authority over students and staff; their counterparts at private universities are excluded. Professional associations are included only where they exercise delegated governmental authority with legal force – a bar association that controls admission to legal practice qualifies; an industry lobby group does not. Advisory bodies are excluded unless they hold enforcement authority. The treatment of judicial officials – included with specific independence safeguards – is addressed in §2.2.6.

The guiding principle across all boundary cases is consistent: does this person make decisions that citizens must obey? If yes, they are an appropriate subject for civic judgment. If they advise, recommend, or process without deciding, they are excluded.

2.3 Judgment Mechanism

2.3.1 The Binary Choice: Trust or Distrust

Citizens judge officials through a deliberately simple mechanism: trust or distrust, with neutrality expressed by not judging at all. The point is to keep the cognitive cost close to zero so anyone can participate within seconds, including right after an encounter with an official, without composing justifications or learning a rating rubric. This simplicity reflects how people naturally form judgments about authority in real life.

A binary input avoids false precision. Ten-point or multi-criteria scales look scientific but invite arbitrary distinctions (what really separates a "6" from a "7"?) and force hidden weighting schemes. A clear yes or no signal, aggregated at the level of the mandate and the calculation period, produces transparent percentage indices that the public, the media and officials can read consistently, with confidence intervals rather than spurious decimals.

Privacy improves when the Platform asks less. A single trust/distrust signal reveals minimal information about the person who submitted it; multi-dimensional ratings or written reasons would create richer profiles and greater risk of political-opinion exposure. Keeping inputs binary fits the aggregates-only design and helps meet data-protection expectations without sacrificing usefulness.

The binary choice does not flatten nuance. Citizens can trust some officials and distrust others; they can change or withdraw their current judgments as circumstances evolve. At the collective level, nuance emerges through movement over time and across offices: steady declines, sharp drops with recovery, or volatile trajectories all carry different meanings that a complex input scale does not magically improve.

In short: a small, human-scale action from each person becomes a clear, auditable public signal when aggregated – without over-engineering the input or over-exposing the individual.

2.3.2 What Is NOT Collected

The binary judgment mechanism is deliberately minimal not only in what it asks but in what the Platform retains. No reasons or justifications are collected. No intensity of feeling is measured. No policy-specific breakdowns, forced rankings, or demographic correlations are captured. No per-user judgment histories or behavioural profiles are derived. The Platform stores only the current state – citizen X currently trusts or distrusts official Y – and nothing more.

This minimisation is architectural, not merely a policy commitment. The database schema omits fields for the categories listed above; API endpoints cannot expose what does not exist; queries below publication thresholds are rejected. Even in a hypothetical data breach, there is no trove of personal political opinions to extract – because the Platform never collected them. The canonical list of excluded data categories and the enforcement mechanisms that make this irreversible are described in §5.4.7; publication thresholds in §5.4.8; and API access controls in §5.4.10.

2.3.3 User Actions and Constraints

The Platform offers three actions to every verified citizen. A citizen may render an initial judgment, trust or distrust, in respect of any mandate in the database. A citizen may change that judgment as their assessment evolves, moving from trust to distrust or the reverse. And a citizen may withdraw a judgment entirely, returning to neutrality and removing their input from the aggregate. Participation is voluntary and self-directed: a citizen may judge many officials or only a few, and may register without judging anyone at all.

A judgment, once rendered, is perpetual. It stands until the citizen changes or withdraws it, or until the mandate closes. It is bound to no period, it does not expire, and it does not age: the moment at which a judgment was rendered is not a parameter of the act and carries no weight in any computation. A change overwrites the existing record rather than adding to it, and a withdrawal deletes it; the Platform therefore holds no history of positions as a class of data at all.

Three constraints protect the integrity of the signal. Each citizen holds one standing judgment per mandate, trust or distrust, with no mechanism for multiple simultaneous positions; neutrality is not a third position but the absence of a record. Judgments cannot be delegated to a party, an influencer or an organisation; each judgment is an individual act, which prevents organised influence-trading and mass delegation. And no bulk operations exist: there is no mechanism to apply a single judgment across a group of officials, so that every input reflects a deliberate individual assessment.

Rate-limiting mechanisms constrain how frequently a citizen can change a judgment for any given official, preventing rapid toggling that would add noise rather than signal. The specific parameters of these controls are not published, consistent with the anti-manipulation disclosure policy described in §5.4.11.

2.3.4 The Role of Neutrality

Every citizen begins in a neutral state towards every mandate. Neutrality means only that no judgment has been rendered, and it carries no signal, positive or negative. A citizen may be neutral because they lack information about an official, because they have had no dealings with that office, or because they have deliberately chosen to abstain. The Platform does not interpret silence. Indices are computed from standing judgments alone: if a mandate has accumulated 10,000 judgments of trust and 5,000 of distrust, the index stands at 66.7, irrespective of how many registered citizens have not judged that mandate. Non-participants are excluded from the denominator entirely.

This design reflects a methodological principle: treating silence as a signal would inject noise into every index. No citizen can meaningfully track thousands of officials, and requiring blanket judgments would produce arbitrary inputs rather than genuine assessments. The Platform measures explicit, voluntary acts of civic judgment – trust or distrust – and nothing else. Neutrality is both a right and a quality safeguard: it preserves citizen autonomy, protects data integrity, and ensures that every published index reflects intentional expression rather than assumptions about what silence might mean.

2.4 Legitimacy Index Calculation

2.4.1 Basic Formula

For each mandate the Platform maintains two live counters: the number of verified citizens whose standing judgment is trust (TI) and the number whose standing judgment is distrust (DI). These are integers, and they move as citizens render, change and withdraw judgments. No per-user histories are stored. The Legitimacy Ratio (LR) is the share of trust among all standing judgments, scaled to 0–100: $LR = TI / (TI + DI) \times 100$. The Distrust Ratio is the simple complement, $100 - LR$. Both figures are displayed together to aid interpretation. Citizens who have rendered no judgment, or who have withdrawn one, enter neither counter and do not affect the denominator; the ratio reflects the balance of expressed trust against distrust among those who chose to judge (§2.3.4).

The index is a snapshot. It is computed from all standing judgments on a mandate at the moment of a scheduled calculation, and it is that snapshot which is published. Calculation occurs at a cadence set as a parameter of each jurisdiction. Between calculations the published value does not move, and it does not move for the reason that might be assumed: not because the figure refers to some period of time, but because the next snapshot has not yet been taken. The period is a dimension of the publication of an index, never a property of a judgment. The unit of publication is accordingly the mandate together with the calculation period, and outside the Platform no operation at the level of an individual judgment exists as a class.

The snapshot is taken irrespective of the publication threshold; the threshold governs visibility alone. An index is published once a set number of standing judgments has accumulated. Before that point the profile publishes the progress of accumulation, the number of standing judgments recorded and the threshold to be reached, but not the ratio; below a minimum of counter visibility, also a parameter of the jurisdiction, the profile shows only a neutral state of collection in progress. The moment an index opens is a public event. Thresholds are differentiated by level of authority and, like the counter visibility minimum, are parameters of jurisdiction configuration rather than constants of the methodology. The full publication policy, including k-anonymity requirements and threshold enforcement, is described in §5.4.8–5.4.9.

LR is a privacy-preserving measure of the current public acceptance of a person exercising authority under a given mandate. It is not a measure of job performance, of policy wisdom or of legal validity, and it is not an election forecast. The published figure is accompanied by any applicable transparency notes; the confidence interval and the sample size behind it belong to the analytical level (§5.4.9).

2.4.2 Confidence Intervals and Sample Size

For every published Legitimacy Ratio the Platform computes a 95% confidence interval, provided to subscribers as part of the analytical layer (§5.4.9). The interval reflects statistical uncertainty and depends on both the observed ratio and the sample size n (where $n = TI + DI$). Larger samples narrow the interval; smaller samples widen it.

For calculation purposes, the trust proportion is expressed as $p = TI/n$ (a decimal between 0 and 1), then scaled to the 0–100 display format. For mid-range proportions and sufficiently large samples, the 95% confidence interval uses the normal approximation: $CI_{95} = p \pm 1.96 \sqrt{p(1-p)/n}$. When n is small or p lies near 0 or 1, the Platform uses Wilson intervals, which remain well-calibrated at boundaries where the normal approximation breaks down. To illustrate: for an official with 1,550 trust and 950 distrust judgments ($n = 2,500$), $LR = 62.0$ and the 95% CI is approximately 60.1–63.9. An official with only 120 total judgments and a near-even split would show a much wider interval – roughly ± 9 percentage points – signalling that the index has not yet stabilised.

The Legitimacy Ratio is displayed to one decimal place and the confidence interval bounds likewise, which avoids false precision. Where the number of standing judgments has not yet reached the threshold for the level of authority concerned, no ratio is displayed and the profile shows the progress of accumulation instead. Overlapping confidence intervals between two officials signal that an apparent difference may be statistical noise rather than meaningful divergence, a point the Platform makes visible through its presentation design.

2.4.3 Snapshots, Series and Trend Analysis

A sequence of snapshots forms a historical series, and it is the comparison of snapshots over time that yields the dynamics of an index. The Platform preserves every computed value for longitudinal analysis, and displays the current snapshot distinctly from the historical curve, so that the latest value is unmistakable without the loss of trajectory.

Trailing horizons, a 7-day short horizon and a 30-day default horizon, are instruments of trend analytics and nothing else. Trend indicators are computed from the series of snapshots and never from judgments directly. They are not a method of computing the index itself, they do not filter judgments, and they introduce no ageing: a judgment rendered years ago carries exactly the weight of one rendered this morning, for as long as it stands. Where the series of snapshots does not yet reach the depth of a horizon, the corresponding indicator is not formed at all rather than being estimated from a shorter run of data. It follows that the cadence of calculation must be more frequent than the shortest trailing horizon in use, since no trend can be derived from a series sparser than its own window.

Publication thresholds apply to every plotted point: only above-threshold snapshots appear on a curve, and sub-threshold intervals show the progress of accumulation. Each historical point carries uncertainty consistent with the confidence interval computed for it.

When a material recalculation or a correction of methodology occurs, the historical record is versioned and accompanied by a dated public note explaining what changed and why. No historical

value is silently revised. This discipline of versioning ensures that any reader, whether journalist, researcher or official, can reconstruct the history of an index in full and verify that data cited at an earlier date have not been altered retroactively.

2.4.4 Comparative Metrics

A single index gains meaning in context. The Platform supports four comparative lenses: peer comparison (mandates of the same type, all cabinet ministers, all mayors in a region), geographic comparison (mandates across regions within a country, surfacing territorial patterns), temporal comparison (the trajectory of a single mandate over time), and institutional comparison (aggregated averages for departments, agencies or levels of authority, revealing systemic strengths and weaknesses). Cross-jurisdiction benchmarking, comparing equivalent roles across countries, is possible but calls for careful interpretation given differences in political culture and rates of participation. In every case comparisons display sample sizes and confidence intervals, and mandates below their publication threshold are excluded from comparison until that threshold is met.

2.4.5 Handling Edge Cases and Anomalies

The Platform favours disclosure over suppression. When anomalies are detected – coordinated campaigns, sudden volume spikes, or statistically improbable patterns – the index continues to be published but is accompanied by a visible flag and a plain-language transparency note. The detection framework and governance principles behind this approach are described in §5.4.11. No index is silently removed or adjusted; readers always see both the data and the context needed to interpret it.

The Platform also handles the lifecycle of the mandates it monitors. A newly opened mandate may show a volatile index while the body of judgment builds; results are published only once the threshold is met, and early above-threshold snapshots are marked as preliminary. When a mandate closes, whether through resignation, the expiry of a term or electoral defeat, the judgments rendered on it cease to stand, no further judgments are accepted, and the counters of the successor mandate start from zero: the assessment of a predecessor is never carried across to a successor. The historical series of the closed mandate is preserved and belongs to the analytical level. Where a single individual holds distinct positions each carrying separate authority, each is a separate mandate with an index of its own, and trust in one role is measured independently of trust in another. A change of party affiliation or of personal name does not reset an index, since the mandate is unchanged: the person and the office are the same.

2.5 Citizen Value Proposition: The Psychology of Participation

2.5.1 The Participation Paradox

Democratic theory assumes engaged citizens keeping continuous watch over governmental authority. Reality diverges sharply. In established democracies most citizens show minimal political engagement outside electoral campaigns: they cannot name their representatives, they rarely follow proceedings, and they invest virtually no time in tracking what officials do.

Traditional civic technology initiatives have repeatedly attempted to bridge this gap – parliamentary monitoring platforms, petition systems, civic complaint mechanisms – yet struggle to achieve sustained mass engagement. The pattern repeats: initial enthusiasm, modest early adoption, gradual decline into niche usage by politically hyperactive minorities. The failure stems from fundamental misunderstanding of user motivation: most civic technology treats political participation as moral obligation, appealing to civic duty and democratic responsibility. These appeals prove insufficient against platforms engineered to deliver immediate psychological rewards.

Anthony Downs's theory of "rational ignorance" explains why: the personal cost of becoming informed exceeds the marginal benefit of one voice among millions. Traditional civic platforms fail because they demand cognitive investment without offering commensurate individual return. The social benefit may be substantial, but individual incentive remains weak.

The participation paradox thus defined: democracy requires citizen engagement, yet citizens rationally decline to engage because individual costs exceed individual benefits. Any platform attempting to bridge the accountability vacuum must solve this paradox through genuine individual value creation, not stronger moral appeals.

2.5.2 The Need: Dignity, Agency, Voice

Every person who lives under governmental authority experiences a fundamental tension: others make decisions that bind them, yet they possess no routine mechanism to signal whether they accept that authority as legitimate. This is not a gap between elections – it is a permanent condition. Elections, where they occur, offer a single binary choice once every several years, covering only a fraction of the officials who exercise power. Appointed administrators – the officials citizens encounter most frequently and most directly – never face even this minimal test. The result is a chronic asymmetry: authority flows downward continuously, while the citizen's capacity to respond flows upward only in rare, episodic, and highly constrained moments.

This asymmetry frustrates one of the most basic of human needs. In Abraham Maslow's hierarchy, esteem needs occupy the level above safety and belonging, and in consolidated democracies, where institutional infrastructure broadly secures those lower tiers, esteem needs become an active motivator for large segments of the population. Esteem operates on two axes. Internal esteem, meaning self-respect, capacity to act, and the sense that one's judgment matters, is threatened whenever a person feels powerless or insignificant in the face of authority. External esteem, meaning recognition, social standing, and the knowledge that others see and hear you, is threatened when no channel exists for expressing that judgment visibly. Governmental authority, exercised daily without structured feedback, frustrates both. The citizen is not merely uninformed or disengaged; the citizen has no instrument through which engagement could take meaningful form.

2.5.3 The Product: From Need to Market

This is the need the Platform addresses, not as a civic obligation but as a consumer product delivering individual psychological value. Participation on Teisond is a small action at negligible cost, a single judgment of trust or distrust, and it produces a result that is both immediate and durable: the judgment enters the standing body from which the official's index is computed, and it remains there until the citizen decides otherwise. The citizen's voice becomes part of a public signal that officials, the media and peers can see. Internal esteem is restored through capacity to act, through the knowledge that one's judgment has been registered and counted. External esteem is restored through visibility, through the knowledge that the aggregated expression to which one has contributed is now a matter of public record. No existing instrument offers this combination.

Petitions collect signatures but produce no persistent signal. Opinion polls sample a fraction of the population and disappear after publication. Posts on social media generate noise without structured measurement. The Platform converts individual judgment into a continuous, measurable and publicly visible index, a mechanism that did not exist before. Participation is sustained by intrinsic motivation rather than artificial incentives: the Platform deliberately avoids gamification, meaning points, badges and rewards, because people who find an activity inherently meaningful continue it longer than people paid in tokens to perform it. Participation aligns with natural cycles of attention, a political scandal, an encounter with a bureaucracy, a report in the media, rather than demanding dedicated time or rituals of engagement.

The consumer of this product is any adult resident of a jurisdiction the Platform serves who has ever felt that their opinion of an official does not matter. This is not a niche audience of political activists; it is a general population whose esteem needs are routinely unmet by existing democratic infrastructure. Across the consolidated democracies the addressable population runs to hundreds of millions. The realistically addressable segment, meaning citizens motivated enough to complete identity verification and render at least one judgment, is estimated at 20 to 40 per cent of the adult population in active jurisdictions, a rate of penetration far exceeding that of any existing civic technology platform.

Teisond is, in this sense, a social enterprise operating through market mechanisms. The citizen's need for voice and recognition generates participation. Participation generates data. Data generates revenue from officials who subscribe to monitor their own indices (Section 4). Revenue sustains the infrastructure that serves the citizen's need. This cycle is self-reinforcing: the more citizens participate, the richer the data, the more valuable the product, the more sustainable the mission. The business model does not merely align with the social mission – it is structurally identical to it.

2.5.4 From Individual Motivation to Collective Accountability

Teisond's democratic value resides in no single judgment. It emerges from the aggregation of thousands of individual acts into a collective signal that neither any participant nor the Platform itself deliberately constructs. Each citizen judges an official for reasons of their own: frustration at an encounter with a bureaucracy, recognition of competent leadership, a need for voice. No individual judgment carries public weight on its own. But as judgments accumulate towards the publication threshold, the profile shows the progress of that accumulation, and once the threshold is crossed the index opens and becomes a continuously updated public signal. The transition is not gradual but threshold-based: the progress of accumulation is visible throughout, the ratio itself only once it is statistically sound, and then to everyone at once. The pattern is familiar from other domains: markets emerge from individual transactions, encyclopaedias from individual edits, electoral outcomes from individual preferences. The Platform applies the same logic of aggregation to the relationship between citizens and governmental authority, a space in which no equivalent mechanism currently exists.

The relationship between individual motivation and collective effect is reinforcing. As participation grows, indices become more statistically robust, which increases their public visibility, which increases officials' responsiveness, which demonstrates to citizens that participation matters, which motivates further participation. The individual act is identical at every stage of this cycle; its collective significance is transformed. What distinguishes this aggregation from existing mechanisms is the combination of four properties simultaneously: it is continuous (not episodic), verified (one citizen, one account), census-aspiring (not sampled), and citizen-initiated (not researcher-driven). The Platform's role is not to create accountability but to create the conditions under which accountability emerges from citizen behaviour that is individually motivated and collectively significant. The structural dynamics this produces – reciprocity, mutual accountability, systemic pressure – are examined in §2.9.

2.5.5 A New Channel Between Governing and Governed

The Platform does not appeal to idealistic motivations. It does not rely on civic consciousness, democratic duty, or altruism. Its reason for existence is simpler: to open a channel of information exchange between groups whose relationship has been structurally unidirectional. Governmental authority flows downward continuously – decisions, permits, refusals, regulations, enforcement. The reverse signal – how citizens perceive and judge those who exercise this authority – has no channel. It is not suppressed; it is architecturally absent. Elections offer a momentary, highly constrained valve; for appointed officials, no valve exists at all. The result is a latently conflictual relationship in which frustration accumulates without outlet, and officials operate without structured feedback from the people over whom they hold power.

Citizens participate because they want to be citizens, not subjects – to have a voice in a relationship where voice has been structurally denied. Officials engage because they are the interested recipients of what the Platform produces: a continuous, public signal of how their authority is perceived. Media process the Platform's data because they cannot afford to remain outside the social context it creates. Each participant in this information exchange acts from their own motivation. The cumulative effect is societal acceptance of a civic technology infrastructure that none of them individually set out to create or initiate.

Personal interests and societal interests need not conflict. The Platform, as a new social institution, generates value that exceeds any individual participant's intent: mutual recognition between governed and governing, a continuous legitimacy signal where none existed, and reduced tension in relationships that were previously one-directional and opaque. This added social capital – accountability, transparency, bilateral awareness – is not the Platform's direct function but the emergent consequence of an information channel that connects two groups whose exchange was, until now, blocked.

2.6 Anti-Manipulation Safeguards

Even with verified identity ensuring one citizen, one account, organised groups can coordinate legitimate users to express trust or distrust en masse. This is not fraud – all participants are real citizens with verified accounts – but organised mobilisation, a form of democratic participation no different in principle from petition drives or voter turnout campaigns. The methodological challenge is that unchecked coordination could make indices primarily reflect organisational capacity rather than organic citizen sentiment. In the most serious scenario, foreign states could activate networks of authentic but directed users, producing movements in indices that carry no domestic democratic meaning. The Platform's response is transparency rather than censorship: coordinated activity is detected, flagged, and disclosed to readers – never silently suppressed or removed. The detection architecture and disclosure framework are described in §3.5 and §5.4.11.

2.7 Methodological Transparency and Auditability

2.7.1 Open Methodology

The Platform's methodology for calculating legitimacy indices is fully public. The formulas, confidence interval methods, aggregation rules, publication thresholds, edge case handling, and exclusion criteria are documented and available for scrutiny by researchers, journalists, regulators,

and citizens. What is not published – deliberately – is the specifics of anomaly detection algorithms, because disclosing detection parameters would provide a roadmap for circumventing them. The methodology documentation is versioned: when any element changes, the previous version is preserved and a dated public note explains what changed and why (§2.4.3). The Platform's public API (§5.4.10) enables independent verification of published indices by researchers, journalists, and any interested party.

2.7.2 Independent Audits and Third-Party Verification

The Platform's transparency commitment extends to independent verification of its own operations. Security, methodology, privacy, and compliance are subject to audit by third parties – with scope and frequency staged to the Platform's maturity. The roadmap progresses from pre-launch code review and vulnerability assessment through independent penetration testing to formal certification as operational scale requires (§7.7). Audit results are published, with sensitive security details redacted to prevent exploitation.

2.8 Limitations, Biases and Ethical Considerations

2.8.1 Self-Selection Bias

Participation is voluntary. Citizens who register and submit judgments are not a random sample of the population – they are likely to be more civically engaged, more digitally connected, and may differ from the general population by age, education, or location. Legitimacy indices therefore reflect the judgments of participating citizens, not a census-level portrait of public sentiment. This is an inherent property of the Platform, not a flaw to be engineered away.

The Platform addresses self-selection through three measures. First, transparency: every published index is accompanied by a threshold notice, its sample size and confidence interval are available in the subscriber analytical layer, and the Platform's documentation makes explicit that indices represent aggregated signals from participants, not weighted estimates of population-level opinion. Second, sustained effort to broaden participation through multilingual interfaces, accessible design, and outreach to under-represented communities as operational capacity allows. Third, honest refusal to apply demographic weighting or representativeness corrections – the Platform does not collect demographic attributes by design (§5.4.7), and applying statistical adjustments to data it does not possess would be methodologically dishonest.

2.8.2 Digital Divide and Access Barriers

Not all citizens have equal access to digital platforms. Older adults, rural residents, low-income communities, and people with disabilities face real barriers to participation, and the Platform's indices will reflect these gaps until they are addressed. Two commitments are non-negotiable from launch: citizen participation is permanently free, and the Platform is designed for accessibility by default – mobile-first delivery, multilingual interfaces covering all official languages in each country, and compliance with established accessibility standards. Broader inclusion measures – partnerships with public institutions, low-bandwidth optimisation, digital literacy support – are developed progressively as operational capacity and local partnerships allow. The Platform does not claim to have solved the digital divide; it commits to not deepening it.

2.8.3 Populism and "Tyranny of the Majority" Concerns

Indices of legitimacy can reflect popular prejudice, short-term emotion, or majoritarian bias against officials who protect minorities. The Platform acknowledges the tension. It measures what citizens express; it does not declare who deserves trust. Low indices remove no one from office, and constitutional processes remain intact. Trends over time and comparisons with peers help readers to interpret whether a movement reflects prejudice or a change in the actual standing of the person concerned.

Does making current sentiment visible create an incentive to pander? Does continuous monitoring invite a tyranny of the majority, in which officials shy away from defending unpopular minorities? The pressures towards populism already exist, through polls, the media and social platforms; Teisond organises those pressures and makes them legible. Indices are not commands: officials may act against the grain when they judge it right, and sustained explanation can rebuild trust over time. Democracy is majoritarian but constitutionally tempered, and Teisond does not alter that balance. Protections for minorities come from constitutions, courts and frameworks of rights, not from any index. The Platform reports a single dimension, public legitimacy, and leaves the other dimensions visible to the institutions designed to uphold them.

Over the long run, transparency creates counter-pressure to demagoguery. Persistent pandering without results tends to erode trust; difficult decisions that pay off can restore it, and the trajectory is visible in the record.

In short, Teisond makes public sentiment continuous and interpretable without turning it into a veto. It clarifies – rather than replaces – the existing constitutional settlement in which rights, courts, and law protect minorities while elected and appointed officials remain free to lead, explain, and, when justified, swim against the current.

2.8.4 Manipulation by Misinformation

Citizens will sometimes judge officials on the basis of false claims or partisan propaganda. The Platform neither can nor should audit the reasoning behind each judgment. Democracy does not require voters to demonstrate adequate information at the ballot box, and the Platform extends that principle between elections. What the Platform measures is perception: whether people currently accept an official's authority. That is a feature, not a flaw, because legitimacy concerns belief, not a forensic score of "deservingness."

Safeguards focus on integrity and clarity rather than censorship. The anomaly detection and disclosure framework (§2.6, §5.4.11) ensures that unusual activity is visible to readers. Over time, misinformation-driven swings usually wash out, while durable sentiment persists; trajectories make that distinction visible. The Platform remains neutral: indices report aggregated citizen sentiment, not claims about truth or merit. Interpreters may discount a move if they judge it misinformation-driven, but the Platform itself does not adjudicate narratives.

Combating falsehoods is the job of journalism, fact-checking, civic education, and open debate. The Platform's role is to make sentiment visible, auditable, and researchable – without exposing individuals or enabling profiling. Sharp moves should be read as prompts to seek context; the Platform supplies the visibility, the public sphere supplies the argument.

2.8.5 Emotional vs. Rational Judgment

Citizens often judge officials in the moment – after a specific encounter, a news story, or a visible decision. The Platform does not try to engineer this away. Democracy already runs on a mix of reason and affect; continuous measurement simply makes that mix visible. In political behaviour research, emotion is not a flaw to be filtered out – it is part of how people assess trustworthiness, fairness, and competence. When citizens feel angry, disappointed, reassured, or inspired, those are politically meaningful signals.

Continuity moderates volatility. Because measurement is ongoing, short-lived surges of emotion are followed by recovery if concern fades; sustained anger shows up as a lasting decline. The same mechanism that records a sharp drop also records correction when it happens. Officials are not powerless in the face of emotional response – clear communication, remedial action, or policy adjustment can rebuild confidence over time. Continuous feedback creates opportunities for course correction rather than locking anyone into a permanent verdict.

The alternative is not pure rationality. Elections themselves are saturated with emotion – campaigns, rallies, partisan identity, last-minute scandals. If continuous legitimacy monitoring is criticised for reflecting emotional responses, consistency requires the same criticism of elections. The Platform's contribution is to turn democratic sentiment into a transparent time-series signal that can be read with context, confidence intervals, and historical trajectory, rather than guessed at from episodic impressions.

2.9 From Unidirectional Authority to Mutual Accountability

The methodology described in preceding sections delivers more than measurement infrastructure. It creates a structural transformation in the relationship between citizens and governmental authority. This final section addresses the question that binds the methodology together: what does continuous legitimacy monitoring actually change?

2.9.1 The Structural Problem

The relationship between governing and governed is structurally unidirectional. Authority flows downward continuously – decisions, regulations, enforcement, resource allocation – while the citizen's capacity to respond flows upward only through episodic, constrained mechanisms. Elected officials face voters once every four to five years; between elections, the feedback channel is effectively closed. For appointed officials – the vast majority of those exercising governmental authority – even this episodic mechanism is absent. The asymmetry is not incidental; it is architectural. Elections, courts, media, and internal oversight each address fragments of the accountability relationship, but none creates what is fundamentally missing: a continuous channel through which citizens' aggregated judgments flow back to the officials whose authority depends, in democratic theory, on public acceptance. This blocked feedback defines the relationship as latently conflictual – frustration accumulates without outlet, officials operate without structured signals from those over whom they hold power, and both sides default to assumptions about the other rather than information. The Platform opens this channel.

2.9.2 How Continuous Monitoring Creates Reciprocity

For the citizen, the opening of this channel transforms a fundamental experience. Where previously frustration, approval, or concern had no structured outlet, each now has a destination: a judgment that enters a public, continuously updated index. The citizen does not gain power over the official's decisions – constitutional authority remains intact – but gains something that did not exist before: a persistent, visible signal that flows upward. The relationship shifts from unidirectional to bilateral. The citizen is no longer a silent recipient of authority but a participant in an information exchange whose output is public.

For the official, the channel introduces structured feedback from a direction that was previously silent. Officials routinely receive feedback from superiors, institutional peers, and media – but almost never from the citizens over whom they exercise daily authority. The Platform changes this. An official who subscribes to monitor their own index develops continuous awareness of how their authority is perceived by those it affects. Declining indices prompt investigation; stable indices provide confirmation. This is not external pressure imposed from above – it is information arriving from below, through a channel that previously did not exist.

For the system as a whole, the cumulative effect is a shift in norms. When legitimacy indices become available across officials at every authority level, comparison becomes inevitable – political rivals reference them, media highlight contrasts, supervisors notice patterns, and citizens develop expectations of responsiveness. The pressure this creates is not coercive; no index removes anyone from office. It is informational: the cost of ignoring citizen sentiment rises steadily as the signal becomes more visible, more cited, and more expected. Over time, responsiveness to the governed becomes not an act of virtue but a practical response to an environment in which indifference is publicly measurable.

2.9.3 Mutual Accountability as Emergent Property

What emerges from this bilateral information flow is not a single outcome but a cluster of social capital that did not previously exist. Accountability is the most visible component – officials become responsive to citizen sentiment because that sentiment is now public and persistent. But it is not the only one. Mutual recognition arises: officials see, for the first time, how their authority is perceived by those it affects, while citizens see that their judgment registers and matters. Reduced tension follows: relationships that were latently conflictual because feedback was blocked become less volatile when both sides have access to a shared signal. None of these outcomes is the Platform's direct function. The Platform opens an information channel between governing and governed; the social capital is generated by the exchange that flows through it. This is not revolutionary transformation but incremental structural change – adding a missing feedback mechanism to democratic systems that currently operate without one. The theoretical significance of this transformation – including principal-agent theory, information asymmetry resolution, and compound republic theory – is examined in Appendix A.

2.9.4 Integration with Existing Democratic Mechanisms

Continuous legitimacy monitoring supplements existing democratic mechanisms – it does not replace or compete with them. Elections remain the source of legal mandate. Courts protect constitutional rights. Media investigate and inform. Civil society advocates for change. Each addresses a distinct dimension of the democratic relationship. What the Platform adds is a specific capability absent from all of them: continuous, structured, verified expression of citizen judgment across every level of governmental authority, flowing through a channel that remains open between elections and extends to officials who never face elections at all. As the Platform's data becomes established, it naturally integrates into the existing ecosystem – informing media coverage,

enriching public discourse, and providing researchers with a longitudinal signal that no current instrument produces.

2.9.5 From Methodology to Significance

The methodology described in this section defines what the Platform measures and why. The sections that follow describe how that methodology is implemented in practice: the technical architecture enforcing its guarantees of privacy and integrity (Section 3), the revenue model sustaining it without compromising neutrality (Section 4), the legal framework governing its operation across the jurisdictions it serves (Section 5), and the principles of governance keeping it faithful to its mission as it scales (Section 6).

SECTION 3: TECHNICAL ARCHITECTURE

This Section provides a non-technical overview of the Platform's architectural principles. It is intended to demonstrate that Teisond's design enforces the privacy, neutrality, and transparency commitments described in Sections 2 and 5 – not merely as policy, but as structural properties of the system itself. Detailed technical specifications are maintained internally; what follows describes the architectural decisions that shape the Platform's guarantees to citizens, officials, and regulators.

3.1 Design Philosophy: Single Engine, Multiple Configurations

Teisond operates as a multi-tenant platform: a single codebase serves every country deployment simultaneously. Each country runs on its own isolated configuration and database, but shares the same core logic for index calculation, anti-manipulation safeguards, and data governance.

This architecture means that a methodological improvement or security patch deployed once is instantly active across all countries. There is no version fragmentation – every national deployment runs identical code at all times. National differences – language, governmental structure, authority levels, identity verification method, publication thresholds – are expressed entirely through configuration files, not through code changes. Launching a new country deployment requires no software modification: it requires a configuration file describing that country's institutional structure, verification provider, data residency location, and localisation parameters (§5.3.1).

The multi-tenant approach also eliminates a class of governance risks inherent in federated architectures – version fragmentation, methodological divergence between deployments, and inconsistent access controls. Because AGPT Ltd operates all deployments centrally from a single codebase, privacy protections, methodology, and incident response are uniform across every jurisdiction by construction, not by agreement.

3.2 Identity Verification: One Citizen, One Account

The integrity of indices of legitimacy depends upon a strict guarantee of one citizen, one account. Without it the Platform would be indistinguishable from an online poll, vulnerable to bots, duplicate accounts and coordinated manipulation. Teisond secures that guarantee through identity verification performed via national digital identity services, under the eIDAS framework where it applies, wherever such a service exists and is connected, and otherwise via an authorised verification provider operating across the jurisdictions the Platform serves. No weak method of verification, whether email, telephone or social media, is accepted. Verification is requested not on entry to the Platform but at the moment a citizen records a first judgment: viewing current indices requires no account and no verification. At the same time, the Platform's operational independence requires that neither its activation nor its continued operation ever depend upon governmental

identity infrastructure. An infrastructure of civic accountability must not be architecturally dependent upon decisions taken by the officials it monitors.

Upon verification, the citizen's identity is immediately transformed through irreversible cryptographic hashing (SHA-256 with a seasonal salt). The Platform retains only the resulting fingerprint – never the original identity data. The salt rotates periodically, rendering previous fingerprints unlinkable to current identities. After a defined retention period, old salts are permanently deleted, making retroactive identification technically impossible – not merely prohibited by policy, but precluded by the absence of the cryptographic material required to reverse the hash.

Verification of identity occurs once in the life of a citizen account. Routine return to the account does not repeat it. On the first judgment, the citizen's own device generates a cryptographic access key (a passkey) that never leaves the device; the Platform stores only a non-identifying account identifier and the public component of that key. The citizen unlocks the key locally – by fingerprint, facial recognition, or PIN – and the Platform recognises the account holder without storing any password, email, or contact detail. If the device is lost, re-verification yields the same fingerprint, allowing the Platform to recognise the existing account and issue a new key to it. The identity fingerprint thus serves two functions only: enforcing one citizen, one account, and anchoring account recovery.

The result is that the Platform can confirm every judgment as coming from a unique verified citizen without knowing, or being able to discover, who that citizen is. The fingerprint that makes this possible is itself pseudonymised personal data under the General Data Protection Regulation, and the Platform treats it as such throughout. What distinguishes the arrangement from ordinary pseudonymisation is not a change of category but the destruction of the means of reversal: once the salt from which a fingerprint was derived has been deleted, the material required to link that fingerprint to a person no longer exists anywhere, including within the Platform.

3.3 Data Architecture: Separation and Minimisation

The Platform enforces architectural separation between three categories of data: Identity data (hashed fingerprints confirming uniqueness) is stored in isolation from judgment data (trust/distrust records). These datasets cannot be joined or cross-referenced, even by system administrators. Technical controls – separate storage systems, no shared keys, no join endpoints – enforce this separation at the infrastructure level, not through access policies that an administrator could override.

Judgment data record the current state alone: a citizen's standing judgment of trust or distrust in respect of a mandate. Neutrality is not a stored value but the absence of a record. When a citizen changes a judgment, the previous value is overwritten rather than appended, and when a citizen withdraws one, the record is deleted. There is no timeline of opinions, no pattern of change, and no behavioural data capable of supporting a profile.

Aggregate index data (published legitimacy ratios, trends, confidence intervals) is computed from judgment data but contains no individual-level information. The aggregation layer applies k-anonymity thresholds before any data reaches publication endpoints, ensuring that no published aggregate permits inference of an individual judgment.

The database schema is deliberately minimal. Fields enabling demographic correlation, political profiling, or behavioural tracking do not exist in the schema – they cannot be collected because the containers for such data were never built. This is what "privacy by construction" means in practice:

not a policy restraining what the system could do, but an architecture limiting what the system can do.

3.4 Publication and Access Controls

Indices of legitimacy are published only once the number of standing judgments exceeds a configurable minimum threshold, set per jurisdiction and per level of authority. Below that threshold no ratio is displayed, and the profile shows instead the progress of accumulation: the number of standing judgments recorded and the threshold to be reached. Below a further minimum of counter visibility the profile shows only that collection is in progress. This protects both statistical validity, since small bodies of judgment produce unreliable indices, and the privacy of participants, since small groups may be re-identifiable. Published indices are rounded to prevent false precision, and confidence intervals accompany them at the analytical level, where they inform analysis rather than mislead a casual reader. These are not choices of presentation but privacy mechanisms embedded in the publication pipeline. The full publication policy, including k-anonymity requirements and anomaly flagging, is described in §5.4.8–5.4.9.

Access to published data follows a two-tier architecture – a public current index available to all without an account, and subscriber analytical data – described in §4.1. Access controls are enforced at the infrastructure level: no API endpoint exists that could return individual-level data regardless of authentication, and queries requesting demographic breakdowns or sub-threshold disaggregation are rejected by the system architecture, not by a policy layer that could be circumvented (§5.4.10).

3.5 Anti-Manipulation Safeguards

The Platform's identity verification requirement (§3.2) eliminates the most common attack vector against online platforms: bot accounts and duplicate registrations. Since only verified, unique citizens can participate – each confirmed as a real person through national digital identity or an authorised provider – the threat model shifts from fabricated identities to coordinated campaigns by real people, a fundamentally different and more constrained problem. The verification layer adds further safeguards: checks that prevent one person from registering more than once, and established anti-fraud controls applied at the moment of verification.

For coordinated campaigns by verified citizens, the Platform employs multiple detection layers – including volumetric, temporal, and geographic analysis – combined with rate-limiting mechanisms that constrain the speed at which any campaign can move an index. Detailed specifications are not published to prevent gaming. When anomalies are detected, the Platform favours disclosure over suppression: affected indices display a visible anomaly indicator with a plain-language note explaining what was detected. The index continues to be published, but readers can see that the data may reflect organised activity rather than organic citizen sentiment. The governance framework for this approach – including the principle that legitimate collective action should not be silently erased – is described in §5.4.11.

3.6 Infrastructure Resilience

The Platform is designed so that no adverse event in a single jurisdiction can disable operations elsewhere. Tenant isolation at country level ensures that a legal challenge, a regulatory action or a technical failure affecting one national deployment does not propagate to others. Each jurisdiction's data reside in infrastructure appropriate to that jurisdiction, hosted by providers selected for compliance with the applicable data protection regime, for guarantees of availability, and for independence from the governmental structures the Platform monitors.

Contingency infrastructure matures alongside the Platform itself. At the outset, resilience rests on tenant isolation, automated backups, and the ability to migrate any jurisdiction's data to an alternative hosting provider within the same legal space. As operational scale grows, the contingency architecture expands to include diversification of providers, testing of failover, and documented procedures of migration. The staging of these measures follows the security and compliance roadmap described in §7.7; the governance framework for contingency decisions, including trigger conditions and procedures of escalation, is described in §5.7.

The resilience philosophy is simple: no single point of failure – technical, legal, commercial, or political – should be capable of disabling the Platform or compromising its data.

SECTION 4: REVENUE MODEL AND ECONOMICS

This section explains how Teisond sustains itself financially while preserving its public mission. Teisond is a Crowdsourced Measurement Platform: it does not connect its users, affords the parties to the exchange no means of acting upon one another directly, and does not mediate between them. It receives judgments from one category of user and, by processing them analytically and synthetically, produces structured information of professional value to others. Everything that follows proceeds from that construction, and from one core principle: the Platform's revenue model must never create incentives in conflict with accurate and neutral measurement of legitimacy. Every design choice described below is tested against that principle. If a revenue source could bias indices, distort methodology or compromise neutrality, it is excluded.

4.1 Data Access Architecture: Public and Subscriber

Teisond provides two levels of access to legitimacy data, serving two distinct purposes:

Public access, open to all and requiring no account: anyone may see the Legitimacy Ratio as a current figure for every mandate that has crossed its publication threshold, the progress of accumulation for every mandate that has not, and the methodology in full. This is not a teaser for a paid product; it is the Platform's public mission in its entirety, and it is the level at which the institution the Platform embodies actually exists. Every citizen, unconditionally, can see where every official stands. The current index is given freely because citizens have a right to it, not in order to draw them towards something else.

Subscriber access (paid): Subscribers access the full analytical layer: absolute trust and distrust counts, consensus metrics, trend indicators and directional movement over time, confidence intervals, historical time-series, comparative analytics across officials at the same authority level, and anomaly detection reports. This is the Platform's commercial product and its only source of direct revenue.

The boundary between the two is deliberate. The public tier discloses a single, self-sufficient figure that means something on its own; everything that interprets that figure over time or against others – including any directional indicator, which functions as a political signal in its own right – belongs to the analytical layer. Because the public obligation is fully met by the free index, the analytical layer can be offered commercially with a clear conscience. The mission and the business model reinforce one another without the one being staged as bait for the other: the more citizens participate, the richer the aggregate becomes, and the more valuable the analytical product grows. The publication policy governing what is available at each level, and what is never published, is described in §5.4.9.

4.2 Primary Revenue: Officials Monitoring Themselves

The Platform's primary revenue source is subscription fees from officials who monitor their own legitimacy indices. This is not a speculative revenue hypothesis – it rests on a psychologically universal mechanism observable at every level of governmental authority.

The psychological mechanism is straightforward: once an official's legitimacy index becomes publicly visible and is cited by media, colleagues, and constituents, ignoring the Platform becomes costlier than subscribing. Media organisations and opposition figures may have access to detailed analytics; an official without a subscription sees less about their own standing than observers do. This information asymmetry creates natural demand for the subscription product. The motivations are identical whether the official is a prime minister or a municipal council member: control (real-time feedback), curiosity (unfiltered citizen sentiment), peer pressure (colleagues monitoring creates social expectation), and professional necessity (indices become metrics that matter in career advancement and institutional standing).

Critically, a subscription has zero effect on the official's index. The subscription purchases access to a mirror – it does not alter the reflection. This separation is absolute and architecturally enforced. A subscribing official and a non-subscribing official with identical citizen judgments will display identical public indices.

Subscription pricing is fixed by authority level (not by judgment volume or index value), eliminating any potential conflict of interest between Platform revenue and judgment activity. Pricing is jurisdiction-adjusted for accessibility: two officials at the same authority level in different jurisdictions pay amounts calibrated to local economic conditions, but both pay a fixed fee that does not vary with their index. Pricing scales with authority level – from L4 at the lowest price point to L1 at the highest.

The pricing structure is designed so that no official is priced out of self-monitoring. If legitimacy indices become a standard reference point in democratic discourse – cited by media, consulted by voters, referenced by institutional peers – then the subscription is not a luxury but a professional necessity. The Platform's growth strategy depends on making this transition: from novelty to standard infrastructure.

4.3 Secondary Revenue Sources

The Platform generates secondary revenue from three subscriber categories, all accessing the same subscriber analytical layer (§4.1) but for different professional purposes.

The most natural secondary audience is news media. For newsrooms under constant cost pressure, the Platform replaces ad-hoc polling commissions with a continuous, structured data source. A journalist with subscriber access can generate a data-driven story on any official at any time – time-series trends, comparative analytics across officials at the same authority level, anomaly indicators – without commissioning a poll or waiting for an election cycle. The value proposition is not a single dataset but a permanent editorial resource.

Academic institutions and policy organisations represent a second subscriber category, accessing anonymised and aggregated datasets for democratic governance research under terms that prohibit re-identification attempts. Early research partnerships serve a dual purpose: they generate

peer-reviewed validation of the Platform's methodology and contribute to the emergence of Public Legitimacy Analytics (PLA) as a distinct research domain.

The third category comprises political consulting firms, public affairs agencies, and governmental analytics units. These subscribers use legitimacy indices as inputs to their own advisory work – campaign strategy, stakeholder mapping, institutional risk assessment. As the Platform's data becomes a standard reference in the political intelligence ecosystem, revenue from this segment grows proportionally. The governance framework for institutional and consultancy relationships is described in §6.4.6.

4.4 Cost Structure: Automation-First Operations

Teisond operates on a lean, automation-first model. The Platform is designed so that routine operations – index calculation, publication, anti-manipulation monitoring, country configuration updates, threshold enforcement – run autonomously without human intervention. Human resources are reserved for exceptions, strategic decisions, quality oversight, and stakeholder relationships.

This architectural choice has direct financial implications. Adding a new country deployment does not require proportional headcount growth – it requires deploying a configuration file and activating identity verification for that jurisdiction. The marginal cost of an additional country is primarily infrastructure (hosting, verification integration), not personnel. This means the Platform's cost structure scales sublinearly with geographic expansion, creating improving unit economics as the Platform expands to additional countries.

The clearest evidence for this cost structure is the Platform's own construction. The engine, the applications, the multilingual site, the White Paper and the whole of the operational infrastructure were built without external capital, by a single founder working with AI-assisted development tools. What in a conventional model would have required a team and a funding round was carried by architecture instead: one body of code serving every jurisdiction, configuration in place of bespoke development, and automation of everything that recurs. The economics described in this section are not a projection from a business plan; they are a description of how the Platform was actually produced.

The automation-first approach also reduces operational risk. Routine decisions – when to publish, what thresholds to apply, how to flag anomalies – are made by the system according to documented rules, not by individual operators exercising discretion. This consistency is both an operational advantage and a governance commitment: the Platform operates the same way whether it is monitoring a controversial politician or an obscure local administrator.

4.5 What the Revenue Model Excludes

The following revenue sources are permanently excluded by design – not as aspirational commitments subject to future reconsideration, but as structural constraints embedded in the Platform's architecture and governance framework.

The first category of exclusions eliminates revenue streams that would compromise the Platform's neutrality. Advertising of any kind – display ads, sponsored content, paid visibility – is excluded

because it creates incentives to maximise engagement rather than accuracy. Sale of user data or behavioural profiles is excluded because individual-level data does not exist in exportable form by architectural design, and even if it did, selling it would destroy the trust that makes participation possible. Political consulting and campaign services are excluded because offering strategic advice to officials would compromise the neutrality that makes the data credible. The Platform provides data; it does not advise on how to use it.

The second category eliminates any arrangement where payment could create differentiated treatment. A subscribing official's public profile appears identically to a non-subscriber's – subscription purchases analytical access, not favourable presentation. Pricing is fixed by authority level and jurisdiction; no official, institution, or third party can pay to alter, suppress, delay, or prioritise the publication of any index. There is no premium tier that buys better visibility and no volume discount that rewards institutional pressure.

These exclusions answer a question every informed reader will ask: "If this platform depends on officials' money, how do I know the indices are honest?" The answer is architectural: the revenue model is designed so that paying more – or paying at all – cannot change what the Platform publishes. The mirror does not flatter its subscribers.

SECTION 5: LEGAL STRUCTURE AND JURISDICTIONAL FRAMEWORK

The Platform's legal framework is not a single legal regime extended uniformly across countries. It is organised in bands, defined by each jurisdiction's legal kinship to AGPT Ltd's home jurisdiction: the single legal space of the European Union and the European Economic Area, AGPT Ltd's own home jurisdiction operating a domestic deployment, and jurisdictions beyond the single space. Each band sits beside the others, not on top of them: a band defines how the Platform lawfully operates within a given legal space without altering how it operates in any other. What differs between bands is not the Platform but the legal construction beneath it. This banded structure is the legal expression of the Platform's design (§1.7): the mission is universal, but its legal realisation is disciplined, and each band is a construction of that discipline. Sections 5.1 to 5.8 describe the foundation band; §5.10 describes the method by which jurisdictions beyond the single space are admitted.

5.1 Operational Structure Within the Single Legal Space

Within the single legal space of the European Union and the European Economic Area, a shared standard of data protection (GDPR), a common framework of electronic identity (eIDAS), uniform intermediary and anti-SLAPP protections, and a single mechanism of consumption tax allow one controller to operate every deployment under one set of rules. This is the most developed band because it is a single legal space governed by a single set of rules, not because it marks the limit of where the Platform can operate.

One invariant holds across every band. The Platform has one founder, one published standard, one methodology, and one owner of its intellectual property and brand: AGPT Ltd. Where a single controller suffices for an entire band, as within the single legal space, AGPT Ltd is that controller directly. Where a jurisdiction requires a local controller, that controller operates under licence to the same standard, with AGPT Ltd retaining ownership of the methodology, software, and brand. Undivided accountability does not depend on there being a single legal entity; it depends on there being a single standard and a single party answerable for it. The bands describe where the Platform operates and under what legal construction; they never fragment the standard to which it is held.

Within this band, Teisond operates through a single legal entity. AGPT Ltd, incorporated in the United Kingdom, is the sole operator and sole data controller for every deployment in the band, and the sole holder of the Platform's intellectual property in all bands. Here there are no franchised national operators, no local subsidiaries, and no delegated controllers, because a single controller operating under the EU adequacy framework (§5.4.3) is sufficient to serve the entire band lawfully under one set of rules.

This single-controller arrangement is the form this band takes; it is not a constraint imposed on the Platform as a whole. It is the appropriate structure precisely because the band is a single legal space: one controller eliminates coordination overhead between entities, removes transfer pricing

complexity, ensures that methodology and privacy standards are applied uniformly without inter-entity negotiation, and places undivided accountability for every deployment in one organisation. Where a band lies outside this single legal space and a jurisdiction requires a local controller, that controller operates under licence to the same standard (§5.10). When something goes wrong in any deployment within this band, the responsible party is unambiguous: it is AGPT Ltd.

The legitimate concern with a single-controller arrangement is concentrated risk – legal challenge, regulatory action, or operational failure in one jurisdiction could in principle affect the operator's capacity to serve others. This risk is mitigated through three mechanisms: jurisdiction-first data residency ensures that each jurisdiction's data is architecturally isolated regardless of corporate structure (§5.3); insurance coverage addresses defamation, cyber, and professional liability exposure across jurisdictions (§5.5.3); and contingency mechanisms define the conditions and procedures for maintaining service continuity under adverse scenarios (§5.7). If the Platform's growth within the band reaches a stage where a second legal entity becomes operationally necessary, the path for structural evolution is described in §5.9.

5.2 Jurisdictional Home

5.2.1 Jurisdictional Choice: Why the United Kingdom

AGPT Ltd is incorporated in the United Kingdom. This is a deliberate jurisdictional choice grounded in the specific risk profile of the Platform, not a default selection based on founder convenience.

The most consequential factor is UK defamation law. The Defamation Act 2013 introduced a serious harm threshold and other reforms that rebalanced the relationship between reputation protection and public interest speech. For a platform that publishes legitimacy data about named officials across many jurisdictions, the legal environment governing its home jurisdiction matters more than for most technology companies. English law provides a more predictable and balanced framework for this type of publication than many EU civil law jurisdictions, where reputation protections can be significantly stronger.

English contract and corporate law offer a second practical advantage. The legal frameworks governing AGPT Ltd's Terms of Service, data processing agreements, and commercial contracts are well-understood internationally, reducing friction in relationships with EU-based partners, subscribers, and regulatory counterparts. UK intellectual property law provides clear and enforceable protections for the Platform's software, methodology, trademarks, and trade secrets.

The United Kingdom also benefits from an EU adequacy decision under GDPR Article 45, which provides the legal foundation for AGPT Ltd to act as data controller for EU citizen data (§5.4.3). This adequacy status, combined with Standard Contractual Clauses maintained as an independent safeguard, ensures that the Platform's jurisdictional home does not create a data protection deficit for EU participants.

5.2.2 Legal Structure

AGPT Ltd is incorporated as a private company limited by shares under the UK Companies Act 2006. This corporate form provides limited liability protection for the founder and any future shareholders, straightforward governance through standard articles of association, and full transparency through Companies House filing obligations. The structure accommodates future

evolution – including the admission of mission-aligned investors or transition toward community governance models – without requiring re-incorporation.

The path for such evolution is described in §5.9. AGPT Ltd also holds all intellectual property associated with the Platform, including the Teisond trademark, software, methodology, and visual identity.

5.3 National Data Governance

5.3.1 Country-Specific Configuration

Each country deployment is operated by AGPT Ltd through a country-specific configuration file that defines all jurisdiction-specific parameters without requiring separate legal entities or local teams. The configuration determines four core dimensions of each deployment.

The method of identity verification is defined per country. Each country configuration specifies which path of verification is used when a citizen records a first judgment. Where a national electronic identity system exists and is connected to the Platform, it is the preferred path and offers the strongest assurance. Where it is unavailable, unconnected, or restricted, an authorised independent provider serves as the always-available alternative, so that no deployment depends upon a system administered by the officials the Platform monitors.

Official database scope determines which categories and levels of officials are monitored in that country, sourced from official registries and institutional directories. The scope expands progressively – from Level 1 national officials at launch to comprehensive coverage across all four authority levels as the deployment matures.

Data residency defines which hosting provider and geographic region stores citizen data for that country. Citizen data is always stored within the country itself where suitable infrastructure exists, or within the EU/EEA where it does not – ensuring jurisdictional compliance independent of AGPT Ltd's UK domicile.

Localisation covers user interface language, date and number formats, currency display, and jurisdiction-specific legal text including privacy notices and terms of service adapted to local consumer protection requirements.

This configuration-driven approach enables AGPT Ltd to launch new country deployments rapidly – activating a new country requires deploying a configuration file, not writing new code – while maintaining full consistency of methodology, privacy architecture, and publication standards across all jurisdictions.

5.3.2 AGPT Ltd Responsibilities per Country

AGPT Ltd bears full and undivided responsibility for every deployment in the EU/EEA band. Within this band there are no local operators, sub-processors acting as independent controllers, or franchised entities. AGPT Ltd is the sole data controller under GDPR for every jurisdiction in the band (§5.4.1), manages hosting infrastructure and database operations centrally (§5.3.1), builds and maintains the officials database from official registries for each country (§7.3), handles regulatory compliance with applicable national laws, and coordinates crisis response – whether legal challenge, manipulation attempt, or political pressure – from a single operational centre with

country-specific adaptation as needed. This centralised model eliminates ambiguity about who is accountable when something goes wrong: the answer, in every country, is AGPT Ltd.

5.3.3 Country Adaptation and Consistency

The configuration-driven architecture described in §5.3.1 defines the boundary between what adapts and what does not. Identity verification method, official database scope, data residency, localisation, and jurisdiction-specific legal text are configurable per country. Core methodology, privacy architecture, anti-manipulation systems, publication thresholds, and ethical commitments are fixed at the platform level and cannot be overridden by any country configuration. All deployments share the same codebase – a country launch is an activation, not a fork.

5.3.4 Country Deployment Lifecycle

Each country deployment progresses through defined lifecycle stages – from waitlist through active operation – controlled centrally by AGPT Ltd. The activation criteria and progressive rollout logic are described in §7.2. If a country deployment must be suspended due to legal, regulatory, or operational reasons, or permanently decommissioned, the contingency mechanisms described in §5.7 govern the process, including GDPR-compliant data portability and erasure. Lifecycle transitions in one country do not affect the operation of any other deployment.

5.4 Data Governance and Compliance

Privacy protection is foundational to the Platform's mission. Citizens judging officials must trust that their judgments remain private, protected from governmental surveillance, political profiling, and commercial exploitation. Without strong privacy guarantees, citizens in sensitive political contexts – polarised environments, vulnerable minorities, states with weakening democratic norms – cannot safely participate. The legal framework therefore treats privacy as mission-critical, not merely as regulatory compliance.

The privacy architecture combines legal compliance (GDPR as baseline across the EU/EEA band), technical enforcement (privacy by design at the infrastructure level), and operational discipline (data minimisation, access controls, breach response). This multi-layered approach ensures that privacy protections survive even if any single layer fails.

5.4.1 GDPR as Baseline Standard

AGPT Ltd applies GDPR as the baseline data protection standard across all deployments within the single legal space, and as the reference standard elsewhere, regardless of whether a given jurisdiction's national framework would require it. This is a deliberate architectural decision rather than a minimum compliance exercise. GDPR provides the most comprehensive and well-understood data protection framework available, and its uniform application eliminates the risk of inconsistent protection levels between jurisdictions.

The Platform implements GDPR's core principles through design choices specific to its architecture. Data minimisation governs every layer: identity verification confirms that a participant is a unique

adult resident of the relevant country, but the Platform does not store identity documents, precise dates of birth, or exact addresses after verification is complete. Purpose limitation is enforced architecturally – data collected for identity verification cannot be accessed by the systems that process and aggregate judgments, and judgment data cannot be linked back to verification records without a technical process that no single operator can initiate. Storage policy distinguishes between the current state of judgment, retained for as long as the account is active, since continuous monitoring requires a live signal, and the history of judgments, which is not stored, since the Platform measures current legitimacy rather than historical patterns of individual behaviour. A judgment stands until it is changed or withdrawn; a change overwrites the record rather than appending to it.

Accountability mechanisms are staged to the Platform's maturity. Prior to launch, AGPT Ltd completes a Data Protection Impact Assessment covering all processing activities, establishes records of processing, and designates a data protection lead. Independent audit and formal DPO appointment follow as operational scale requires, in line with the security and compliance roadmap described in Section 7.7.

5.4.2 Legal Basis for Processing

The Platform processes personal data under distinct legal bases depending on the nature of the processing activity, in accordance with GDPR Article 6(1).

Account creation, judgment submission, and access to Platform services rely on contract performance (Article 6(1)(b)). When a citizen accepts the Terms of Service, the processing necessary to operate the account, record judgments, and deliver the service follows directly from that contractual relationship. This is the Platform's primary legal basis for the majority of its processing activities. Where processing extends beyond what is strictly necessary for service delivery – such as optional communications or participation in research – explicit consent (Article 6(1)(a)) is obtained separately, and can be withdrawn without affecting the citizen's account or participation rights.

Identity verification relies on legitimate interests (Article 6(1)(f)). The Platform has a documented legitimate interest in confirming that each participant is a unique adult resident of the relevant jurisdiction, since the guarantee of one citizen, one account is essential to the integrity of every index the Platform publishes. A balancing assessment demonstrates that this interest does not override the data subject's rights: verification data is processed by a third-party provider (§3.2), the Platform receives only a confirmation result, and no identity documents are stored after the verification process is complete. The public interest in reliable democratic accountability data serves as a supporting factor in this balancing assessment, though the Platform does not rely on public interest as an independent legal basis.

5.4.3 Cross-Border Data Flows

The Platform's data architecture is designed around jurisdiction-first residency. Citizen judgment data and aggregated indices for each jurisdiction are stored and processed within that jurisdiction, using hosting infrastructure located there or, where that is not available, in the nearest jurisdiction with equivalent data protection standards. This is an architectural constraint enforced at the tenant level, not a policy preference – the system does not permit judgment data from one jurisdiction's tenant to be queried or accessed by another.

Cross-border data flows arise in limited operational scenarios. AGPT Ltd, incorporated in the United Kingdom, is the sole data controller. Routine Platform operations – judgment submission, index calculation, publication – occur entirely within each country tenant and do not require data to leave

the hosting jurisdiction. However, technical support, system maintenance, and backup operations may require AGPT Ltd personnel to access country-level data from the United Kingdom. These transfers are governed by Standard Contractual Clauses as the approved transfer mechanism under GDPR Chapter V.

The United Kingdom benefits from an EU adequacy decision under Article 45 GDPR, recognising UK data protection standards as essentially equivalent to those of the EU. This provides the foundational legal basis for the controller relationship between AGPT Ltd and its EU/EEA operations. AGPT Ltd monitors the status of this adequacy decision and maintains Standard Contractual Clauses as an independent safeguard, ensuring continuity of lawful data transfers regardless of any future change in adequacy status.

5.4.4 User Rights and Data Subject Access

AGPT Ltd implements the full set of data subject rights under GDPR Articles 15–22 through Platform interface controls and documented response procedures. Citizens can access and download their current judgment state and account information, correct inaccurate account data, and export their data in a machine-readable format. These functions are available directly through the user interface without requiring a formal request, though the formal channel remains available for any right that cannot be exercised through self-service.

Account deletion requires specific attention because of its interaction with aggregated indices. When a citizen requests erasure, the Platform deletes all personal data – account information, verification status, and the link between the citizen's identity and their judgments. The judgments themselves are anonymised: the aggregate index is recalculated to reflect the removal, but no record remains that could connect the deleted account to any contribution. This is true anonymisation, not pseudonymisation: once the account is deleted, re-identification is technically impossible. The Platform retains no history of an individual's positions (§5.4.1), so erasure reaches only the current state: the withdrawn judgment ceases to stand and is absent from every subsequent snapshot. Snapshots already published are not revised, in accordance with the versioning discipline described in §2.4.3.

Citizens may also restrict their account temporarily, pausing participation without triggering full deletion. The right to object under Article 21 applies to processing carried out under legitimate interests – specifically, identity verification (§5.4.2). An objection to verification processing is assessed on its merits; if upheld, it results in account suspension since the Platform cannot operate an unverified account. No automated decisions with legal or similarly significant effects are made about any individual; the Platform aggregates citizen inputs into statistical indices and does not make determinations about citizens themselves.

5.4.5 Privacy by Design and by Default

The Platform implements privacy by design and by default in accordance with GDPR Article 25 – not as a compliance layer added to a functioning system, but as a foundational architectural principle. The distinction is practical: database tables that would enable profiling, judgment history tracking, or demographic correlation of opinions do not exist in the schema. API endpoints that would return individual-level data have not been built (§5.4.10). These capabilities are not restricted by access controls or policy – they are absent from the architecture entirely. The technical details of this approach are described in Section 3; the publication thresholds that prevent statistical inference of individual opinions from aggregated data are described in §5.4.8.

Privacy by default means that a new account, with no settings adjusted, operates at the maximum privacy level the Platform offers. Judgments are never publicly visible at the individual level. No

social features, follower mechanisms, or activity feeds exist that could reveal participation patterns. The only output the Platform produces from citizen activity is the aggregated index – a statistical summary in which no individual is identifiable.

5.4.6 Security Measures

AGPT Ltd implements security across four layers: infrastructure (hosting environment, network protection, backup and recovery), application (secure development practices, input validation, session management), operational (personnel controls, access governance, incident response), and third-party (vendor assessment ensuring that hosting providers, identity verification partners, and payment processors meet equivalent security standards). These layers follow a defence-in-depth model – compromise of any single layer does not expose citizen data, because each layer enforces independent controls.

The security programme is staged to the Platform's maturity, progressing from pre-launch code review and vulnerability assessment through independent penetration testing, and toward formal certification as operational scale requires. The full staging roadmap – including SOC 2 and ISO 27001 milestones – is described in §7.7. Breach response procedures comply with GDPR Article 33 notification requirements: documented detection and containment protocols, assessment of risk to data subjects, and notification to the relevant supervisory authority within 72 hours where required.

5.4.7 Data We Do Not Collect (Architectural Minimisation)

Teisond implements an aggregates-only publication model. The following categories of data are never collected, stored, linked, or made available through any Platform interface, API, or export:

Personal identifiers: names, emails, phone numbers, government IDs, and social media handles are never written to storage. What the Platform keeps is the one-way cryptographic fingerprint generated at verification, which remains pseudonymised personal data under GDPR and is treated as such; the source data are discarded, and with them the means of reversal.

Per-user judgment histories: no longitudinal linkages are maintained across sessions or events. The Platform maintains no 'user timelines' of opinions. A citizen's pattern of judgments across officials or over time is architecturally unrecoverable.

Reasons or explanations for judgments: the binary trust/distrust mechanism accepts no free-text justifications, tags, or categorical motives tied to individual citizens. The Platform does not ask why – only whether.

Demographic attributes and opinion correlations: age, gender, ethnicity, income, religion, education, and party affiliation are never collected. No analysis of how judgments correlate with demographic characteristics is possible, because the demographic data does not exist in the system.

Behavioural profiles: no clustering or scoring of individuals, no interest graphs, no look-alike modelling. The Platform cannot distinguish one citizen's behaviour from another's, because individual behaviour is not tracked.

Precise geolocation and device fingerprinting: no GPS-level location data, no persistent device or browser fingerprints. The Platform does not know where a citizen is when they render a judgment, nor what device they use.

Advertising and third-party trackers: no advertising pixels, retargeting beacons, or cross-site identifiers. The Platform carries no advertising and shares no data with advertising networks.

Raw personal data exports: the Platform never provides raw individual-level records to any party — including AGPT Ltd itself, researchers, media subscribers, or law enforcement — because such records do not exist in retrievable form.

These exclusions are enforced by architecture, not by policy. The data model lacks tables for individual-level opinions. Pre-aggregation gates discard any potentially identifying fields before data enters the publication pipeline. The API accepts only aggregate queries and rejects any request that could return profiling or row-level results. The user interface provides no input fields for personal details beyond the verification boundary. Necessary operational security logs — such as transient IP addresses for abuse detection — follow strict minimisation and short retention policies defined in § 5.4.6.

5.4.8 Aggregation and Publication Thresholds

To protect both individual privacy and measurement quality, the Platform publishes legitimacy indices only when they meet defined statistical thresholds. The primary safeguard is a minimum number of standing judgments on a mandate, differentiated by level of authority and configured per jurisdiction: several hundred for mandates of national rank, several dozen for local ones. This ensures that published indices carry genuine statistical weight and that no small group of citizens can disproportionately determine a published number.

Beyond minimum sample size, the Platform applies k-anonymity guardrails: no metric is published if doing so risks revealing information about identifiable small groups. These guardrails are jurisdiction-configurable, allowing country deployments to set stricter thresholds where local data protection standards or demographic conditions require them — though never looser than the Platform-wide default.

Published aggregates are rounded to one decimal place to avoid false precision and reduce re-identification risk. Where a mandate has not yet reached its publication threshold, the Platform displays the progress of accumulation — the number of standing judgments recorded and the threshold to be reached — rather than suppressing the entry entirely, making the state of collection visible rather than silent. Below a further minimum of counter visibility, also configured per jurisdiction, only a neutral state of collection in progress is shown.

When the Platform's integrity systems detect volumetric anomalies — sudden spikes, coordinated patterns, or statistical irregularities — the affected indices remain published in their aggregated form but are flagged with a visible anomaly notice and a link to the corresponding transparency note. Suppression is avoided; disclosure is the default.

Country deployments may configure stricter local thresholds within their deployment configuration, aligned with the privacy architecture defined in § 5.4.1–5.4.6. No country deployment may set thresholds below the Platform-wide minimums.

5.4.9 Publication Policy (Public vs Subscribers vs Never)

The Platform operates three tiers of data access, distinguished not by the sensitivity of the underlying data — which is always aggregated — but by the depth of analysis and the audience it serves.

The first tier is public access, available to any visitor at no cost. This includes the headline legitimacy index – the current percentage – for every mandate that has crossed the publication threshold, the progress of accumulation for every mandate that has not, full methodology documentation, and anomaly flags. The Platform's commitment to transparency means that any detected irregularity is visible to the public, not reserved for paying subscribers. Directional information is deliberately withheld from this tier: a public trend indicator, however simplified, functions as a political signal in its own right, and is therefore reserved for the subscribers whom such movement concerns. Confidence intervals are likewise reserved for subscriber access, where they inform analysis rather than mislead a casual reader.

The second tier is subscriber access, available to officials monitoring their own indices and to media, researchers, civic organisations, and consultants through paid subscriptions. Subscriber data remains strictly aggregated – no subscriber at any level receives individual-level records. What subscribers receive is analytical depth: trend indicators and directional movement over time, confidence intervals indicating statistical reliability, benchmarks and comparisons across mandates and institutional categories, historical series of snapshots at configurable granularity, threshold-crossing alerts and anomaly advisories, and programmatic API access for integration with dashboards and research pipelines. The API enforces the same aggregation rules described in §5.4.10 – it is a delivery mechanism for published aggregates, not a backdoor to underlying data.

The third tier is data that is never available – to anyone, at any price, under any circumstances. This includes individual citizen judgments, per-user judgment histories, demographic correlations of opinions, any output that could enable political profiling or re-identification of citizens, and raw datasets or row-level exports. These exclusions are not policy decisions subject to future revision – they are architectural properties of the data model. The data does not exist in a form that could be exported even if the decision were made to do so.

5.4.10 Public API and Access Controls (Aggregates-Only)

The data access architecture described in Section 4 distinguishes public data and subscriber data, alongside data that is never released – described in §4.1 and §5.4.9. The Platform's API operates strictly within this framework, serving exclusively aggregated metrics. No endpoints exist for individual-level retrieval, and no query can return data that would enable profiling or re-identification. This is not an access control decision that could be reversed – it is an architectural constraint: the endpoints that would serve individual-level data have not been built.

Query validation enforces this boundary at the infrastructure level. Requests for demographic or location breakdowns of participant opinions are rejected. Profiling queries and row-level requests return errors regardless of the caller's authentication level. Rate limits are enforced to protect service integrity and prevent bulk extraction attempts. API keys are revocable; usage is logged at the aggregate level (never individual-level) for audit purposes.

Terms of use explicitly prohibit attempts to re-identify individuals, infer demographic correlations of opinions, or reverse-engineer individual judgments from aggregate data. Violations trigger immediate key revocation and may result in legal remedies. These terms are not aspirational – they are backed by architectural constraints that make the prohibited actions technically infeasible even if the terms were ignored.

5.4.11 Anti-Manipulation and Transparency Disclosure

The Platform's anti-manipulation framework operates at two levels: structural prevention and behavioural detection. The guarantee of one citizen, one account, enforced through identity verification via national digital identity or authorised providers (§3.2), eliminates bot-driven and

duplicate-account manipulation at the architectural level. No unverified entity can participate in the judgment process. Rate-limiting mechanisms restrict how frequently a citizen can change a judgment on any given mandate, removing the primary vector for rapid coordinated swings. The specific parameters of these controls are not published to prevent gaming.

For coordinated campaigns by verified citizens – which are legitimate democratic activity, not fraud – the Platform employs volumetric anomaly detection, temporal clustering analysis, and campaign-burst monitoring. When suspected coordinated activity is detected, it is disclosed to users through visible labels and plain-language transparency notes rather than silently suppressed. This reflects a deliberate design choice: organised civic action, even if it produces sharp movements in an index, should not be erased without explanation. Content is removed only where it violates applicable law or Terms of Service.

The Platform applies the same visibility discipline to itself that it applies to officials. Material interventions – threshold changes, methodology updates, publication rule modifications – follow documented procedures with public changelogs. No change is made silently. Rules change only with notice, reasons, and records.

5.5 Liability and Risk Allocation

5.5.1 Defamation and Speech-Related Risks

The Platform publishes legitimacy indices that attach numerical values to named public officials. This creates inherent defamation exposure – not because the data is false, but because any publication about identifiable individuals invites legal challenge in jurisdictions where reputation is strongly protected.

Several features of the Platform's design substantially reduce this exposure. Citizen judgments are structured as binary expressions – trust or distrust – with no accompanying text, no accusations, and no factual claims about conduct. The Platform publishes only aggregated indices derived from these judgments, never individual responses. What appears on a public profile is a statistical fact: that a given percentage of participating citizens expressed trust or distrust. Reporting verifiable statistical outcomes is fundamentally different from making editorial claims about an official's character or conduct, and this distinction is recognised across both common law and civil law traditions.

The EU Digital Services Act provides the primary regulatory framework for the Platform's intermediary status. Under the DSA, platforms that host and organise user-generated content without exercising editorial control over individual contributions benefit from conditional liability protections. The Platform does not select which officials receive low or high indices, does not editorially frame the results, and does not encourage any particular judgment. It operates as infrastructure for aggregating citizen sentiment, not as a publisher advancing a position.

Defamation law varies considerably from one jurisdiction to another. Common law and civil law systems apply different standards as to the burden of proof, the distinction between fact and opinion, and the weight given to defences of public interest. Some jurisdictions offer robust doctrines concerning public figures; others protect the reputation of officials more strongly. AGPT Ltd assumes no uniformity of legal protection across the jurisdictions it serves. A national legal review is conducted for each jurisdiction before activation, identifying specific points of exposure and adapting the Terms of Service accordingly.

Despite these structural protections, residual risk is not zero. Officials may initiate strategic lawsuits against public participation (SLAPP) – actions intended not to succeed on merits but to impose financial and operational burden. The EU Anti-SLAPP Directive, currently being transposed into national law across member states, will provide procedural safeguards including early dismissal mechanisms for abusive claims. Until full transposition is complete, the Platform's mitigation rests on three pillars: dedicated media and defamation insurance coverage (§5.5.3), Terms of Service that clearly define the nature of published data as aggregated statistical outputs, and qualified legal counsel in jurisdictions identified as higher-risk during national legal review.

5.5.2 AGPT Ltd Liability Framework

As sole operator of all national Platform deployments, AGPT Ltd bears comprehensive liability for the Platform's operations across every jurisdiction it serves. This centralised liability model – a direct consequence of the single-entity architecture – means that citizens and subscribers anywhere deal with one responsible party, governed by one set of standards, regardless of which national deployment they use.

AGPT Ltd assumes full responsibility for all operational decisions and Platform-generated content across all jurisdictions, including the accuracy of published indices within the bounds of the stated methodology. The company bears liability for all aspects of user data processing and privacy compliance under GDPR and applicable national data protection laws. Any defamation or speech-related claims arising from Platform publication – including legitimacy indices, anomaly flags, and transparency notes – are the responsibility of AGPT Ltd as publisher, not of the citizens whose aggregated judgments produced the data. Customer disputes, subscription issues, and employment claims relating to AGPT Ltd staff fall under the company's standard commercial liability.

Certain categories of harm fall outside any party's liability by their nature. Third-party attacks on Platform infrastructure – including hacking attempts and distributed denial-of-service attacks – do not create liability for either AGPT Ltd or its users, unless the damage results from AGPT Ltd's negligence in maintaining adequate security measures. Government actions compelling data disclosure or Platform shutdown in a specific jurisdiction are treated as regulatory force majeure: AGPT Ltd complies with lawful orders while exhausting available legal remedies, but does not assume liability for consequences of sovereign state action. Natural disasters, wars, and other force majeure events are governed by standard contractual provisions.

Individual users bear liability only for their own actions that violate the Platform's terms of service – such as attempting to create multiple accounts, circumventing verification controls, or misrepresenting the Platform's methodology or outputs to third parties.

AGPT Ltd maintains comprehensive liability insurance and legal reserves appropriate to the scale and jurisdictional complexity of operating civic infrastructure across multiple jurisdictions. Insurance coverage is reviewed annually and adjusted as the number of active national deployments and the subscriber base grow.

5.5.3 Insurance Requirements

Operating a civic accountability platform across multiple jurisdictions creates a specific risk profile that requires dedicated insurance coverage. The Platform publishes legitimacy indices about named public officials, creating defamation exposure. It processes citizen identity verification data, creating cyber and privacy risk. And it operates under several regulatory frameworks simultaneously, creating multi-jurisdictional compliance exposure.

The insurance programme covers four domains from the outset of operations. Professional Liability (Errors and Omissions) addresses claims arising from incorrect index publication, methodology errors, or negligent provision of data services. Cyber Liability covers data breaches, privacy violations, cyber extortion, and business interruption resulting from attacks. Media and Defamation Liability provides specific protection for claims related to the publication of legitimacy data about identifiable officials – a risk category distinct from general professional liability. Directors and Officers coverage protects AGPT Ltd leadership from personal liability arising from organisational decisions.

Coverage levels will be established in consultation with specialist brokers experienced in technology platform and media liability, and reviewed annually as the Platform expands to additional jurisdictions. Each new jurisdiction may introduce specific liability exposures that require adjustment to the programme.

5.5.4 Tax Structure and VAT Compliance

AGPT Ltd operates as a single legal entity with a deliberately simple tax structure. The company is subject to UK Corporation Tax on its worldwide profits, filed annually with HMRC. This simplicity is an intentional choice at the current stage – a single-entity model eliminates the transfer pricing documentation, inter-company agreements, and multi-jurisdictional corporate tax filings that characterise more complex structures.

Consumer-facing VAT obligations across the European Union are managed through the Platform's Merchant of Record payment partner, which acts as the legal seller of subscription services to end users. The Merchant of Record calculates, collects, and remits VAT at the correct rate in each jurisdiction, files all required VAT returns, and issues locally compliant invoices to subscribers. AGPT Ltd receives net payouts after VAT has been handled, removing the need for direct VAT registration in individual member states at this stage.

Should the Platform's scale and operational requirements justify establishing a separate operational entity within the European Union in future (§5.9), cross-border tax considerations including withholding taxes on IP licensing fees, transfer pricing compliance, and dual-jurisdiction corporate tax optimisation will be addressed at that point, with structures designed to satisfy arm's-length requirements and documented in consultation with qualified tax advisors in each relevant jurisdiction. Until then, the single-entity model keeps administrative overhead low and ensures that resources are directed toward Platform development and jurisdiction activation rather than corporate structure maintenance.

5.6 Dispute Resolution

5.6.1 Governing Law and Jurisdiction

All subscriber agreements and Platform terms of service are governed by English law – a jurisdiction chosen for its well-developed body of technology and platform case law, predictable contract enforcement, and global recognition. Disputes are subject to the exclusive jurisdiction of the English courts, with one important exception: citizens and subscribers who qualify as consumers under their national law retain the right to bring claims in their local courts. Nothing in the Platform's terms limits statutory consumer rights under applicable EU or national consumer protection legislation.

For disputes involving personal data rights, users may additionally file complaints with their national data protection authority, which has independent investigative and enforcement powers under GDPR – regardless of what the Platform's terms say about jurisdiction. This dual-track protection – contractual remedies through English courts, regulatory remedies through national DPAs – ensures that no user is left without accessible recourse.

5.6.2 Escalation Process

Disputes are resolved through a staged process designed to address issues at the lowest appropriate level before formal proceedings become necessary.

The first stage is direct resolution: the user contacts AGPT Ltd's support team, which handles the matter through standard operational channels. The majority of disputes – account access issues, data display questions, subscription billing queries, and service quality concerns – are resolved at this stage.

The second stage is management review: if direct resolution fails or the dispute involves policy interpretation, account termination, or data deletion decisions, AGPT Ltd management reviews the matter and issues a formal response. Users receive written reasoning for any decision that affects their account or data.

The third stage is mediation: if management-level resolution is unsatisfactory, either party may propose mediation through a neutral third party. Mediation is non-binding but provides a structured opportunity for both sides to present their positions before an independent mediator.

The fourth stage is formal proceedings: if mediation fails, the dispute proceeds to the English courts – or, where applicable consumer protection law provides, to the user's local courts. Users may simultaneously or alternatively pursue complaints through their national data protection authority, whose powers operate independently of any contractual dispute resolution mechanism.

AGPT Ltd maintains documented complaint-handling procedures across all country deployments, ensuring consistent process, fair treatment, and timely responses regardless of which national Platform a user registered through.

5.7 Operational Resilience and Contingency

5.7.1 Contingency Architecture

The Platform's design incorporates contingency at the architectural level – not as a separate disaster recovery layer, but as a property of the choices already made. A single-entity structure with cloud-based infrastructure, a Merchant of Record payment model, and configuration-driven country deployments means that migration of any component does not require rebuilding the system – it requires changing a configuration.

Hosting infrastructure runs on a cloud provider with EU data centres. If the provider becomes unsuitable – whether due to commercial terms, regulatory pressure, or service quality – citizen data can be migrated to an alternative EU-based provider. The Platform stores no data in proprietary formats that would create lock-in; standard database exports and documented deployment procedures ensure that migration is an operational task, not an engineering project. At the current

stage, migration would take days rather than hours, but the architectural prerequisites for rapid migration are in place.

Payment processing is handled by a Merchant of Record partner that manages all subscriber billing, VAT compliance, and invoicing. If the payment partner becomes unavailable, the Platform can transition to an alternative MoR provider or to direct payment processing through a conventional gateway. Subscriber relationships are maintained by the Platform – not by the payment partner – so no customer data is lost in transition.

Domain registration for teison.com and all national subdomains is managed through standard registrars with DNS served by a global CDN provider. DNS-level failover to alternative configurations is achievable within hours.

The United Kingdom was chosen as the home jurisdiction of AGPT Ltd for its legal stability, its protection of intellectual property and its treaty network. Should conditions there deteriorate materially, whether through regulatory change incompatible with the Platform's privacy architecture, the loss of EU adequacy status, or political interference with the Platform's operation, AGPT Ltd retains the option of re-domiciling to another jurisdiction assessed as viable on its legal framework, its technology infrastructure and its data protection environment. Re-domiciliation is a significant undertaking that would be executed only under serious and sustained adverse conditions, and never as a routine response to regulatory inconvenience.

5.7.2 Trigger Conditions

Contingency measures are activated when conditions in any jurisdiction cross defined thresholds that threaten the Platform's core commitments – specifically, its ability to protect citizen privacy, maintain methodological independence, and publish indices without interference.

Regulatory triggers include new legislation requiring disclosure of individual citizen judgments to government authorities, prohibition of end-to-end encryption or one-way hashing for identity data, mandated content moderation incompatible with the Platform's deterministic publication methodology, or compliance burdens that make continued operation in a jurisdiction financially unviable.

Commercial triggers include termination of critical service relationships – hosting, payment processing, or identity verification – due to political pressure rather than commercial terms, or coordinated refusal of service by multiple providers in a jurisdiction.

Political triggers include direct governmental demands for preferential treatment of specific officials, use of regulatory or prosecutorial authority to pressure the Platform into altering indices or suppressing publication, or legal actions designed to harass rather than to remedy legitimate grievances.

The appropriate response to each trigger is proportionate: a regulatory change in one jurisdiction may require adjusting that jurisdiction's deployment configuration, while a fundamental change in UK law might necessitate corporate re-domiciliation. The contingency framework distinguishes between jurisdiction-level responses, which affect a single national deployment, and entity-level responses, which affect AGPT Ltd's corporate structure. Jurisdiction-level contingencies are executable by the current team; entity-level contingencies would be undertaken with professional legal and tax advisory support.

5.7.3 Preparedness and Maturity

At the current stage, contingency preparedness consists of architectural choices that preserve optionality: no vendor lock-in, no proprietary data formats, no single points of failure in the deployment pipeline, and pre-identification of alternative jurisdictions and service providers. Formal migration playbooks – documented step-by-step procedures with tested timelines for each contingency scenario – are developed as the Platform scales and operational resources permit, in step with the security and compliance roadmap described in §7.7.

5.8 Verification Independence

Civic accountability infrastructure faces a unique architectural risk: dependence on governmental systems for the identity verification that enables citizen participation. If Platform launch requires permission from the officials the Platform monitors, the resulting vulnerability is not merely operational but existential – it inverts the accountability relationship the Platform exists to create.

Teisond addresses this through verification independence as a design principle. National digital identity systems under the eIDAS framework are the preferred verification path: where a country's identity infrastructure is available and connected, the Platform uses it as the primary means of confirming that each citizen is a unique, real person. This path delivers the strongest assurance and the lowest cost per verification.

Crucially, this preference never becomes a dependency. Where national digital identity is unavailable or not connected, authorised identity verification providers confirm uniqueness across every jurisdiction the Platform serves, without any governmental approval or integration, delivering a guarantee of one citizen, one account sufficient for the Platform's integrity requirements. Because this independent path always remains available, the Platform's activation and continued operation in any jurisdiction are never conditional on access to a national system. A citizen who first verified through one path and later verifies through another resolves to the same identity fingerprint, and so returns to the same account without loss of continuity.

This architecture ensures that no official – whether through deliberate obstruction, bureaucratic delay, or political pressure – can prevent the Platform from operating in any jurisdiction. The Platform's independence runs not against the state, an institution derived from society and which the Platform serves, but against those who act in its name and whom the Platform exists to hold to account.

5.9 Legal Structure Evolution

The current single-entity structure – AGPT Ltd (UK) operating all national deployments through a centralised multi-tenant architecture – is an intentional choice for the Platform's current stage. It minimises administrative overhead, eliminates inter-company complexity, and ensures that all resources are directed toward Platform development and jurisdiction activation rather than corporate structure maintenance.

This structure is not permanent by design. As the Platform scales and operational complexity grows, the architecture preserves the option to establish a separate operational entity within the

single legal space, in a member state assessed on the merits at the time. Such an entity would operate the Platform's deployments in that space under licence from AGPT Ltd, which would retain ownership of the methodology, software, and brand. The separation would simplify regulatory relationships, eliminate the need for an Article 27 Representative, and provide locally domiciled institutional partners with a locally incorporated counterparty. This step is justified only when the operational and commercial benefits clearly exceed the costs of maintaining a dual-entity structure – a threshold that is assessed continuously, not scheduled to a predetermined date.

Structural evolution is not limited to the single legal space. As the Platform extends to jurisdictions beyond the EU/EEA (§5.10), the same logic governs: where a jurisdiction can be served lawfully by AGPT Ltd as sole controller, it is; where a jurisdiction requires a locally established controller, that controller operates under licence to the Platform's published methodology, privacy architecture, and brand, all of which AGPT Ltd retains. A licensed local controller is an extension of the framework, not a fragmentation of it. The standard to which every deployment is held remains single regardless of how many controllers operate beneath it, preserving the undivided accountability described in the band architecture at the head of this section.

The Platform's long-term governance vision extends beyond conventional corporate structures. The founding commitment is that Teisond ultimately transitions from founder-operated infrastructure to citizen-governed civic institution – where the people who use the Platform hold meaningful governance rights over its direction. The full civic ownership architecture – including distributed infrastructure, token model, governance distribution, and the pathway from community formation to citizen ownership – is described in Section 9.

5.10 Jurisdictions Beyond the Single Legal Space

The EU/EEA band (§5.1 to §5.8) is the foundation of the Platform's legal framework, but it is not its boundary. The mission is universal (§1.7); jurisdictions outside the single legal space are admitted under purpose-built legal constructions and activated through the same mechanism of configuration and subdomain that governs every deployment (§5.3.1). No architectural redesign is required. What a new jurisdiction requires is not new code but a closed legal construction, and the discipline of admission is uniform: four conditions must be satisfied before any jurisdiction beyond the single space is activated.

The first is a lawful basis for the controller relationship: a recognised legal route by which citizen data originating in the jurisdiction is processed by AGPT Ltd, or, where the jurisdiction requires it, by a local controller operating under licence to the Platform's published standard (§5.9).

The second is an independent path of verification: confirmation of one citizen, one account without dependence upon the systems of the officials the Platform monitors, through a national electronic identity scheme as the preferred path and an authorised independent provider as the always-available alternative (§5.8).

The third is a mechanism of consumption tax: subscription revenue collected and remitted in compliance with the tax law of the jurisdiction, whether through the Platform's Merchant of Record or, where required, by direct registration.

The fourth is a defined regime of speech and dispute: the legal environment governing publication about named officials, and the forum for resolving disputes, identified and addressed before activation, with the Terms of Service adapted accordingly (§5.5.1, §5.6.1).

Where a jurisdiction lacks the procedural layer the band provides, whether an intermediary-liability framework or transposed anti-SLAPP safeguards, the mitigation the band itself relies upon before full transposition applies equally: dedicated insurance, clearly defined Terms of Service, and qualified counsel within the jurisdiction (§5.5.1, §5.5.3). Where the gap cannot be closed by mitigation, the jurisdiction is not activated until it can be. The fourth condition is a condition, not a preference.

This band is therefore defined not by a region but by a method: any jurisdiction, anywhere, may be admitted once these four conditions are closed. The construction is written once and applied thereafter, and each admitted jurisdiction is published, with the composition of the network, on teisond.com.

5.11 Conclusion: Legal Framework as Mission Enabler

The legal framework described in this section is designed to do one thing well: to enable a company registered in the United Kingdom to operate an infrastructure of civic accountability across the jurisdictions it serves, while protecting the privacy of citizens, maintaining methodological independence, and complying with the regulatory requirements of every jurisdiction in which it operates.

The framework is deliberately simple at this stage. A single legal entity serves as data controller, platform operator, and commercial counterparty across all jurisdictions. Privacy is enforced by architecture – one-way hashing, aggregates-only publication, jurisdictional data isolation – not by policy commitments that could be reversed. Liability is centralised and insured. Dispute resolution is accessible to citizens in their own jurisdictions. Contingency mechanisms preserve operational flexibility without over-engineering for scenarios that may never materialise.

As the Platform scales, the legal structure will evolve – from single-entity to dual-entity if EU operational presence justifies it, from bootstrapped contingency planning to formal resilience infrastructure, and ultimately toward governance models that give citizens a direct stake in the infrastructure they use. The framework described here is built to accommodate that evolution without requiring reconstruction – each component can be extended, replaced, or supplemented as operational reality demands.

The measure of this legal framework is not its sophistication but its adequacy: whether it enables the Platform to operate and to grow while keeping every commitment made in the Neutrality Charter and in the Sovereignty and Trust Framework. The commitments are permanent. The structures implementing them will adapt.

SECTION 6: GOVERNANCE AND ETHICS

Teisond is democratic infrastructure requiring governance that ensures it serves the public interest, resists capture, and maintains integrity under pressure. Governance for a civic accountability platform carries a specific burden: the Platform applies visibility discipline to officials, and must therefore apply the same discipline to itself. This section establishes the governance framework guiding all Platform decisions – principles embedded in operating standards, enforced through architectural constraints, and subject to external accountability.

6.1 Governing Principles

6.1.1 Independence and Neutrality

The Platform maintains strict independence from governmental, partisan, and commercial interests. This independence is not aspirational – it is structurally enforced through architectural, legal, and operational commitments.

AGPT Ltd operates all national deployments as a single entity with no governmental ownership, no partisan investors, and no political affiliations. Officials being monitored cannot influence Platform operations, methodology, or data presentation – the centralised multi-tenant architecture means no local actor has access to modify code, methodology, or publication rules. The Platform monitors officials across all parties and ideologies without favour – legitimacy indices apply uniformly regardless of political category, and the Neutrality Charter, published on every national Platform, commits Teisond to this principle publicly.

While the Platform operates as a sustainable business, commercial imperatives never override the accountability mission. Subscribing officials cannot purchase preferential treatment, suppression of unfavourable indices, or influence over methodology. Calculation methods and privacy protections remain consistent regardless of external pressure, with changes occurring only through documented, transparent processes with public changelogs.

6.1.2 Transparency and Auditability

A Platform that demands transparency from public officials must practise transparency itself. Teisond implements this principle across every layer of its operations.

All calculation methods, aggregation formulas, and data processing procedures are fully documented and publicly available. The Platform's methodology is described in sufficient detail – in this White Paper and in the published technical documentation – to enable independent verification by any researcher, journalist, or interested party. As the Platform matures, additional transparency measures are planned: publication of core calculation logic as open source, third-party security audits by independent cybersecurity firms with results published in full, and annual financial

summaries showing revenue sources and major expenses. The timeline for these measures is defined in the Security and Compliance Roadmap (§ 7.7).

6.1.3 Privacy Protection as Foundational Commitment

Privacy protection is architectural, not policy-based. The system is designed so that individual judgments cannot be publicly linked to specific citizens – not through access controls that could be overridden, but through database schema that excludes the fields necessary for such linkage (see § 5.4 for comprehensive data governance framework).

The Platform never stores histories of judgment, demographic correlations, or behavioural patterns. API endpoints technically cannot return individual-level data. Political profiling is architecturally impossible. This standard of privacy by impossibility exceeds regulatory requirements and provides the strongest available protection for citizens exercising political judgment. The question is not whether the Platform will protect privacy, but whether anyone – including the Platform's own operators – could violate it. The architectural answer is no.

6.1.4 Accessibility and Inclusion

Legitimacy monitoring infrastructure is only as strong as the breadth of participation it enables. If the Platform is accessible only to the technically literate, the urban, or the affluent, the indices it produces will reflect a skewed population – undermining both their statistical validity and their democratic legitimacy.

The Platform is designed for maximum participation: free citizen access (the judgment function is never paywalled), multilingual interfaces in every national deployment language, accessibility compliance with WCAG standards, progressive web application design eliminating app store installation barriers, and low-bandwidth optimisation for areas with limited connectivity. Accessibility is not an add-on feature – it is a design constraint applied from initial architecture, tested across devices and connection conditions, and monitored as a key performance indicator.

6.1.5 Sustained Operation and Long-Term Commitment

Legitimacy monitoring infrastructure must operate continuously and indefinitely. A Platform that collects years of citizen judgments and then shuts down does more damage than one that never existed – it betrays the trust of participants and discredits the concept.

The Platform is designed for financial sustainability from the outset – diversified revenue streams from official subscriptions and Data Access subscriptions reduce dependence on any single source. As revenue grows, the Platform builds operational reserves as a buffer against temporary disruption. Contingency planning – including hosting migration procedures, payment processing alternatives, and domain failover – is embedded in the Platform's architecture from the outset of operations (see §5.7). AGPT Ltd's long-term commitment to sustained operation is formalised in the Platform's Terms of Service, establishing clear obligations regarding continuity of service, advance notice of any national deployment closure, and GDPR-compliant data portability and erasure procedures for affected citizens.

6.2 Roles and Jurisdictions Passport

6.2.1 Parties and Corporate Roles

AGPT Ltd (UK) is the sole operator of the Teisond Platform across all jurisdictions. It owns the methodology, software, and brand. It operates all national deployments through a centralised multi-tenant architecture. It acts as data Controller for each national Platform under GDPR. It manages all subscription revenue, hosting infrastructure, and regulatory compliance.

National deployments are jurisdiction-specific configurations of the single Teisond Platform, operated by AGPT Ltd. Each deployment stores citizen data in infrastructure appropriate to its jurisdiction. National deployments are not separate legal entities – they are isolated tenants within a single codebase managed by AGPT Ltd. This structure ensures methodological consistency, privacy uniformity, and centralised incident response across all jurisdictions.

Citizens are free Platform users who verify their identity through the Platform's verification process, render judgments of trust or distrust in respect of officials, and view published indices. Officials are objects of monitoring – public figures exercising governmental authority – and optional subscribers to analytics concerning their own mandate.

6.2.2 Contracting and Dispute Resolution

Subscriber Terms govern the relationship between AGPT Ltd and paying subscribers (officials, media organisations, researchers, civic organisations and consultancies). These terms are governed by English law, with local consumer protection applying where mandatory.

User Terms govern the relationship between AGPT Ltd and citizens. These terms are governed by the local law of the citizen's country of residence, with disputes subject to local courts. This ensures that citizens are never required to litigate in a foreign jurisdiction to exercise their rights.

The separation between Subscriber Terms and User Terms reflects the Platform's dual nature: a commercial product for subscribers and a civic infrastructure for citizens. The legal frameworks for each are designed to serve their respective audiences appropriately.

6.2.3 Data Protection Compliance

AGPT Ltd operates as data Controller for all national Platforms, bearing full responsibility for lawful data processing in each jurisdiction. GDPR serves as the baseline standard applied uniformly across all deployments – including any future deployments outside the EU where equivalent or higher standards are adopted. This baseline-up approach means the Platform never operates below GDPR-level protections, regardless of what a specific jurisdiction might permit.

Citizen data for each jurisdiction are stored in infrastructure appropriate to that jurisdiction, ensuring compliance with data residency requirements independent of AGPT Ltd's UK domicile. Cloud infrastructure providers act as Sub-processors under data processing agreements that specify technical and organisational measures, breach notification timelines, data deletion and return procedures, and audit rights. AGPT Ltd conducts due diligence on Sub-processors before engagement and maintains contractual rights to audit compliance.

As a UK-registered entity processing the personal data of residents of the European Union, AGPT Ltd has appointed an EU Representative pursuant to Article 27 GDPR. The Representative acts as the designated point of contact for data protection authorities and for data subjects. The Representative's identity and contact details are published in the Privacy Policy on every national Platform. This appointment supplements – but does not replace – AGPT Ltd's direct responsibility as data Controller.

6.2.4 Revenue and Taxation

AGPT Ltd collects and manages all subscription revenue centrally. The company's tax structure – UK Corporation Tax on worldwide profits, consumer-facing VAT managed through the Platform's Merchant of Record payment partner – is described in § 5.5.4. This centralised approach eliminates the inter-entity transactions, transfer pricing obligations, and multi-jurisdictional corporate filings that would arise from a more complex corporate structure.

6.2.5 Regulatory Posture

The Platform operates as an information service – it publishes aggregated statistical data about public acceptance of governmental authority. It is not a financial instrument, not a political organisation, and not a media publisher. This classification is significant because it determines which regulatory frameworks apply. The Platform does not make editorial decisions about content (indices are mathematically computed, not curated), does not offer financial products or investment advice, and does not engage in political campaigning or advocacy.

6.3 Ethical Commitments and Boundaries

6.3.1 Commitment to Democratic Values

The Platform exists to strengthen democratic accountability – not to serve as a tool for authoritarian surveillance, partisan advantage, or commercial exploitation. This commitment has operational consequences.

Admission of a jurisdiction requires assessment of democratic conditions: the Platform does not deploy where monitoring infrastructure could be repurposed for political persecution, and the criterion of admission is the mark of a consolidated democracy under the classification of independent international institutions (§1.7). The Platform monitors governmental authority regardless of political orientation – it is neither a progressive nor a conservative instrument, but accountability infrastructure that applies uniformly. The Neutrality Charter, published on every national Platform, formalises these commitments in a publicly binding document.

6.3.2 Commitment Against Harassment and Abuse

The Platform enables structured civic judgment, not harassment. The binary trust/distrust mechanism without free-text commentary is a deliberate design choice: it prevents the Platform from becoming a vehicle for personal attacks, defamatory statements, or coordinated abuse campaigns. There are no comment sections, no public forums, no messaging features.

Officials facing declining indices may experience discomfort – this is accountability, not abuse. The Platform clearly distinguishes between legitimate accountability pressure (public visibility of aggregated civic sentiment) and harassment (targeted personal attacks). For officials who experience threats or intimidation as a consequence of their public indices, the Platform maintains documented protocols for cooperation with law enforcement while preserving the integrity and publication of the indices themselves.

6.3.3 Commitment to Evidence-Based Operation

Methodology decisions follow evidence and statistical best practice, not political convenience or commercial pressure. Anti-manipulation algorithms are validated against empirical data before deployment. Publication thresholds are statistically grounded – minimum sample sizes, confidence intervals, and rounding rules are derived from established statistical methodology, not arbitrary choices.

Claims about Platform impact are verified through independent research rather than marketing assertions. The Platform welcomes external scrutiny of its methodology and publishes sufficient documentation for independent replication. If research reveals methodological weaknesses, the Platform commits to addressing them transparently – including publishing the finding, the response, and the timeline for remediation.

6.3.4 Commitment to User Agency and Control

Citizens control their participation at every stage. They can render judgment on any mandate in the system, change that judgment as circumstances evolve, withdraw it entirely, or delete their account permanently. No citizen is locked into the Platform without the ability to modify or exit their engagement, and account deletion is irreversible: all personal data are permanently removed, and the withdrawn judgment ceases to stand and is absent from every subsequent snapshot.

Officials exercise the right of reply through official statements published alongside their own index. An official may publish a statement visible to every citizen viewing that index, offering context or explanation in the same plane of public visibility in which the index appears. The Platform provides the channel; it neither moderates nor edits what is placed in it, and it neither expects nor requires that the channel be used.

6.4 Stakeholder Relationships and Accountability

6.4.1 Citizens (Participating Users)

The Platform owes citizens: free access to the judgment function without paywall or conditions beyond identity verification; privacy protection through architectural impossibility of identification; transparent methodology enabling citizens to understand how their judgments become indices; responsive support for account, verification, and data access issues; and honest communication about the Platform's capabilities and limitations – including what the index does and does not measure.

Citizens owe the Platform: honest judgments reflecting a genuine personal assessment, neither paid for nor coerced; compliance with verification on the basis of one citizen, one account; and

respect for the Platform's structured binary format. The Platform has no mechanism for verifying sincerity, but the architecture of one citizen, one account ensures that even where individual judgments are strategic rather than sincere, they cannot be multiplied or amplified beyond a single signal per citizen.

6.4.2 Officials (Objects of Monitoring and Subscribers)

Officials occupy a dual position: they are objects of monitoring and potential subscribers. The Platform owes officials a fair and uniform methodology applied identically irrespective of party, ideology or subscription status; protection of their personal data, as distinct from their public indices of legitimacy; the right of reply through published statements; access to methodology documentation sufficient to understand how indices are computed; and equal treatment whether or not they subscribe.

Subscription purchases analytics access – never influence over indices, methodology, or treatment. Non-subscribing officials receive identical public indices as subscribers. This separation is absolute and architecturally enforced.

The Platform does not seek officials' consent for monitoring. Public officials exercising governmental authority are subject to civic scrutiny as an inherent aspect of their public role. This parallels media coverage, freedom of information requests, and electoral accountability – mechanisms that operate without requiring officials' agreement to be monitored.

6.4.3 Media Organisations

The Platform provides media with structured data, transparent methodology, and API access enabling integration into journalistic workflows. For media, the Platform is a permanent, verified data source that supplements (not replaces) traditional political reporting.

Media organisations maintain full editorial independence in interpreting and presenting indices. The Platform does not control media narratives, approve coverage, require favourable treatment as a condition for data access, or restrict critical reporting. If a journalist uses the data to argue that the Platform's methodology is flawed, the Platform's response is to engage with the criticism – not to restrict access.

6.4.4 Researchers and Academia

The Platform provides researchers with comprehensive data access (aggregated, anonymised datasets), transparent methodology documentation, and active cooperation in validation studies. The Platform anticipates that Public Legitimacy Analytics will become an academic subfield and actively supports its development.

Research findings – including critical ones – are welcomed as contributions to Platform improvement. Academic independence is unconditionally protected: the Platform does not review, approve, restrict, or delay research publications. If peer-reviewed research identifies methodological weaknesses, the Platform treats this as a quality signal, not a threat.

6.4.5 Civic Organisations and Civil Society

The Platform engages civil society as partners, critics, and advocates. Civic organisations can use legitimacy data for advocacy (citing indices in campaigns for governmental reform), analysis (longitudinal tracking of accountability patterns), and civic education (teaching citizens about democratic oversight mechanisms).

The Platform maintains independence from any particular civil society organisation – it does not endorse specific advocacy positions, campaigns, or political outcomes. It supports the civic ecosystem broadly by providing reliable, neutral data that any organisation can use according to its own mission.

6.4.6 Consultancies and Institutional Subscribers

The Platform provides consultancies and institutional subscribers with the same data available to media and researchers – legitimacy indices, comparative benchmarks, anomaly reports, and API access. Use cases include political advisory, stakeholder mapping, risk assessment, and strategic communications. The Platform does not endorse, validate, or take responsibility for the conclusions that consultancies draw from its data. Legitimacy indices are inputs to analysis, not conclusions – and the Platform maintains strict neutrality with respect to how subscribers apply the data in their professional practice.

6.5 Ethical Dilemmas and Resolution Frameworks

Governance principles provide compass bearings; real-world situations require judgment. This section describes four tensions the Platform will inevitably face and the frameworks for navigating them.

6.5.1 Privacy Versus Transparency

When research requests require data granularity approaching individual identification, privacy takes precedence – even at the cost of reduced analytical utility. The Platform errs systematically toward privacy protection. This is not a case-by-case judgment but a standing rule: if there is doubt about whether a data release could enable re-identification, the data is not released.

The deferred demographic extension illustrates this principle in practice. Demographic breakdowns of legitimacy data (by age, gender, region) would be analytically valuable for researchers and media. The Platform deliberately excludes this capability from the core product – it will be considered only if and when privacy safeguards are proven adequate through independent assessment. Potentially valuable research capability is deferred rather than risk citizen exposure.

6.5.2 Neutrality Versus Justice

If indices in certain regions reflect discriminatory patterns – for example, if officials from minority backgrounds consistently receive lower indices than peers with comparable conduct – the Platform faces a tension between methodological neutrality and social justice.

The Platform's resolution is clear: it measures accurately without manipulating indices to correct suspected bias. Methodology integrity is maintained unconditionally. The Platform does not adjust results to produce outcomes it considers more just – this would make the Platform an editorial actor rather than a measurement instrument, destroying the neutrality that makes the data credible.

However, neutrality does not mean silence. The Platform provides contextual information helping users interpret potential patterns. Research examining bias in legitimacy data is actively supported. But correcting injustice is society's work – through education, legislation, institutional reform – not the Platform's algorithmic adjustment.

6.5.3 Sustainability Versus Mission

When funding relationships would compromise independence, mission takes precedence regardless of financial consequences. This is not a hypothetical – it is a predictable scenario. A government may offer partnership funding contingent on methodology modifications. A commercial entity may offer sponsorship contingent on data access beyond published parameters. A political actor may offer support contingent on favourable treatment.

The Platform's resolution: revenue diversification reduces dependence on any single source, making it possible to refuse compromising offers. If diversification proves insufficient, the Platform is willing to scale back operations – narrowing its jurisdictional scope, deferring expansion, or operating at reduced capacity – rather than accept revenue that would compromise independence.

6.5.4 Official Responsiveness Versus Populism

Officials may abandon sound but unpopular policies to improve their indices. This is a legitimate concern – and it is inherent to democracy itself, not specific to Teisond. Elections create identical incentives: officials routinely adjust positions based on polling data, focus group research, and electoral calculus.

The Platform measures legitimacy – public acceptance of authority – not governance quality. An official who makes unpopular but wise decisions may see a declining index; an official who makes popular but harmful decisions may see a rising one. Distinguishing between responsive governance and populist pandering is society's responsibility, exercised through media scrutiny, expert analysis, institutional checks, and the voters' own judgment. The Platform provides a signal; interpreting that signal requires the full ecosystem of democratic institutions.

6.6 Governance Evolution and Future Considerations

6.6.1 Long-Term Governance Direction

As the Platform matures, governance evolves beyond the founder-led model toward structures that give citizens a direct role in stewarding the infrastructure they use. The civic ownership architecture – including distributed infrastructure, token model, governance distribution between community and professional management, and the concrete pathway from community formation to citizen ownership – is described in Section 9. The scope boundary is fixed: community governance extends to publication conventions, transparency standards, labelling formats, governance structure changes, and strategic direction; it never extends to personal data handling, index calculation methodology, operational security, or regulatory compliance (§ 9.4).

6.6.2 Advisory Board and Stakeholder Councils

As the Platform scales beyond its initial national deployments, formal advisory structures provide external expertise and diverse perspectives without binding operational authority.

Formal advisory structures provide legitimacy-enhancing consultation and diverse perspectives without binding authority. Planned structures include an Ethics Board (political philosophy and democratic theory scholars providing guidance on ethical dilemmas and boundary cases), a Methodology Council (statisticians and political scientists advising on index calculation, threshold settings, and anti-manipulation approaches), a User Council (representative citizens providing feedback on Platform design, accessibility, and communication), and a National Platform Advisory Council (coordinating standards across national deployments).

These advisory bodies complement rather than replace operational decision-making. AGPT Ltd retains final authority on operational matters – advisory input informs decisions but does not bind them. This structure ensures that the Platform benefits from diverse expertise without creating governance paralysis or capture by advisory interests.

6.6.3 Conclusion

Governance is continuous practice, not fixed design. The Platform will face pressures to compromise independence for financial gain, manipulate methodology for political advantage, and sacrifice privacy for analytical convenience. These pressures are not hypothetical – they are inevitable consequences of operating civic accountability infrastructure in politically charged environments.

Principles provide compass bearings; navigating toward them requires judgment, institutional culture, and willingness to uphold principles against pressure. The governance framework described in this section is designed to make the right decisions easier and the wrong ones harder – through architectural constraints, public commitments, external accountability, and a culture of transparency that begins with the Platform itself.

SECTION 7: ROADMAP AND IMPLEMENTATION

This Section outlines Teisond's deployment strategy and timeline. The approach reflects the Platform's centralised, multi-tenant architecture: simultaneous presence across its launch set from day one, with progressive deepening of functionality. The roadmap is designed for a digital-first platform that requires no physical infrastructure per country – enabling a pace of geographic expansion that would be impossible for a traditional service organisation.

7.1 Simultaneous Presence

Teisond's strategy of deployment rests on a simple observation: a digital-first platform requiring no physical infrastructure in any country has no reason to arrive sequentially. Every jurisdiction meeting the criterion has a national presence from the outset, in its own language and under its own subdomain, and that presence exists whether or not the national platform has yet been activated in full.

This approach serves two purposes. First, it occupies the nascent space of legitimacy measurement as a whole rather than country by country, establishing Teisond as the reference platform for Public Legitimacy Analytics across the democracies it serves. Second, it communicates what the project actually is: an infrastructure conceived for consolidated democracies as a class, not an experiment in a single country that might later be exported. A social institution of this kind forms its environment by the fact of its presence in the public space, and presence therefore precedes activation rather than following it.

7.2 Activation as Readiness Permits

The Teisond project is not announced; it operates. Activation of a national platform in full requires two things and no others: a connected channel of identity verification, whether the national digital identity system or an authorised provider, and a populated national database of the mandates to be monitored.

Of these, only the second takes appreciable time. Verification is a matter of integration, and the multi-tenant architecture means that no code is written for a new country at all: a configuration file describes the national institutional structure, and the same software serves every jurisdiction. The period required for a further jurisdiction to join the operating network accordingly amounts to a matter of days, and the Platform publishes that figure as an operational metric rather than treating it as an internal statistic.

The pace of expansion is limited solely by the operational readiness of the national databases. It is not limited by engineering capacity, by financial cycles, or by any assessment of consumer demand: the criterion of admission to the network is the mark of a consolidated democracy, and nothing in the sequence of activation is determined by how many citizens have signalled interest in advance. The architecture imposes no limit on how many jurisdictions may be activated at once. Where a dozen national databases reach readiness in the same week, a dozen national platforms open in the same week.

7.3 Phased Functionality

Each national deployment passes through defined phases. The timelines below are relative to the activation of the jurisdiction concerned; later jurisdictions follow the same sequence at an accelerating pace as operational practice matures.

Phase 0, national presence. A national page in the language of the jurisdiction, carrying a description of the Platform, the Neutrality Charter, and the current state of preparation for that country. Its purpose is presence: to make the project findable, legible and verifiable in the national language before any judgment can be rendered.

Phase 1, population of the database, four to eight weeks before activation. The Platform's operational team populates the national database with Level 1 mandates, meaning members of parliament, ministers and heads of national agencies, from official government registries, parliamentary rosters and publicly available institutional records. The database draws only on information describing a public office and the person holding it, namely position, jurisdiction, level of authority, and name as published in official sources, all of which remains publicly accessible by its nature as a record of public function. Where a jurisdiction restricts access to particular registers, the Platform sources the same information from the registers and institutional directories that remain open, since what it requires is the public fact of who holds which office and no protected personal attribute. Expansion to Levels 2 to 4 proceeds progressively after activation, with AI agents systematically identifying and cataloguing mandates at regional, municipal and local levels from public records, government rosters and institutional directories.

Phase 2, civic participation, from activation day. Identity verification is live, citizens may register and render judgments of trust and distrust, and the Platform begins computing indices at the cadence configured for the jurisdiction. Until a mandate reaches the publication threshold for its level of authority, the profile shows the progress of accumulation rather than a ratio. The transition from Phase 1 to Phase 2 is the public opening of the country.

Phase 3, full operation, eight to twelve weeks after activation. Subscriptions for officials and Data Access for institutional subscribers are activated. Comparative analytics, historical series and anomaly reporting are fully operational. The Platform then enters what may be called quiet presence: accumulating judgment, serving its users, refining its indices, and letting the numbers speak for themselves.

7.4 Election Sensitivity

Democratic legitimacy monitoring must be especially careful during election periods – the moment when public attention to political data is highest and the potential for misuse or misinterpretation is greatest.

The Platform operates freeze windows during electoral periods in each jurisdiction. During a freeze no new features are deployed, no changes of methodology are made, no thresholds are adjusted, and the Platform's communication is confined to factual operational notices. Existing indices continue to be published and recalculated as normal: the freeze applies to changes made by the Platform, not to the judgments of citizens. Citizens continue to judge officials throughout an electoral period, and the Platform simply refrains from any act that could be perceived as influencing the electoral process.

Specific freeze periods are configured per country in accordance with local electoral legislation. In countries with staggered regional elections, freezes apply to the affected region's officials while other regions continue normal operation. The freeze mechanism is documented in the Platform's public methodology and activated automatically based on the country configuration file.

7.5 Long-Term Vision

The purpose towards which the Platform is built is to operate as standard civic infrastructure across the democracies it serves: a permanent, neutral, privacy-preserving channel through which citizens in any jurisdiction of the network may render and follow their acceptance of officials at every level of government.

The Platform's success will be measured not by metrics of engagement but by whether indices of legitimacy become a routine point of reference in democratic discourse, cited by the media alongside electoral results and economic indicators, consulted by officials as feedback that bears on a career, used by researchers as a standard dataset for the study of accountability, and trusted by citizens as a reliable reflection of collective judgment.

The stages of that ascent are qualitative rather than calendrical. The first is operational maturity: every activated national platform running stably and approaching financial self-sufficiency. The second is institutional recognition: continuous monitoring of legitimacy acknowledged as an accountability mechanism in its own right, alongside elections, courts, the media and civil society. The third is ubiquity: coverage extending across the greater part of the world's consolidated democracies, with the Platform functioning as ordinary democratic infrastructure. Beyond that lies a change the Platform cannot itself schedule, in which officials who have known continuous monitoring of legitimacy for the whole of their careers govern differently from the generation that knew only episodic accountability.

The pace of that progression rests on the Platform's architecture: configuration-driven deployment, automation-first operations, and sublinear scaling of cost. Expansion is constrained by the readiness of national databases and of verification infrastructure, and by nothing else.

7.6 Infrastructure and Partner Ecosystem

The Platform's operational infrastructure rests on a curated ecosystem of external service providers, each chosen for compatibility with an early-stage operation, for alignment with the regulatory regime binding the operator, and for the ability to scale alongside the Platform without a change of provider. The guiding principle is deliberate simplicity: one primary provider serves each function, with architectural independence preserved so that a switch remains possible should commercial terms, quality of service or regulatory conditions change.

Identity verification is provided through national digital identity systems where these exist and are connected, and otherwise through an authorised verification provider operating across the jurisdictions the Platform serves. The provider layer is selected for GDPR-compliant architecture, broad document coverage, and white-label capability allowing the experience of verification to feel native to each national platform. National digital identity is the preferred path wherever it exists; the authorised provider guarantees that verification works in every jurisdiction regardless, so that the Platform never depends on a single piece of national infrastructure, least of all one administered by the party it monitors.

Payment processing and tax compliance are managed through a Merchant of Record partner, which acts as the legal seller of all subscription services and handles the collection of payment, the calculation and filing of VAT across the European Union and the European Economic Area, the generation of invoices, the management of chargebacks and the conversion of currency. AGPT Ltd receives net payouts once all tax obligations have been settled, which removes the need for direct VAT registration in individual member states and with it one of the heaviest operational burdens facing any company selling digital services into that regulatory space.

Cloud infrastructure is hosted by a provider with data centres inside the European Union, which secures compliance with requirements of data residency. The Platform uses standard database formats and documented deployment procedures, with no proprietary data formats and no vendor lock-in, preserving the ability to migrate to an alternative provider should that become necessary.

Representation under the EU General Data Protection Regulation is provided by a specialist compliance firm appointed pursuant to Article 27, serving as the designated point of contact for data protection authorities and for data subjects. The representative also supplies privacy operations tooling, including a system for managing the requests of data subjects and an incident management system for the notification of data breaches, which gives the Platform baseline compliance infrastructure from the first day of operation.

Legal services are provided through a credit-based legal platform specialising in cross-border startup operations. This model provides access to GDPR specialists, contract lawyers, and corporate counsel across multiple jurisdictions without retainer commitments – legal capacity scales with operational needs rather than imposing fixed costs during pre-revenue periods. For matters requiring specialist English law or complex regulatory expertise, a boutique digital law firm with dual qualification in English and EU law serves as secondary counsel.

Accounting and financial compliance are managed by a UK-based firm specialising exclusively in startups and scale-ups, providing bookkeeping, tax filing, payroll, and investor-ready financial reporting. The choice of a startup-specialist accountant – rather than a general-purpose provider – reflects the expectation that the company's financial reporting needs will evolve rapidly as it transitions from pre-revenue to active operations to fundraising.

Automated communications – transactional notifications, subscription confirmations, alert emails, and data subject request acknowledgements – are delivered through a dedicated email infrastructure provider, separate from the company's person-to-person email. This separation ensures that automated Platform communications maintain high deliverability without interference from general business correspondence.

All external service providers processing personal data on behalf of AGPT Ltd operate under Data Processing Agreements specifying technical and organisational measures, breach notification timelines, data deletion procedures, and audit rights. DPA execution follows a staged schedule aligned with the Platform's deployment phases: providers handling citizen data (cloud infrastructure, identity verification) require executed DPAs before the first country activation; providers handling subscriber data (payment processing) require executed DPAs before subscription services launch; providers handling only operational data (email infrastructure, accounting) require executed DPAs before the relevant service begins processing personal data. Legal counsel reviews all DPAs for adequacy before execution.

7.7 Security and Compliance Roadmap

The Platform's security posture matures through defined stages, each corresponding to a level of operational scale and institutional exposure. The approach is pragmatic: security investment is directed where it produces the greatest risk reduction at each stage, rather than pursuing comprehensive certification before the Platform has users.

Stage 1 covers the pre-launch and initial activation period. Security at this stage is embedded in the development process itself. The Platform is built using AI-assisted development tools with a dual-agent methodology: one agent writes code, a second agent performs security-focused review – examining authentication flows, data encryption implementation, input validation, injection protection, and cross-site scripting defences. Before the first country activation, an independent security engineer conducts a focused code review of the Platform's critical paths: identity verification integration, cryptographic hashing pipeline, data isolation between country tenants, and publication controls. This review produces a documented assessment that serves as the Platform's initial security baseline.

Stage 2 begins once the first countries are active and citizens are using the Platform. At this point, the Platform commissions a formal penetration test from an independent cybersecurity firm. The penetration test simulates real-world attacks against the Platform's production infrastructure – probing for vulnerabilities that code review alone cannot detect, including configuration errors, network-level exposures, and authentication bypass scenarios. The resulting report – including all findings, severity ratings, and remediation steps – becomes part of the Platform's security documentation. This document can be shared with data protection authorities, institutional partners, and investors as evidence of the Platform's security posture.

Stage 3 corresponds to the Platform's growth phase, typically following the first funding round. As institutional subscribers – media organisations, research institutions, civic organisations – begin relying on the Platform's data, they will require evidence of systematic security management. SOC 2 Type II certification provides this evidence: an independent auditor examines the Platform's security controls, availability, processing integrity, confidentiality, and privacy over a sustained observation period (typically 6–12 months). SOC 2 certification is increasingly a prerequisite for enterprise contracts and institutional partnerships. The certification process also imposes internal discipline – formalising incident response procedures, access control policies, change management processes, and vendor management standards.

Stage 4 addresses long-term institutional credibility. ISO 27001 certification – the international standard for information security management systems – provides the most widely recognised evidence that the Platform manages information security through a comprehensive, auditable framework. This level of certification is relevant when the Platform operates at scale across multiple jurisdictions, processes significant volumes of citizen data, and engages with governmental or quasi-governmental institutional partners who require ISO 27001 as a baseline condition. The certification is also a signal to data protection authorities that the Platform takes its security obligations seriously beyond minimum regulatory compliance.

Each stage builds on the previous one: code review findings inform penetration test scope, penetration test findings inform SOC 2 control design, and SOC 2 controls form the foundation of the ISO 27001 management system. This progressive approach ensures that security investment produces cumulative value rather than redundant assessments.

SECTION 8: TEAM AND ORGANISATION

8.1 Organisational Philosophy

Teisond is designed as an automation-first organisation. The Platform's multi-tenant architecture, config-driven country deployment, and algorithmic index calculation mean that routine operations – publishing indices, enforcing thresholds, detecting anomalies, managing country configurations – run without human intervention. People handle exceptions, strategy, stakeholder relationships, and quality oversight. The system does the work; the team directs and governs it.

This is not a temporary staffing compromise – it is a permanent architectural choice. Adding a new jurisdiction does not require hiring a national team; it requires deploying a configuration file and connecting a verification provider. Scaling from a handful of jurisdictions to many does not proportionally increase headcount. The marginal cost of expansion is infrastructure, not personnel. This means Teisond can maintain presence across many jurisdictions with a team an order of magnitude smaller than a traditional multi-country service organisation would require.

The organisational model follows from the Platform's mission. Civic accountability infrastructure must be financially sustainable without grant dependence or extractive monetisation. Automation-first operations make this possible: low operational costs relative to deployment scale enable profitability at modest adoption rates, reducing the pressure to compromise mission for revenue.

8.2 Founder and Leadership

Oleksiy Loboyko – Founder, CEO. Nearly five years developing the Teisond concept across its theoretical, methodological, legal, and architectural dimensions. Background in strategic communications, political analysis, and civic technology.

The founder's formative experience is relevant context, not a liability. Teisond was conceived by someone who has seen at first hand what happens when infrastructure of accountability is absent – where the consequences of unchecked authority are not academic abstractions but lived realities. That experience informs the Platform's design: the insistence on privacy by construction, because citizens in vulnerable environments cannot afford exposure; the architectural impossibility of political profiling, because such tools have been abused elsewhere; and the commitment to neutrality, because an instrument that serves one political faction is a weapon, not infrastructure.

The founding stage is intentionally solo. The concept, methodology, legal architecture, and technical design have been developed to a level of completeness that allows recruitment to target execution rather than ideation. The leadership team expands as the Platform transitions from documentation to implementation – with recruitment prioritising mission alignment alongside technical capability.

A note on long-term intent: the founder's vision for Teisond is not a company to be permanently owned but infrastructure to be progressively shared. The legal architecture deliberately preserves pathways toward citizen co-governance (see §6.6 and §9.5). The founder's role is to establish and prove the model – not to retain permanent control over civic infrastructure that, by its nature, should belong to the public.

8.3 Team Development

Teisond's team grows in response to operational milestones, not predetermined timelines. The automation-first architecture means the Platform can operate its initial national deployments with a small core team; subsequent hiring is triggered by operational needs as they emerge, not by org-chart projections written years in advance.

The first hires address the functions that cannot be automated: technical leadership (platform architecture, security, privacy engineering), country expansion management (verification provider integration, official database sourcing, regulatory navigation), and legal and compliance oversight (multi-jurisdictional GDPR compliance, operating agreements, dispute resolution). These are the roles where human judgment, cross-jurisdictional expertise, and stakeholder relationships are irreplaceable.

As the Platform scales beyond its initial jurisdictions, the team expands into data science (methodology refinement, anomaly detection improvement), product management (user experience, subscriber value), and regional coordination. The principle remains constant: hire when a function demonstrably requires a dedicated person, not when an org chart says it should exist. Every role must justify itself against the alternative of automation or outsourcing.

Remote-first operations enable global talent access while reducing overhead. Compensation balances competitiveness with social enterprise positioning – competitive base salaries supplemented by equity participation rather than above-market cash. The goal is to attract people who are drawn to the mission and capable of the work, not people optimising for compensation alone.

8.4 Advisory Board

External advisors provide expertise the core team does not possess and institutional credibility that a young organisation cannot generate on its own. The advisory board is structured around the domains where independent perspective matters most: political science and democratic theory (ensuring the Platform's conceptual framework withstands academic scrutiny), data protection law (navigating compliance across the jurisdictions the Platform serves), platform business models (validating commercial assumptions and pricing strategy), and civic technology (learning from predecessors' successes and failures).

Advisory board members provide guidance without operational authority – they inform decisions but do not make them. This structure ensures diverse perspectives reach the leadership team without creating governance paralysis or diffusing accountability. Advisors are selected for substantive expertise and independence; the Platform does not appoint advisors for their names or connections.

8.5 Governance and Succession

AGPT Ltd governance follows a natural trajectory: founder-led during the startup phase, transitioning to board governance as the Platform matures and the team grows. The timing of this transition is driven by operational scale and institutional readiness, not by a predetermined date.

Succession planning begins early – not because founder departure is anticipated, but because infrastructure that serves millions of citizens across many countries must not depend on any single individual. Documentation of methodology, strategic rationale, stakeholder relationships, and operational procedures ensures continuity. Key-person dependencies are systematically identified and mitigated through knowledge distribution, cross-training, and documented decision frameworks.

The long-term governance vision – described in § 6.6 and § 10.5 – includes potential citizen participation in Platform governance. Whether governance evolves toward decentralised participation or remains within a traditional board structure, the principle is the same: the Platform's governance must be resilient enough to survive the departure of any individual, including its founder.

8.6 Community as Institutional Foundation

Civic accountability infrastructure that monitors officials exercising governmental authority operates in an inherently adversarial environment. Legal protections (Section 5) and architectural resilience (Section 3) address institutional and technical dimensions of this exposure. Neither is sufficient alone. A Platform that relies exclusively on legal rights and server architecture remains vulnerable to a class of threats that neither lawyers nor engineers can neutralise: sustained political pressure, coordinated reputational campaigns, or strategic withdrawal of commercial partnerships under governmental influence. The missing layer is social: a publicly visible community whose documented commitment to the Platform's mission makes interference politically costly.

This community is not expected to emerge organically. It is built through three deliberate mechanisms, deployed in sequence as the Platform matures. The first mechanism is the Platform itself. From launch, every verified citizen who renders judgment becomes a documented stakeholder – a person who has invested identity verification, time, and a civic act into infrastructure that did not exist before. The accumulated base of verified participants is the Platform's most fundamental source of institutional weight: not users of a service, but citizens exercising a right they did not previously have. The second mechanism is professional stakeholder formation through the Data Access tier. Journalists who build editorial workflows around legitimacy indices, researchers who publish studies using Platform data, civic organisations that integrate benchmarks into advocacy – each develops a professional dependency on the Platform's continuity. This layer is smaller in number but disproportionate in influence: a newspaper that regularly cites NOLI scores has both the incentive and the public reach to challenge any attempt to suppress the data source. The third mechanism is targeted public mobilisation: civic crowdfunding campaigns, a public supporter registry, and academic validation partnerships with research institutions whose independent assessment of the Platform's methodology provides external credibility. These instruments convert diffuse public sympathy into a documented, countable, and citable base of support.

The strategic logic is straightforward. Pressure against a solo founder operating a UK limited company is low-cost and low-risk for the aggressor. Pressure against a Platform with thousands of

verified citizens, dozens of professional subscribers whose published work depends on its data, a public register of named supporters, and independent academic endorsement of its methodology is a qualitatively different proposition – one that generates media coverage, parliamentary questions, and reputational damage for the entity applying pressure.

Community formation does not replace legal and architectural protections – it complements them. All three layers operate simultaneously: legal structures define rights and remedies, architecture prevents single points of failure, and community raises the political cost of interference. The Platform's institutional resilience is the product of all three, not any one in isolation.

The community formation strategy described above has a direct relationship to the Platform's civic ownership trajectory (Section 9). Founding supporters who contribute to the Platform's early community – whether through civic participation, professional engagement, or financial backing via civic crowdfunding – represent the natural constituency for the governance mechanisms described in §§ 9.3–9.4. When the Platform issues utility tokens, early documented supporters constitute the first cohort with a demonstrated stake in the infrastructure they helped establish. Community formation is therefore not merely a protective strategy – it is the first practical step toward citizen ownership.

SECTION 9: CIVIC OWNERSHIP ARCHITECTURE

9.1 The Principle: Value Belongs to Those Who Create It

The Platform produces an informational product: continuous, structured and verified data on legitimacy covering officials across the democracies it serves. That product has measurable economic value, and media organisations, researchers, consultancies and civic organisations pay for access to it (Section 4). Yet the body of judgment from which the product is built arises from the participation of citizens, who under conventional platform economics would receive nothing in return for it. Participation generates the aggregate; the profit accrues to the entity.

This model is familiar. Social media platforms monetise user-generated content, attention, and behavioural data without sharing ownership or revenue. Survey companies maintain respondent panels whose aggregate output drives multi-billion-dollar industries while individual panellists receive token compensation or none at all. In each case, the underlying economic logic is the same: the platform captures value created by its users and distributes it to shareholders who may never have used the product.

Teisond rejects this logic as both ethically inconsistent and architecturally unsound. A Platform that invites citizens to render judgment on the officials exercising authority over their lives, and then treats the resulting body of judgment as the private asset of a privately owned business, reproduces the very asymmetry it exists to correct. Citizens would exchange one form of voicelessness for another: instead of having no mechanism through which to express judgment, they would have a mechanism whose output they neither own nor control.

The architectural commitment is therefore explicit: the Platform is designed from its first line of code for eventual citizen ownership. Every mechanism described in this White Paper – from identity architecture to community formation (§ 8.6) to the governance trajectory described later in this Section – is a step on this path. The destination is fixed; the specific legal and technical forms through which ownership is expressed will be determined by regulatory conditions and technological maturity at the time of implementation.

9.2 Distributed Infrastructure

Citizen ownership of civic infrastructure is meaningless if the infrastructure itself resides on servers controlled by a single entity. A company that holds all data can be compelled to delete it, alter it, or surrender it – regardless of what governance documents promise. Genuine ownership requires that the infrastructure physically cannot be captured, because it does not exist in any single location.

Teisond's long-term architectural trajectory is therefore distributed: national databases replicated across the devices of participating users, with node operators maintaining local copies of the cryptographically verified dataset for their jurisdiction. Blockchain technology serves here not as a fashionable label but as the only proven mechanism for maintaining a tamper-evident, collectively held ledger where no single party – including the founding entity – can unilaterally modify or delete records. Each judgment, once cryptographically committed, becomes part of a permanent, auditable, collectively maintained dataset.

Node operators – citizens who dedicate device storage and processing capacity to maintaining the network – occupy a structurally privileged position. They bear the cost of infrastructure maintenance that would otherwise fall on a centralised provider, and their contribution is both measurable and essential. This privileged position is reflected in governance rights: node operators receive enhanced participation in Platform governance decisions proportional to their infrastructural contribution, without violating the one-citizen-one-account principle that governs judgment itself.

The transition from centralised to distributed infrastructure is progressive, not instantaneous. At launch and through the early operational phase, the Platform operates on conventional cloud infrastructure (Section 3) – because distributed systems require a critical mass of participants to function reliably, and because the Platform must demonstrate methodological integrity before asking citizens to host its data. The migration path is designed into the architecture from the outset: data formats, cryptographic commitments, and API structures are built to support eventual distribution without requiring reconstruction.

9.3 Token Model and Ownership Pathway

Ownership in distributed civic infrastructure requires a mechanism that is verifiable, transferable, and resistant to centralised revocation. Tokenisation – the representation of rights and stakes as cryptographic tokens on a distributed ledger – provides this mechanism.

The Platform's token model proceeds in two stages, each triggered by community readiness rather than a predetermined schedule. The first stage is utility token issuance. Utility tokens grant holders specific functional rights within the Platform ecosystem: participation in governance decisions (§ 9.4), priority access to Data Access tiers, eligibility for node operator status, and recognition as documented stakeholders in the Platform's institutional base. Utility tokens do not represent equity, do not pay dividends, and do not constitute financial instruments. They are functional keys to a civic infrastructure, issued to citizens who contribute to its existence – whether through civic participation, financial support via crowdfunding campaigns (§ 8.6), or infrastructural contribution as node operators.

The second stage is conversion from utility to security tokens – a transformation that formalises citizen ownership in legal and economic terms. This conversion is not a management decision. It is triggered exclusively by a supermajority decision of token holders themselves – requiring approval of no less than seventy-five per cent of participating holders. The threshold is deliberately high: the conversion changes the fundamental legal character of the tokens and introduces regulatory obligations under the EU's Markets in Crypto-Assets (MiCA) framework, national securities regulations, and potentially cross-border compliance requirements. A decision of this magnitude must reflect overwhelming community consensus, not a narrow majority.

The regulatory landscape for both utility and security tokens within the European Union is complex but navigable. MiCA, fully applicable since December 2024, establishes a comprehensive framework for the issuance of crypto-assets, the provision of services, and market conduct. The Platform's token design is informed by that framework from the outset, not as an afterthought but

as a design constraint. Compliance with MiCA's requirements as to white papers in the regulatory sense, reserve obligations and consumer protection is built into the token architecture before issuance rather than retrofitted afterwards. This is an area in which professional legal and regulatory advice is essential.

9.4 Governance Distribution

The question of what citizens govern – and what remains under professional management – is not abstract. It determines whether citizen ownership is substantive or decorative. Teison's answer is guided by a simple test: if a decision requires specialised expertise and carries legal liability, it belongs to professional management; if it shapes the Platform's relationship with its users and the public meaning of its output, it belongs to the community.

Community governance scope includes: publication conventions and labelling standards – how indices are presented, what contextual information accompanies them, and what terminology is used in public communications. Community guidelines – the norms governing citizen conduct on the Platform. Governance structure changes – including the threshold and process for utility-to-security token conversion. Strategic direction – whether to expand to new jurisdictions, whether to develop new data products, and how to allocate community-controlled resources. These are decisions that affect the Platform's civic character and public legitimacy – precisely the domain where citizen judgment is not merely appropriate but essential.

Professional maintenance scope includes: legal compliance across all operating jurisdictions, security operations and incident response, identity verification provider relationships, index calculation methodology, personal data handling, and regulatory reporting. These functions require specialised expertise, carry personal and institutional liability, and must be executed with speed and consistency that deliberative governance cannot provide. They are analogous to the role of a management company in a condominium: residents decide whether to renovate the lobby; professionals maintain the electrical system. Residents can replace the management company; they do not rewire the building themselves.

This distribution is not static. As the community matures and its governance capacity grows, the boundary between community and professional scope may shift. The direction of this shift is always toward greater community authority – never the reverse. Functions that move into community governance do not return to professional management. The principle is ratchet, not pendulum.

9.5 From Community Formation to Citizen Ownership

The pathway from a founder-led startup to citizen-owned civic infrastructure is not a single transition but a sequence of concrete steps, each building on the institutional foundation laid by the previous one.

The first step is community formation, described in § 8.6. Verified citizens who render judgment, Data Access subscribers whose professional work depends on Platform data, and civic crowdfunding backers who financially support the Platform's expansion collectively constitute the documented stakeholder base from which all subsequent governance structures emerge. This step requires no token issuance, no blockchain infrastructure, and no regulatory approval – only a

functioning Platform and a deliberate strategy for converting users and supporters into a visible, countable community.

The second step is utility token issuance. Once the community has reached sufficient scale and the Platform has demonstrated operational stability, governance tokens are issued to existing stakeholders – verified citizens, Data Access subscribers, crowdfunding backers, and node operators. The issuance criteria and allocation methodology are published in advance and subject to community consultation before implementation. Early supporters – particularly those who backed the Platform through civic crowdfunding before tokens existed – receive allocation that reflects their contribution to the Platform's institutional foundation at a stage when its survival was not guaranteed.

The third step is infrastructure distribution. The Platform's data layer migrates progressively from centralised cloud hosting to a distributed network maintained by node operators. This migration is technically complex and operationally sensitive – it proceeds jurisdiction by jurisdiction, with extensive testing and fallback mechanisms, and only when the node operator base in a given jurisdiction is sufficient to guarantee data availability and integrity.

The fourth step is the community's own decision regarding security token conversion – the moment when citizen ownership is formalised in legal and economic terms. This step is not scheduled, not assumed, and not within the founder's authority to initiate. It belongs to the community, requires supermajority approval, and may or may not occur depending on the community's assessment of regulatory conditions, institutional readiness, and collective preference. The founder's role is to ensure that the option exists – not to exercise it.

The measure of success for this trajectory is specific: a Platform that continues to operate with full methodological integrity, privacy protection, and public trust – without any single individual, company, or jurisdiction being necessary for its survival. Not a platform that belongs to its founder and serves its users, but a protocol that belongs to those who use it and is maintained by those it serves.

SECTION 10: CONCLUSION

10.1 The Case for Continuous Legitimacy Monitoring

This White Paper has established that modern representative democracy suffers from two interconnected accountability deficits: the deficit of extra-electoral influence, which affects elected officials between elections, and the deficit of legitimate public influence, which leaves the vastly larger apparatus of appointed administrators outside any structured citizen oversight (§1.1). Both deficits share a single root cause: the structural absence of an organised system of mutual accountability between citizens and power (§1.1.6).

Teisond addresses both through a single innovation: permanent public infrastructure enabling any verified citizen to express trust or distrust toward any official exercising governmental authority – continuously, privately, and with results aggregated into public indices that make collective civic judgment visible.

Legitimacy is not a status conferred once and presumed thereafter. It is a continuous relationship between those who exercise authority and those over whom it is exercised – a relationship that strengthens or erodes with every interaction, every decision, every encounter. No mechanism existed to make this relationship visible. The Platform provides one.

The Platform does not impose accountability from above. It opens an information channel between governing and governed – groups whose relationship has been structurally unidirectional. Authority flows downward continuously; the citizen's capacity to signal acceptance or rejection of that authority now flows upward through a permanent, verified, privacy-preserving mechanism. What emerges from this bilateral exchange – accountability, mutual recognition, reduced tension – is not the Platform's direct function but the social capital generated when a blocked channel is finally opened.

10.2 Why the Teisond Solution is Viable Now

Several convergent developments – technological, social, and commercial – make this viable now in a way that would have been impossible a decade ago. Identity verification has matured to the point where a reliable guarantee of one citizen, one account is achievable across the democracies the Platform serves while preserving privacy: national digital identity systems provide the strongest path where available, and authorised verification providers cover every jurisdiction where they are not, so the Platform prevents manipulation without ever depending on any single piece of national infrastructure for its operation. Cloud infrastructure has matured to the point where platforms serving millions of users across dozens of jurisdictions can scale without prohibitive capital requirements. Declining institutional trust across consolidated democracies has created genuine citizen need for instruments that restore agency rather than merely document dissatisfaction. The civic technology ecosystem has produced enough successes – and enough instructive failures – to

confirm that social innovations work when their design respects both human psychology and institutional reality. And proven market demand for political analytics demonstrates that subscription-based sustainability is achievable without grant dependence or philanthropic patronage.

Most importantly: Teisond addresses a permanent condition – citizens living under governmental authority with no routine mechanism to signal whether they accept it as legitimate. This is not a gap between elections; it is a structural absence that elections themselves do not remedy. The Platform closes it.

The Platform's viability derives not from idealistic assumptions about civic virtue but from addressing specific unmet psychological needs: restoration of dignity and agency in relations with governmental authority (§ 2.5). Officials subscribe from career self-interest; media integrate indices from editorial pragmatism; researchers access data from academic motives. Each stakeholder category interacts with the Platform from their own interests, yet their collective participation generates shared democratic infrastructure. Teisond works with human nature as it exists, transforming existing motivations into an applied information product of universal application.

10.3 Stakeholder Value Proposition

Citizens gain what no existing mechanism provides: a permanent, private, low-effort channel to render civic judgment on any official who exercises authority over their lives – from a cabinet minister to a local school principal. The psychological value is immediate: restoration of agency and dignity in encounters with governmental authority where helplessness previously prevailed.

Officials gain continuous, verified feedback that no other source provides – not the episodic soundings commissioned by media, but a permanent signal reflecting how citizens judge their exercise of authority. Whether an official subscribes from career self-interest, competitive awareness, or genuine responsiveness, the analytical layer provides insight unavailable through any other channel. The right of reply gives them a channel of official presence alongside their own index.

Media gain a permanent, structured data source that replaces ad-hoc polling commissions. Legitimacy indices provide continuous news hooks beyond episodic scandals, enable data journalism formats previously impossible at local and regional level, and offer citation-ready metrics with transparent methodology – a structural advantage in an industry under constant cost pressure.

Researchers gain a new empirical data layer for governance studies: the mandate as analytical unit, standardised metrics with transparent publication rules, and cross-country comparative possibilities across the democracies the Platform serves. Public Legitimacy Analytics as an academic subfield begins with the data the Platform provides.

Strategic partners see a Blue Ocean market positioning – Public Legitimacy Analytics as a new segment within the Public Opinion Research market – with a mission-aligned revenue model, scalable multi-tenant architecture with sublinear cost growth, and first-mover advantage in a nascent civic infrastructure category.

For democracy broadly, the Platform normalises continuous civic oversight as a complement to elections, courts, media, and civil society. It provides early detection of legitimacy crises, reduces accumulated frustration that otherwise finds expression in protest or withdrawal, and supports the long-term resilience of democratic institutions by making the consent of the governed as continuously visible as the authority of those who govern.

10.4 What the Platform Does Not Provide

Honesty about limitations earns more trust than omissions. Teisond is a specific instrument with clear boundaries.

The Platform does not guarantee governmental responsiveness. Officials can ignore low indices, accepting reputational losses. The Platform creates pressure through visibility, not legal obligation. Whether officials respond to that pressure is a political and cultural question, not a technical one.

The Platform does not prevent bad governance or corruption. It measures public acceptance of authority, not governance quality – competent officials making unpopular decisions may have low indices; charismatic but incompetent officials may maintain high ones. Distinguishing between responsive governance and populism is society's responsibility, exercised through the full ecosystem of democratic institutions.

The Platform does not solve challenges of representativeness. Published indices reflect participating citizens, not the entire population. Transparency about sample sizes, confidence intervals, and the progress of accumulation below threshold helps interpret but does not eliminate participation bias. The Platform discloses these limitations alongside every published index.

The Platform does not prevent manipulation. Coordinated campaigns by real citizens can move indices through legitimate mobilisation. The Platform makes such activity visible through anomaly flags and transparency notes rather than censoring it – respecting the distinction between organised civic action and illegitimate manipulation.

The Platform does not replace other democratic mechanisms. Elections, courts, media, and civil society retain their full functions. The Platform supplements them with continuous civic judgment data – filling a specific structural gap, not claiming to be a comprehensive solution.

Correct expectation: not revolutionary change but gradual, steady improvement in democratic accountability. The timeline is years, not months. The impact is cumulative, not instantaneous.

10.5 Long-Term Governance Vision

Teisond is designed to be built by a founder and ultimately governed by citizens. This is not an aspirational footnote – it is a structural commitment that shapes architectural decisions from the first line of code. Civic accountability infrastructure that permanently depends on a single company, a single founder, or a single jurisdiction contradicts its own premise: that power should be subject to the oversight of those it affects.

The transition from founder-operated to citizen-governed proceeds through three horizons, each building on the stability achieved by the previous one.

The first horizon is operational proof. The Platform operates, activates jurisdictions, accumulates data, demonstrates methodological integrity, and achieves financial sustainability through subscription revenue. During this phase, AGPT Ltd operates as sole decision-maker on all matters – methodology, pricing, publication rules, partner relationships, jurisdiction activation. This concentration of authority is necessary for execution speed at an early stage, but it is understood as temporary. The governance commitments made in the Neutrality Charter and the Sovereignty

and Trust Framework are the first constraints on founder authority – public, binding, and enforceable from day one.

The second horizon is participatory governance. As the Platform matures and its user base grows, governance authority over non-operational decisions progressively extends to citizens. The scope is deliberately narrow at first: publication conventions, transparency note formats, labelling standards, community guidelines – decisions that affect how the Platform communicates with users, not how it processes data or calculates indices. Citizen participation in these decisions is structured through a governance mechanism that gives verified Platform users the ability to propose, deliberate, and decide on matters within the defined scope. The technical form of this mechanism – whether implemented through distributed ledger technology, token-based governance, or a simpler deliberative structure — is determined by regulatory clarity, technical maturity, and community readiness at the time of implementation, not by a predetermined technology choice.

What does not enter citizen governance scope, at any stage: personal data handling, index calculation methodology, operational security, pricing structure, and compliance decisions. These remain under professional management – first by the founder, later by whatever institutional structure succeeds the founder – because they require technical expertise, regulatory accountability, and the ability to act swiftly in response to security incidents or legal obligations.

The third horizon is institutional independence – described in full in Section 9 (Civic Ownership Architecture). The Platform transitions from company-operated infrastructure to a protocol owned and maintained by its users: distributed data storage on citizen devices, tokenised governance rights, and a community-driven pathway from utility to security token conversion. The destination is fixed – citizen-governed civic infrastructure – and the constraints that apply throughout the journey are inviolable regardless of governance structure: aggregates-only publication, privacy by construction, and methodological neutrality as permanent architectural properties.

The founder's role in this trajectory is specific: build the Platform to the point of operational stability and institutional credibility, design the ownership architecture to accommodate progressive decentralisation, and then step back. The measure of success is not whether the founder retains control, but whether the infrastructure is resilient enough to function – and to be trusted – without any single person at its centre.

10.6 Why Centralised Multi-Tenant Architecture

The architectural choice to operate all its deployments as a single multi-tenant platform – rather than a federation of independent national platforms – is not a technical convenience. It is a governance decision with direct implications for the Platform's credibility and mission integrity.

Data sovereignty is preserved through localised hosting: each jurisdiction's citizen data is stored in infrastructure satisfying the data residency requirements that apply to it, ensuring compliance without requiring separate legal entities. Consistent methodology across all deployments is guaranteed by a single codebase – there is no possibility of national operators deviating from published methodology, because there are no national operators. Rapid scaling is enabled by config-driven deployment: activating a new jurisdiction requires a configuration file, not a development project.

AGPT Ltd as sole data controller simplifies regulatory relationships, eliminates coordination overhead between independent entities, and provides a single point of accountability. If something

goes wrong in any deployment, there is one entity responsible, one methodology to audit, and one set of standards to enforce. This clarity is an asset for regulators, researchers, and citizens alike.

10.7 Business Model Aligned with Mission

The Platform's financial sustainability derives from an obvious and psychologically natural source: officials monitoring themselves. The same people whom citizens judge want to see their own legitimacy indices, track dynamics, and compare themselves with colleagues. This creates direct correspondence between business model and mission: the very act of monitoring public legitimacy generates value officials are willing to pay for.

This fundamentally differs from extractive models where user interests conflict with commercial objectives. In Teisond's model, every participant benefits from the same data: citizens gain a voice, officials gain feedback, media gain a data source, researchers gain an empirical layer – and the Platform sustains itself from subscription revenue generated by the data citizens freely provide. No advertising, no data sales, no grant dependence, no conflict of interest between what the Platform publishes and how it earns money.

The pricing structure reinforces this alignment: fixed fees by authority level, jurisdiction-adjusted for accessibility, with zero relationship between payment and index outcome. A subscribing official and a non-subscribing official with identical citizen judgments display identical public indices.

10.8 Governance as Continuous Practice

Governance principles – independence, neutrality, transparency, privacy protection, accessibility – are operational commitments embedded in technical architecture and contractual relationships, not declarations (see Section 6).

Privacy by construction ensures individual judgments remain private through technical impossibility of profiling, not merely policy prohibition. The Platform inevitably faces pressure to sacrifice independence for finances, tweak methodology for political advantage, or weaken privacy for analytical convenience. Principles provide guidelines; sustaining them requires judgment, resilience, and institutional culture.

The Platform applies to itself the same visibility discipline it applies to officials: methodology changes are documented with public changelogs, financial summaries are published annually, third-party audits will be conducted as the Platform scales, with results disclosed publicly (see § 7.7). An organisation that demands accountability from others must practise it internally.

10.9 Realistic Expectations

Creating civic infrastructure requires patience. The Platform activates jurisdictions progressively, as their national databases and verification channels reach readiness (§7.2). The stages that follow are qualitative rather than calendrical: operational maturity, in which every activated national platform runs stably and approaches financial self-sufficiency; institutional recognition, in which continuous monitoring of legitimacy is acknowledged as an accountability mechanism in its own right, alongside elections, courts, media, and civil society; and ubiquity, in which coverage extends across the greater part of the world's consolidated democracies and the Platform functions as ordinary democratic infrastructure. Beyond that lies the generational effect: officials who have known continuous monitoring of legitimacy for the whole of their careers govern differently from the generation that knew only episodic accountability.

The automation-first operational model and sublinear cost scaling mean that financial sustainability is achievable at modest rates of adoption. The Platform does not require mass adoption to survive its early years.

10.10 Acknowledged Risks

Citizen participation may initially be insufficient for meaningful indices, positioning the Platform as an interesting experiment rather than an authoritative source. Official subscription rates may differ from projections, requiring revised commercial terms. Manipulation attempts may episodically distort indices, undermining trust and requiring enhanced safeguards. Political opposition may complicate activation in certain jurisdictions, restraining network potential. Privacy breaches – however unlikely given architectural protections – could seriously undermine user trust, requiring transparent response. Alternative initiatives with better funding may fill the niche before Teisond establishes itself. Mission drift under financial or political pressure remains a constant temptation.

These risks are inherent in any attempt to create new civic-tech infrastructure. They cannot be eliminated – only managed through careful design, honest disclosure, continuous adaptation, and mission discipline. The correct attitude is not confidence that risks will not materialise, but preparedness for when they do.

10.11 Call to Action

For Strategic Partners: This is civic infrastructure at the formation stage – a platform designed for the consolidated democracies it addresses, with a clear revenue model, mission-aligned business logic, and a Blue Ocean positioning in Public Legitimacy Analytics. Read Sections 4 and 5 to assess how the model works and what it commits to.

For Officials: This is not a threat – it is a career management tool. Legitimacy indices give you what no other instrument provides: continuous, verified feedback from the citizens you serve. Early subscribers gain insight before public indices become widely cited. Read § 2.3 and Appendix C to understand how the Platform works and what protections you have.

For Media: Go beyond the "ratings and scandals" paradigm. Replace assumptions with verified data. Tell political stories through the language of legitimacy. Make NOLI and mandate-level scorecards front-page metrics – a new system for public analytics.

For Researchers and Academia: Enter a new discipline at its formation stage. Make Public Legitimacy Analytics a living laboratory where theories of accountability and trust are tested on data. Set the academic standard for methodology in this field.

For NGOs and Civil Society: Engage as partner, user, and advocate. Support sustainable infrastructure of civic judgment – instead of investing in episodic bursts of media, petition, or street emotions. In the digital age, this is more effective, more reliable, and safer for participants.

For the Sceptical: Read on. This document is designed to withstand scrutiny, not to avoid it.

10.12 Final Reflections: Democracy as Continuous Practice

Elections are primary democratic infrastructure. Courts protecting rights, free media investigating abuses, civil society conducting change – all basic infrastructure. The civic institution of governmental legitimacy monitoring aspires to join this list, supplementing existing elements with a component that closes accountability deficits they do not cover.

The vision: a society in which citizens can declare their attitude toward any official whose authority is exercised on their behalf; where judgments of the governed aggregate into public indices which the governing ignore at their peril; where accountability operates continuously; where the question "does this official retain citizens' trust?" receives a clear, verified answer rather than remaining speculation until the next elections.

The accountability deficit exists in all democracies. The question is whether societies will accept it as an inevitable feature or begin building infrastructure for its elimination. Teisond is less a single product than a missing layer of democratic infrastructure: a mechanism for making continuous consent of the governed as visible in the twenty-first century as elections made consent visible in the nineteenth.

This White Paper transitions from documentation to implementation. The concept is articulated. The methodology is specified. The architecture is designed. The legal structure is established. The governance framework is committed. What remains is execution – and the participation of citizens, officials, media, researchers, and partners who share the conviction that democratic accountability should not be confined to election day.

APPENDIX A: THEORETICAL AND PHILOSOPHICAL FOUNDATIONS

A.1 Introduction: Why Theory Matters

This Appendix lays out the theoretical footing of Teisond: what legitimacy means as a measurable construct, why its continuous measurement is both possible and necessary, and how these ideas shape product design, governance choices, and publication rules.

Theory is not ornament. Without clear concepts, "legitimacy" collapses into popularity or partisanship. Theory prevents that collapse by distinguishing legitimacy from approval or single-issue satisfaction, clarifying who is judged (officials exercising governmental authority), and specifying what can be measured (citizen judgments) and how results should appear (aggregated indices with thresholds and confidence intervals).

The Platform's architecture follows from these first principles. Aggregates-only publication protects persons while revealing patterns – no individual records exposed, indices published only above minimum sample thresholds, every published value accompanied by a confidence interval (§5.4). Universality of scope means any office wielding governmental authority belongs in scope, not just high-profile positions. Continuity in time means measurement is ongoing – recomputed at a cadence configured per jurisdiction – because legitimacy drifts between elections and, for appointed officials, no electoral test exists at all. Neutrality by construction means guardrails prohibit political profiling, micro-segmentation below thresholds, and outputs enabling targeted manipulation.

Classical accounts of legitimacy centre on systems and offices, but citizens interact with officials. A citizen's willingness to accept decisions depends on judgments about a specific official's trustworthiness, fairness, and competence. Measuring this personal legitimacy safely and in aggregate connects lived experience with democratic theory.

Clear concepts also discipline governance choices. When anomalies appear – bursts, coordination signals – the Platform discloses flags rather than silently erasing data, because public reason produces better outcomes than hidden curation. If legitimacy belongs to citizens, they should eventually help steward the standards by which it is measured – but only for non-operational governance matters, never for access to personal data (§6.6.1). And because norms travel but laws vary, GDPR serves as the baseline localised upward, with roles and responsibilities mapped explicitly (§6.2).

The appendix proceeds as follows: §A.2 establishes the conceptual framework for legitimacy (Weber, Easton, personal legitimacy as continuous variable); §A.3 identifies two fundamental lacunae in electoral legitimacy (distortion and remission); §A.4 reconceptualises social control as horizontal civic power; §A.5 examines the crisis of civic cohesion; §A.6 synthesises how Teisond addresses these theoretical gaps; §A.7 outlines the civic ownership philosophy behind potential DAO and tokenisation; and §A.8 concludes with how theory informs practice. Throughout, the operative principle is that theory is the contract the Platform makes with readers about what its numbers mean – and what they will never be used to do.

A.2 Legitimacy: Conceptual Framework

Legitimacy, as this White Paper uses the term, is the publicly recognised right to rule – the belief that an official's exercise of authority is appropriate, justified, and should be complied with. It is not a synonym for popularity or policy agreement; it concerns citizens' acceptance of authority over time.

This definition draws on a long tradition in political theory. The sections below trace three foundational contributions – Weber's typology, Easton's distinction between system and authority support, and the treatment of personal legitimacy as a continuous variable – and show how each informs Teisond's design decisions.

A.2.1 Max Weber's Typology

Weber identified three classic sources of legitimacy:

- Traditional legitimacy – acceptance grounded in custom, continuity, and inherited roles.
- Charismatic legitimacy – devotion to a leader's perceived extraordinary qualities; intense but fragile and episodic.
- Legal-rational legitimacy – obedience to impersonal rules and offices; authority attaches to the office, not the person.

Teisond operates within a legal-rational order: the Platform measures citizens' recognition of the authority of officials, not the constitutional validity of the system itself. Results are presented at the level of the mandate – personal to the officeholder, yet framed by the office – published only in aggregated form and with statistical guardrails.

A.2.2 David Easton's Three Types of Legitimacy

For democratic systems, it is useful to distinguish:

- Ideological (principled) legitimacy – belief in the regime's core values and purposes.
- Structural (procedural/institutional) legitimacy – confidence in the "rules of the game" (elections, courts, administration).
- Personal (authorities) legitimacy – acceptance of particular officials based on perceived trustworthiness, fairness, and competence.

Teisond's primary object is personal legitimacy of officials (authorities). The Platform remains neutral on ideological disputes and partisan outcomes. This separation keeps measurement focused and prevents category errors: a citizen who distrusts a specific mayor is not necessarily expressing dissatisfaction with democracy itself. Easton's framework makes this distinction analytically precise.

A.2.3 Personal Legitimacy as a Continuous Variable

Elections are episodic; legitimacy drifts between them – and for appointed officials, no electoral test exists at all. Teisond treats personal legitimacy as a state that is acquired, maintained, and lost, strengthening or eroding in response to conduct, decisions, and events.

The Platform measures this through a deliberately simple mechanism. Verified citizens provide binary signals – personal trust or distrust toward a specific official. These signals are governed by one citizen, one account and aggregated per mandate into a scaled index (0–100) with confidence intervals, computed as a snapshot of all standing judgments at each scheduled calculation. Publication thresholds protect privacy and quality through minimum sample sizes and rounding. Below threshold, the profile displays the progress of accumulation rather than a number.

The resulting index represents the current public acceptance of authority for a specific official. It does not represent general job performance, policy wisdom, or legal validity, and it is not a profiling tool or a vehicle for micro-targeting. Guardrails enforce this distinction by design: aggregates-only publication with no individual-level exposure, no per-user histories, and no demographic correlations of opinions; anomaly detection with transparency, where suspected bursts or coordination are flagged rather than silently suppressed; and neutral APIs that serve only aggregated outputs, rejecting micro-segments below thresholds.

A continuous measure of personal legitimacy at the level of the mandate, presented with statistical and privacy guardrails, gives democratic systems an instrument for visible, non-violent accountability that operates continuously across every level of governmental authority – without crossing into profiling or partisanship.

A.3 Electoral Legitimacy: Two Fundamental Lacunae

Elections are essential but episodic. Between elections, two gaps undermine the informational quality of democratic control: distortion of political preferences at the ballot box and remission of accountability afterward. These are not failures of democratic design but structural limitations inherent in episodic mechanisms. Teisond addresses both by providing a continuous, privacy-preserving signal of personal legitimacy of officials.

A.3.1 Distortion of Political Preferences

Ballots bundle issues, identities, and future contingencies into a single episodic choice. This produces structural distortions. Voters must accept a package – party, coalition, persona – in which specific judgments about particular officials get lost. Strategic voting skews sincere preferences through fear of "wasting" a vote, spoiler dynamics, and tactical considerations. Campaigns compress information into short windows, so that performance signals appearing after election day cannot be expressed until the next cycle. And media salience and polarisation effects can overwhelm fine-grained judgments of trustworthiness and fairness for individual officials.

The consequence is that the electoral result is a coarse, bundled proxy for legitimacy. It tells the public who holds office, not how citizens currently accept or contest the authority of each official. Teisond separates the signal: verified citizens can continuously express trust or distrust toward specific officials, with results aggregated at the level of the mandate and the calculation period (0–100 index with confidence intervals) and published only above privacy and quality thresholds.

A.3.2 Remission of Accountability

After inauguration, accountability tends to remit – it thins out and becomes indirect. Formal checks such as audits, committees, and courts are slow and often opaque to citizens. Officials control the visibility, timing, and framing of decisions between elections. And protests, petitions, or investigative journalism, while important, are episodic and costly – they do not yield a routine, quantitative signal.

The result is that authority can drift away from public acceptance long before the next election – and for appointed officials, no election ever arrives to correct the drift. No shared metric makes this erosion visible. Teisond restores a low-friction, non-violent accountability channel: a continuous, privacy-preserving legitimacy index for each mandate, recomputed at each scheduled calculation and capable of strengthening or eroding over time, with anomaly flags and public transparency notes rather than silent suppression.

A.3.3 Why This Matters for Democratic Theory

Continuous legitimacy measurement matters for democratic theory on several levels. It re-centres citizens: legitimacy is a relationship between citizens and officials, and a continuous measure at the level of the mandate makes that relationship visible without exposing individuals. It bridges representation and responsibility: elections authorise, but ongoing acceptance sustains that authorisation, and visibility of the drift disciplines conduct. It improves learning and trust: early signals enable course corrections by officials and more informed public discourse, reducing the cost of errors and polarisation. And it sets principled guardrails: because a published index is aggregated public information rather than individual personal data, the Platform enforces aggregates-only outputs, minimum sample thresholds, rounding, and no profiling or micro-segmentation below thresholds.

Electoral signals decide who governs; they do not continuously indicate how that authority is being accepted – and for appointed officials, they indicate nothing at all. Teisond supplies the missing instrument: a privacy-safe, statistically disciplined measure of personal legitimacy that operates continuously across every level of governmental authority.

A.4 Social Control Reconceptualised

"Social control" is often heard as coercion or censorship. This appendix reclaims the term in its original civic meaning: the horizontal capacity of citizens to make public power responsive through non-violent visibility and shared standards – without surveillance, profiling, or manipulation. The term has accumulated negative connotations (§A.4.1), but its original meaning (§A.4.2) describes precisely what Teisond provides: a structured, non-coercive mechanism through which citizens collectively influence the informational environment in which authority operates.

A.4.1 Negative Connotations and Historical Baggage

The term "social control" carries baggage that must be acknowledged before it can be reclaimed. It is not coercion – not police power, moral policing, or content takedowns; the Platform exercises no authority over officials but provides information, and what officials do with that information is their decision. It is not stigma or shaming – Teisond never publishes individual citizen data, and official

indices are statistical aggregates, not personal verdicts. And it is not partisan mobilisation – outputs are neutral aggregates produced by uniform methodology applied to all officials regardless of affiliation.

A.4.2 Original Meaning: Horizontal Civic Power

In its original sociological sense, social control refers to the mechanisms through which communities maintain coherence and hold power accountable – not from above (coercion) but from alongside (horizontal feedback). Teisond operationalises this meaning.

Citizens continuously signal acceptance or withdrawal of acceptance – trust or distrust – toward specific officials. The signal is private at the individual level and public only in aggregate. Making these signals visible disciplines officials through reputational incentives rather than force: an official whose legitimacy index declines faces questions from peers, media, and constituents without any formal sanction being imposed. And shared, published rules – thresholds, confidence intervals, anomaly flags – turn diffuse sentiment into legible, auditable public information. This is the difference between "people are unhappy" (vague) and "this official's legitimacy index declined from 64 to 51 across successive calculations, with a stated confidence interval" (precise, verifiable, actionable).

A.4.3 The Democratic Paradox

Democracies promise rule by the people yet often lack routine, low-friction instruments for the people to exercise continuously. This paradox is structural, not incidental. Institutional checks – courts, audit bodies, ombudsmen – exist but are slow, specialised, and often opaque to citizens; they serve institutional accountability, not citizen-facing accountability. Street politics – protests, petitions – matter but are episodic, high-cost, and available only to the motivated and organised; the ordinary citizen with a grievance about a local official has no practical channel. The result is that citizens' day-to-day leverage is weak, and authority can drift from acceptance with no shared metric making the drift visible.

Teisond resolves the paradox by providing a continuous, privacy-preserving channel where citizens shape the informational environment of governance without targeting individuals. It is not the only solution to the paradox – but it is the specific instrument missing from the current democratic toolkit.

A.4.4 Teisond as Social Control Infrastructure

The Platform operationalises social control as horizontal civic infrastructure through several interlocking design properties. The object of measurement is the person holding a specific mandate; the office is an attribute of identification, and the publication unit is the mandate together with the calculation period, with signals aggregated into a 0–100 legitimacy index accompanied by confidence intervals. Privacy is enforced by construction: aggregates-only publication, minimum sample thresholds, rounding, no per-user histories, no demographic breakdowns, and no micro-segments below thresholds. Integrity operates through disclosure rather than suppression – anti-manipulation systems detect bursts and coordination, and when they do, users see public flags and transparency notes rather than silently altered data. APIs serve aggregated outputs only.

The civic outcomes follow from this design. Officials gain timely, non-defensive feedback. Citizens and watchdogs gain a shared reference point. Media gain a standard, auditable metric that reduces

rumour and spin. Reclaimed as horizontal civic power, social control means visibility rather than force – and the Platform makes that visibility safe, neutral, and statistically disciplined, so that authority remains answerable to the public continuously, across every level of governmental authority.

A.5 Crisis of Civic Cohesion

Democratic systems increasingly lack a shared informational spine: citizens inhabit fragmented media spaces; trust erodes; and routine, low-friction accountability between elections is weak. This fragmentation is not merely a media problem – it is a structural challenge to the democratic premise that citizens share a common factual basis for holding authority accountable. Teisond responds by creating a neutral, privacy-preserving signal of the personal legitimacy of officials that different publics can rely on without exposure or profiling.

A.5.1 Systemic Fragmentation

The informational environment in which democratic accountability operates has fractured along several dimensions. Social feeds and niche media produce non-overlapping realities – the same event appears as different "facts" depending on which information ecosystem a citizen inhabits. Speed and virality outrun careful reasoning, so that rumour and spin dominate the time window in which opinions form; by the time corrections arrive, the narrative is set. And coarse partisan frames crowd out office-level judgments of trustworthiness and fairness – citizens are asked to pick sides, not to judge officials.

The result is that public debate lacks a common, auditable reference for how citizens are currently accepting or withdrawing acceptance of specific officials. Everyone has opinions; no one has shared, verified data.

A.5.2 Decline of Horizontal Power

While institutional checks on authority have grown more sophisticated over time, citizens' direct horizontal leverage has arguably weakened. Day-to-day tools are episodic – protests, petitions, exposés – and high-cost, requiring organisation, publicity, and sustained effort that most citizens cannot sustain. Formal checks are slow, specialised, and often invisible to the public: a citizen who knows that an ombudsman investigated a complaint gains nothing if the outcome is sealed. And without shared, periodic measures of public acceptance, officials' reputations are shaped by media narratives and partisan framing rather than by structured citizen input – authority can drift away from acceptance with no mechanism making the drift visible.

The result is that civic cohesion frays as frustration accumulates without a legitimate, non-violent outlet. Citizens feel powerless; officials feel unaccountable; the distance between them widens.

A.5.3 Why Teisond Matters in This Context

In this fragmented landscape, the Platform matters because it provides a common reference point. A neutral index of legitimacy for each mandate (0–100 with confidence intervals) anchors discourse across media, watchdogs, and civil society – different publics can read the same number the same way. Continuity replaces episodic shocks: recalculation at the cadence configured for each jurisdiction produces a series of snapshots, and from it visible trajectories rather than isolated data points.

Safety is embedded by design: aggregates-only outputs, minimum sample thresholds, rounding, no per-user histories or demographic correlations, and no micro-segments below thresholds. When suspected manipulation is detected, the Platform responds with public flags and plain-language notes rather than silent takedowns. And incentive alignment ensures that visibility rewards responsiveness and corrective action by officials, while citizens gain a low-friction channel to register acceptance or withdrawal of acceptance without exposure.

Cohesion requires shared, trusted signals. The Platform supplies one for the acceptance of authority: a privacy-preserving, statistically disciplined, office-level measure that different publics can read the same way – reducing rumour, lowering temperature, and restoring continuous accountability.

A.6 Synthesis: How Teisond Addresses Theoretical Gaps

The preceding sections identified three theoretical gaps: electoral distortion (§ A.3.1), accountability remission (§ A.3.2), and the erosion of horizontal civic power (§ A.4–A.5). Teisond supplies the missing, privacy-preserving instrument for continuous accountability of officials. It resolves the two electoral gaps and operationalises social control as horizontal civic visibility, not coercion. This section synthesises how the Platform's design maps to each gap.

A.6.1 Continuous Measurement of Personal Legitimacy

The core mechanism is simple in concept and disciplined in execution. Verified citizens express trust or distrust toward specific officials. These signals are aggregated per mandate into a 0–100 index with confidence intervals, computed as a snapshot of all standing judgments at each scheduled calculation. Indices appear only above minimum sample thresholds; below threshold, the progress of accumulation is shown instead. Rounding protects anonymity near thresholds, and anomaly flags ensure disclosure over suppression.

The outcome is the first continuous, verified measure of public acceptance of authority at the level of the mandate available in democratic practice – a timely, comparable legitimacy signal that operates across every level of governmental authority, not only between elections but for officials who never face them.

A.6.2 Closing the Remission Gap

Citizens do not wait years to express acceptance or withdrawal of acceptance – the Platform provides low-friction feedback that operates continuously. Officials see movement from one calculation to the next and can address causes early, enabling course correction rather than

discovering erosion only at the next election – or, for appointed officials, never discovering it at all. And a shared, auditable metric reduces rumour, selective framing, and spin by grounding public discourse in verifiable data.

Schedler's view of accountability rests on two pillars: answerability (public reason-giving) and enforcement (consequences for abuse). Without a continuous public signal, accountability thins out between electoral cycles – and for the vast majority of officials who never face elections, it never thickens at all. The Platform supplies the missing informational layer – neutral indices at the level of the mandate, read by citizens, civil society, media, and oversight bodies – while leaving enforcement to existing legal and institutional channels.

A.6.3 Enabling Horizontal Social Control (Non-Violent, Neutral)

The Platform enables horizontal social control by maintaining a clear separation between measurement and publication. The person holding the mandate is the object of measurement; results are published at the level of the mandate and the calculation period, with no personal records exposed. Privacy is enforced by construction: aggregates-only outputs, no per-user histories, no demographic correlations, and no micro-segments below thresholds. When manipulation is suspected, the Platform flags anomalies and publishes plain-language notes rather than silently erasing signals. APIs expose only aggregated endpoints; disallowed breakdowns are rejected.

Legitimacy is a scarce coordination resource: communities allocate power and attention to actors and rules they perceive as legitimate. To sustain that legitimacy, the Platform prioritises process over ad-hoc fixes – clear publication rules, aggregates-only outputs, transparency notes, and the right of reply. Participation is encouraged without profiling; any future governance evolution remains standard-focused and excludes personal data.

A.6.4 Addressing Democratic Fragmentation

The Platform addresses democratic fragmentation by providing a common reference point: a neutral, statistics-first index that anchors debate across media, watchdogs, and civil society. Participation is distributed and continuous – many citizens contributing judgments toward individual offices, not siloed by platform tribes. And incentive alignment ensures that visibility rewards responsiveness and penalises neglect without targeting individuals.

These properties rest on design commitments documented elsewhere in this White Paper: data governance including thresholds, anonymity, and publication policy (§5.4); controller and processor mapping with explicit guardrails (§6.2); and a governance pathway ensuring that any future citizen co-governance remains standard-focused and excludes personal data (§6.6.1).

The boundaries are equally important. The Platform measures public acceptance of authority for each mandate over time, safely and comparably. It does not profile individuals, enable targeted mobilisation, adjudicate legal validity, or replace elections or courts. By turning citizens' trust and distrust into a continuous, privacy-safe signal at the level of the mandate, the Platform restores continuous accountability without force or exposure – filling the structural absence that elections alone cannot address and that, for appointed officials, no existing mechanism addresses at all.

A.7 DAO and Tokenisation: Civic Ownership Philosophy

Purpose. This section articulates the theoretical foundation for civic ownership of legitimacy monitoring infrastructure. The question it addresses is: if legitimacy monitoring infrastructure serves the public, should the public have a role in governing and owning it? The answer is yes – within carefully scoped guardrails that protect privacy, neutrality, and methodological integrity. Section 9 translates these theoretical commitments into a concrete civic ownership architecture, describing the mechanisms through which the Platform transitions from founder-operated infrastructure to a protocol owned and maintained by its users.

A.7.1 From Representation to Participation to Ownership

Democratic accountability evolves through three stages, each building on the previous. Representation through elections authorises officeholders but leaves long intervals with weak citizen leverage – and for appointed officials, provides no leverage at all. This is the starting point: necessary but insufficient. Participation through the Platform restores a continuous, privacy-preserving legitimacy signal about specific officeholders, giving citizens a voice that operates permanently rather than episodically. Ownership goes one step further: citizens and public-interest actors help steward the standards by which the Platform presents its work – labelling conventions, the form of contextual information, the cadence of transparency reporting – within strict guardrails that exclude personal data handling, index calculation methodology, and publication thresholds. Ownership here means stewardship of public rules and artefacts, not equity or revenue. It is the principle that infrastructure serving citizens should ultimately be governed by citizens.

A.7.2 Civic Data as Commons (Without Exposing Persons)

Teisond produces a specific kind of public good: aggregated indices, confidence intervals, notices of accumulation progress, and transparency notes. These outputs are the commons – shared, reusable, and valuable to media, researchers, civil society, and citizens alike.

The commons excludes personal data categorically. There are no individual records in public or subscriber outputs; no per-user histories; no demographic correlations; no micro-segments below thresholds. Publication discipline – minimum sample sizes, rounding, and anomaly flags – ensures that the commons serves the public interest without compromising any individual (see § 5.4).

This distinction is crucial: the Platform produces public goods from private inputs, and the architecture guarantees that the transformation is irreversible. There is no path from published aggregates back to individual judgments.

A.7.3 Tokenisation as Alignment Mechanism (Governance-Utility Only)

The governance-utility token (U-token) is conceived as an alignment mechanism, not a financial instrument. It functions as a key for scoped participation – enabling verified users to propose, discuss, and decide on non-personal-data matters such as transparency note cadence and non-material parameter bounds, all within the guardrails defined in §5.4. The U-token is not a security, not a subscription, and not equity: it carries no dividends, no promise of returns, no access to personal data, and does not substitute for paid subscriptions.

Rollout is compliance-first. No public token sale is planned at this stage; pilots may use non-transferable allocations in compliant jurisdictions, and decisions or hashes can be anchored on-chain while execution remains off-chain (§6.6.1). Anti-capture safeguards include quorums, proposal cooldowns, rate-limits, optional delegation with transparent records, and key revocation for abuse.

A.7.4 Decentralised Governance and Democratic Values

Decentralised governance, if and when it emerges, must align with the Platform's democratic values. Neutrality means governance concerns method and transparency, not political outcomes or profiling. Subsidiarity means national participation comes first, with any network-level layer remaining advisory for shared standards such as taxonomies and open components. Auditability means material decisions carry human-readable changelogs, and where on-chain hashes are used, they provide public audit trails. And accountability symmetry means the same visibility discipline the Platform applies to officials applies to itself – rules change only with notice, reasons, and records.

Civic ownership for Teisond means stewardship of shared standards and public artefacts, enforced by privacy and neutrality guardrails. A governance-utility token and carefully scoped participatory processes can align incentives and widen participation – without exposing individuals, promising financial returns, or departing from the aggregates-only design (§§5.4 and 6.6.1).

A.8 Conclusion: Theory Informs Practice

Democracies need a continuous, privacy-preserving way to see whether citizens accept the authority of specific office-holders – not only between elections, but permanently, including for the vast majority of officials who never face elections at all. Teisond provides that instrument without profiling, force, or partisanship.

The mechanism is straightforward. Verified citizens register trust or distrust toward named officeholders. Signals are aggregated per mandate into a 0–100 legitimacy index, computed as a snapshot at each scheduled calculation and published only when the threshold for the level of authority is met; below it, readers see the progress of accumulation.

This matters for three reasons. It resolves two structural deficits in electoral accountability: distortion at the ballot box (bundling, strategy, timing) and remission of accountability afterward – while extending coverage to officials who fall outside the electoral mechanism entirely. It reclaims social control as horizontal civic visibility: reputational discipline through transparent, aggregated information rather than force. And it gives citizens, civil society, watchdogs, journalists, and public institutions a shared reference point that lowers rumour and spin.

Guardrails are embedded by design. Publication is aggregates-only: no individual records, no per-user histories, no demographic correlations, no micro-segments below thresholds. Rounding protects anonymity near boundaries, and suspected coordination is flagged with public notes rather than silently suppressed. APIs expose only aggregated endpoints; disallowed breakdowns are rejected. Data governance and responsibilities are mapped explicitly (§§5.4 and 6.2), and any future citizen co-governance remains standard-focused and excludes personal data (§6.6.1).

The index should be read for what it is: a statistically disciplined signal of current public acceptance of authority for the person holding a mandate. It is not a prediction of elections, a verdict on policy wisdom, or a legal ruling – and it should be read together with its publication notes, and, at the

analytical level, with the confidence interval that accompanies it. This White Paper covers legitimacy of authority only; extensions to additional civic signals remain out of scope until they can meet the same privacy, neutrality, and statistical standards.

Theory in this appendix is not ornament. It is the contract behind the product. On that basis, Teisond turns civic judgment into a safe, neutral, and continuous public signal – so that authority remains answerable to the governed at every level and at all times.

APPENDIX B: GLOSSARY OF TERMS

Terms used throughout the White Paper. Where helpful, entries cross-reference §§5.4 (Data Governance and Compliance), 6.2 (Roles and Jurisdictions Passport), and 6.6.1 (Potential DAO Integration).

Aggregates-only – a design principle: the Platform publishes only aggregated statistics (never individual records), with privacy and quality guardrails (thresholds, rounding). See §5.4.

Alert (threshold crossing / significant move) – a notification that an index crossed a configured threshold or moved by a material amount over a period. Alerts are aggregated events; no personal data.

Anomaly flag – a public marker shown when volumetric/behavioral anomalies are detected (e.g., bursts, suspected coordination). Favors disclosure over suppression.

API (Aggregated-only API) – public/subscriber endpoints that return only aggregated outputs (indices, benchmarks, alerts). Disallows micro-segments below thresholds; rate-limited and auditable. See § 5.4.10.

Below-threshold / Sub-threshold – a state in which the number of standing judgments on a mandate is below the minimum required for publication. No ratio is shown; the profile displays the progress of accumulation instead.

Benchmark – an aggregated comparison across a set of mandates or regions at a given calculation date (for example, top-N lists). Mandates below their publication threshold are excluded.

Citizen verification (privacy-preserving) – mechanisms enforcing one citizen, one account without retaining the identity data used to establish it. Implementation specifics are omitted to prevent gaming; the White Paper specifies guarantees and architectural properties.

Confidence interval (CI) – an uncertainty band around the index (e.g., 95% CI) reflecting sample size and variance. Every published index includes a CI.

Controller / Processor / Sub-processor – GDPR roles: AGPT Ltd is Controller for national platform data; cloud infrastructure providers are Sub-processors under appropriate data processing agreements. See § 6.2.3.

Crowdsourced Measurement Platform – the type of platform Teisond is: a data platform that does not connect its users, affords the parties to the exchange no means of acting upon one another directly, and does not mediate between them, but receives judgments from one category of user and produces structured information of professional value to others. See §4.

Data Access – the subscription product extending the analytical level to all serving officials of a jurisdiction, rather than to a single mandate. Purchased by media, research institutions, consultancies and the analytical divisions of institutions and corporations. See §4.3.

Data governance – the set of policies and technical measures enforcing privacy, quality, and lawful processing: aggregates-only publication, thresholds, access controls, logs minimisation, and retention rules. See § 5.4.

DPA (Data Processing Agreement) – contractual terms governing Processor obligations, TOMs, breach notices, deletion/return, and audits.

Judgment – a single signal of trust or distrust rendered by a verified citizen in respect of a specific mandate. A judgment is perpetual: it stands until changed or withdrawn by the citizen, or until the mandate closes. It is bound to no period and does not age. Judgments are aggregated; no per-user histories are stored.

AGPT Ltd – Advanced Global Polling Technology Ltd (UK). The company operating all national Teisond deployments. Acts as data Controller for each national platform. Responsible for legal compliance, platform operations, and publication policy enforcement across all jurisdictions. See § 6.2.1.

Governance-utility token (U-token) – a non-financial access key for scoped participation in standards/transparency processes (create/propose/decide within guardrails). Not equity, not a subscription, not a promise of returns. See § 6.6.1 and A.8.

Index (Legitimacy Index) – a 0–100 measure of the current public acceptance of authority for a specific mandate, computed as a snapshot of all standing judgments at the moment of calculation. The index is published at the public level once its threshold is met; the confidence interval accompanying it belongs to the analytical level.

k-anonymity guardrails – practical safeguards to ensure that published aggregates cannot be used to infer information about small groups or individuals (via thresholds and rounding).

Managed Hosting – the operational model in which AGPT Ltd directly operates all hosting infrastructure for every national deployment through a centralised multi-tenant architecture. AGPT Ltd acts as data Controller. See §§ 5.4 and 6.2.

Mandate (publication unit) – the unit at which Teisond publishes results: a person holding a specific office carrying governmental authority, together with the calculation period. Where one individual holds distinct positions each carrying separate authority, each is a separate mandate with an index of its own. When a mandate closes, its judgments cease to stand and the counters of the successor mandate start from zero.

Micro-segmentation (disallowed) – any breakdown or query that would fall below publication thresholds or enable re-identification. Rejected by the API and UI.

n (sample size) – the count of standing judgments on a mandate at the moment of calculation. Publication requires meeting the minimum threshold for the level of authority concerned, set per jurisdiction. See §5.4.

National DAO (future, scoped) – a token-gated process for non-PII governance matters (labels, transparency cadence, non-material parameter bounds). Advisory and compliance-bounded. See § 6.6.1.

Network DAO (future, advisory) – a cross-country standards layer (taxonomies, transparency formats, open components). No PII; advisory unless ratified contractually. See § 6.6.1.

NOLI (National Officials' Legitimacy Index) – the aggregate index of legitimacy for the officials of a jurisdiction, computed from the underlying mandate-level snapshots under a single methodology. The broadest of the Platform's analytical products. See §1.6.1.

OPLS (Official Public Legitimacy Scorecards) – detailed scorecards for individual officials: the current index for a mandate together with its analytical derivatives, including absolute counters, metrics of consensus, historical series, and comparisons with peers at the same level of authority. Available at the analytical level. See §1.6.1, §4.1.

Official – the person currently exercising governmental authority under a specific mandate; the object of measurement for the index of legitimacy. The office is an attribute of identification, not the object measured. No individual citizen record is exposed.

One citizen, one account – a property of verification ensuring that each natural person may hold at most one account, enforced without retaining the identity data used to establish it.

Period (calculation period) – the interval between scheduled calculations, configured per jurisdiction. The period is a dimension of the publication of an index, never a property of a judgment.

Privacy by construction – an architectural stance under which the categories of data capable of exposing an individual have no containers in the schema, so that data which could be handed over do not exist; privacy is not an add-on.

Progress of accumulation – the display shown for a mandate below its publication threshold: the number of standing judgments recorded and the threshold to be reached, without a ratio. Below a further minimum of counter visibility, only a neutral state of collection in progress is shown.

Public Legitimacy Analytics (PLA) – the category of data the Platform produces: continuous, quantified, verified measurement of the public legitimacy of officials across the vertical of governance. See §1.6.1.

Publication thresholds – the minimum number of standing judgments required before an index is shown publicly, differentiated by level of authority and configured per jurisdiction; includes rounding.

Public (free) vs Subscriber (paid) – public outputs: headline aggregated indices, confidence intervals, progress of accumulation below threshold, transparency notes. Subscriber outputs: aggregated benchmarks, historical series, alert feeds, and aggregated API access. No row-level data in either.

Right of reply – the channel through which an official may publish an official statement alongside their own index, in the same plane of public visibility. The Platform provides the channel and neither moderates its contents nor expects it to be used. See §6.3.4.

Rounding – publishing indices at one decimal place (or coarser, if configured) to reduce re-identification risk and false precision.

Roles & Jurisdictions Passport – a living artifact per country that maps roles (controller/processor/sub-processor), lawful bases, local constraints, and escalation trees. See §6.2.

SLA (Service Level Agreement) – availability, latency, incident response targets, and remedies for platform operations. Defined internally by AGPT Ltd as part of operational standards.

Snapshot – the computed state of all standing judgments on a mandate at a single moment of calculation. The published index is a snapshot; a sequence of snapshots forms the historical series from which trends are read. Trailing horizons are computed from the series, never from judgments directly.

Standing judgment – a judgment currently in force: rendered, not withdrawn, not superseded by a change, on a mandate that remains open. Indices are computed from standing judgments alone.

Sub-processor – a processor engaged by the Processor to carry out specific processing activities (e.g., cloud/infra), bound by sub-DPA terms and no secondary use.

Subscriber – a paying organisation (e.g., media, NGO, research, administrations) with access to aggregated dashboards, alerts, and API, within guardrails.

Transparency note – a plain-language public explanation accompanying material changes, anomalies, or method updates; part of the "disclosure over suppression" norm.

Trust / Distrust (input semantics) – the only signals citizens give about officials. These are personal judgments of acceptance or withdrawal of acceptance of authority, aggregated at the level of the mandate.

APPENDIX C: FREQUENTLY ASKED QUESTIONS

Practical answers for citizens, officials, media, researchers, and regulators. See also Appendix B (Glossary), Section 2 (Concept and Methodology), Section 5 (Legal Structure), and Section 6 (Governance and Ethics).

C.1 General

Q1. What does Teisond actually measure?

A. Verified citizens render trust or distrust in respect of specific officials. These civic judgments are aggregated and published as a 0–100 legitimacy index for each mandate, meaning the person holding an office together with the calculation period, for example "Mayor of Riverton, 12 Sep 2025".

Q2. Is this a popularity poll or a rating?

A. No. The index reflects public acceptance of authority (legitimacy), not job performance, policy approval, or personal likability. It is a structured civic judgment, not an opinion survey.

Q3. Do you predict election results?

A. No. The index is not a polling average or a model of electoral intention. It records the current acceptance of authority, and nothing in it forecasts how anyone will vote.

Q4. Who benefits from this signal?

A. Citizens gain a continuous channel for accountability. Officials gain timely feedback on public acceptance. Media, civil society, watchdogs, and researchers gain a shared, auditable reference point that operates continuously.

Q5. Who operates Teisond? Is it independent?

A. Teisond is operated by AGPT Ltd, a UK-registered technology company. AGPT Ltd has no political affiliations, no governmental funding, and no partisan investors. The Platform's revenue comes from subscriptions: officials subscribing to analytics concerning their own mandate, and institutional subscribers purchasing Data Access (see C.5). The Neutrality Charter, published on every national platform, commits Teisond to algorithmic transparency and non-interference.

Q6. Who finances the Platform?

A. Development is self-funded by AGPT Ltd. Ongoing operations are financed through subscriptions from officials and institutions, who pay for detailed analytics. Citizens use the Platform free of charge. There is no advertising, no sale of data, and no political sponsorship.

Q7. In which countries is Teisond available?

A. Every jurisdiction meeting the criterion of a consolidated democracy has a national platform ({country}.teisond.com) in the local language. Some are fully activated; in others the national database of mandates is still being assembled, which is the one component of deployment that takes time. The current composition of the network, and the state of each jurisdiction within it, is shown on teisond.com. Adding a further jurisdiction to the operating network takes a matter of days.

C.2 For Citizens

Q8. How do I participate?

A. Browse your national platform ({country}.teisond.com) freely – no account is needed to view current legitimacy indices. When you decide to record your first judgment on an official, the Platform asks you to confirm you are a unique, real person, through your national digital identity service where available, or an authorised verification provider. That first judgment opens your account; from then on you can express trust or distrust toward any official, and you return to your account without verifying again.

Q9. Is participation free?

A. Yes. Registration, identity verification, and expressing civic judgments are entirely free. Paid features are available only for officials and institutional subscribers who want enhanced analytics.

Q10. Do I have to verify my identity just to look?

A. No. Viewing current indices and official profiles is open to everyone, with no account and no verification. Identity verification is requested only at the moment you record your first judgment, and only to guarantee one citizen, one account. Your name, your document and your contact details pass through the verification provider and are never written to the Platform's storage: what the Platform keeps is a single irreversible fingerprint.

Q11. How is my anonymity guaranteed?

A. Your identity data are processed through one-way cryptographic hashing (SHA-256 with a seasonal salt), and the Platform stores only the resulting fingerprint. That fingerprint remains pseudonymised personal data under the GDPR, and the Platform treats it as such, but nothing exists from which your name or identifier could be recovered: the original data are never written to storage, and even the Platform's developers cannot determine who you are. The salt rotates annually and old salts are permanently deleted, so that after the retention period the material required for any retroactive identification no longer exists.

Q12. Can I change my judgment?

A. Yes. Your standing judgment on any mandate can be changed at any time, or withdrawn entirely, which returns you to neutrality. Neutrality is not a third position but the absence of a record. To prevent manipulation, changes are rate-limited. Only your standing judgment counts, and the system stores no history of your changes.

Q13. What happens if I delete my account?

A. Your account, your access key, and your identity fingerprint are permanently removed, and your active judgments stop counting toward officials' current indices, which are recalculated as if you had never participated. What remains is the historical record of the indices themselves – the values they held on past dates – kept solely as anonymous aggregate figures with no link to you. The contribution your judgments already made to that history cannot be undone, but nothing in it can ever be traced back to you.

Q14. What are my rights under GDPR?

A. You have the right to access your data, the right to erasure (account deletion), and the right to lodge a complaint with your national data protection authority. The fingerprint the Platform holds is pseudonymised personal data under the GDPR and is treated as such, but because the hashing is irreversible and the source data are never written to storage, there is nothing from which you could be identified. For data subject requests, contact privacy@teisond.com.

C.3 Method & Privacy

Q15. Do you measure the office or the person?

A. The object of measurement is the person currently holding the mandate. The unit of publication is the mandate together with the calculation period. No individual citizen record is ever exposed.

Q16. What happens if there are not enough judgments?

A. Below the publication threshold for the level of authority concerned, no ratio is published. The profile shows instead how many standing judgments have accumulated and how many are still needed. The moment the threshold is crossed, the index opens.

Q17. What are the privacy guardrails?

A. Aggregate outputs only; no per-user histories; no demographic correlations; no micro-segments below thresholds; rounding to reduce false precision. The Platform is built as privacy by construction: the categories of data that could expose an individual have no containers in the schema, so data that could be handed over do not exist.

Q18. How do you prevent manipulation?

A. Since only verified, unique citizens can participate – each confirmed as a real person through national digital identity or an authorised provider – bot attacks are structurally impossible. The real threat is coordinated campaigns by real people. Integrity systems detect bursts, temporal clustering, geographic concentration, and account-age anomalies. The Platform favours disclosure over suppression: suspicious patterns are flagged publicly with a plain-language transparency note. Detection specifics are not published to prevent gaming.

Q19. What is the period of measurement?

A. The index is a snapshot of all standing judgments at the moment of calculation, and calculation occurs at a cadence configured per jurisdiction. Between calculations the published figure does not move, because the next snapshot has not yet been taken. The sequence of snapshots forms the historical series from which trends are read.

C.4 Reading and Using the Index

Q20. How should journalists cite the metric?

A. Use mandate, calculation date, index and confidence interval, for example: "Mayor of Riverton, 12 Sep 2025: 63.4 (95% CI 61.9–64.9)". Avoid over-interpreting the noise of a single calculation; discuss trajectory and confidence. Do not use the index as an election forecast.

Q21. What does a decline mean?

A. Erosion of public acceptance of authority. It is a signal for explanation, engagement, or course correction – not a legal verdict or a recall mechanism.

Q22. Can I compare across regions or levels?

A. Yes, via benchmarks (aggregated comparisons), which are available at the analytical level. Ensure comparable calculation dates and note differences in sample sizes and confidence intervals.

Q23. Do you publish breakdowns by age, gender, or party?

A. No. To prevent profiling and re-identification, no demographic breakdowns are provided at any access level.

C.5 Product & Access

Q24. What's public vs. paid?

A. Public (free, no account): the headline legitimacy index for every mandate above its publication threshold, the progress of accumulation for those below it, full methodology, and anomaly flags. Subscriber (paid, officials and institutions): absolute trust and distrust counters, consensus index, confidence intervals, trend indicators and direction of movement, historical series of snapshots, comparative analytics, and anomaly reports. No row-level or individual data at any level.

Q25. Is there an API?

A. Yes – aggregates-only. Endpoints expose indices, benchmarks, and alerts with rate-limits and audit trails. Queries below publication thresholds are rejected.

Q26. How are official subscriptions priced?

A. Fixed pricing by authority level (L1–L4), adjusted per jurisdiction for accessibility. Pricing is structured to avoid any conflict of interest: fees are fixed regardless of the index value, so there is no incentive for the Platform to influence results. The subscription provides access to analytics – it does not affect the index in any way.

C.6 Officials, Media & Civil Society

Q27. I'm an official – how should I use this?

A. Track your trajectory with confidence intervals. Read transparency notes. Address the causes of decline through the conduct of your office. Legitimacy is sustained by accountability, not by messaging.

Q28. Can an official contest the index?

A. The index reports what verified citizens have expressed, so there is nothing in it to contest. What is available is the right of reply: your official statement is published alongside your own index, in the same plane of public visibility. Recalculations occur only under the revision policy, meaning material error, a confirmed bug, or verified manipulation. Individual citizen data are never disclosed.

Q29. Can an official "opt out" of monitoring?

A. No. Public office is an object of legitimate public interest. Publications are aggregated and subject to privacy thresholds. Officials retain the right of reply and may subscribe for detailed analytics concerning their own mandate.

Q30. Can a new office be added to monitoring?

A. Yes. The criterion is that the position involves the exercise of governmental authority. A newly added mandate shows the progress of accumulation until its publication threshold is reached.

Q31. I'm a watchdog/NGO – what can I do with it?

A. Use benchmarks and alerts to prioritise oversight and to surface early-warning signals, and take up sustained declines with the institutions concerned. Subscriber access provides historical series for longitudinal analysis.

Q32. I'm a journalist – what are common mistakes?

A. Treating the index as an election horse-race; ignoring the confidence interval; cherry-picking a single calculation; inferring motives without evidence; asking for disallowed micro-segments; and presenting the index without noting sample size.

C.7 Compliance & Operations

Q33. Who is the data Controller under GDPR?

A. AGPT Ltd is the data Controller for all national platforms. Cloud infrastructure providers operate as Sub-processors under data processing agreements. See § 6.2.

Q34. Where is citizen data stored?

A. Each jurisdiction's citizen data are stored in infrastructure appropriate to that jurisdiction, satisfying the data residency requirements that apply to it. National deployments are isolated tenants: a breach affecting one jurisdiction's infrastructure does not compromise any other.

Q35. What gets published if there's a suspected manipulation attempt?

A. The aggregated index remains (subject to thresholds), accompanied by an anomaly flag and a plain-language transparency note.

Q36. Do you ever remove or revise published numbers?

A. Material changes follow publication policy: rationale, public notice, and versioned records. Revisions are documented, not hidden. The revision history is part of the public transparency archive.

Q37. How do I exercise my GDPR rights or file a complaint?

A. Contact privacy@teisond.com for data subject requests (access, erasure, portability). You also have the right to lodge a complaint with your national data protection authority. Response timelines comply with GDPR requirements (30 days).

C.8 Governance Evolution

Q38. Will there be decentralised governance or tokens?

A. In the long term, Teisond may introduce a governance-utility mechanism allowing citizens and public-interest actors to participate in decisions about standards, transparency processes, and matters not involving personal data. This is not a financial instrument, not equity, and not a substitute for platform access. No token sale is planned at this stage. See §6.6.1 for the governance evolution roadmap and Section 9 for the civic ownership architecture.

Q39. How do you prevent governance capture?

A. Any future governance participation operates within strict guardrails: quorums, proposal cooldowns, rate-limits, transparent delegation, and revocation for abuse. Governance processes never touch personal data, profiling, or index methodology. Core publication rules remain under AGPT Ltd authority as mission protection.

APPENDIX D: BIBLIOGRAPHY AND REFERENCES

Citation style: APA 7th (concise). Purpose: sources that inform the White Paper's theoretical footing, measurement choices, privacy guardrails, integrity controls, and governance stance. Inclusion ≠ endorsement of any policy position.

D.1 Core Theory of Legitimacy and Democratic Accountability

- Weber, M. (1978). *Economy and Society* (G. Roth & C. Wittich, Eds.). University of California Press. – Classic typology (traditional/charismatic/legal-rational).
- Easton, D. (1965). *A Systems Analysis of Political Life*. Wiley. – Regime support vs support for authorities; basis for focusing on officials.
- Easton, D. (1975). A Re-assessment of the Concept of Political Support. *British Journal of Political Science*, 5(4), 435–457. – Refinement of "support" signals over time.
- Beetham, D. (1991). *The Legitimation of Power*. Palgrave. – Legitimacy as a normative and empirical concept (used here to separate acceptance from popularity).
- Dahl, R. A. (1971). *Polyarchy: Participation and Opposition*. Yale University Press. – Accountability and participation between elections.
- Pitkin, H. F. (1967). *The Concept of Representation*. University of California Press. – Representation vs ongoing responsiveness (motivates continuous signals).
- Schedler, A. (1999). Conceptualizing accountability. In A. Schedler, L. Diamond, & M. F. Plattner (Eds.), *The self-restraining state: Power and accountability in new democracies* (pp. 13–28). Lynne Rienner. – Classic treatment distinguishing answerability and enforcement; supports the need for a continuous, inter-electoral accountability signal focused on officials.

D.2 Measurement and Statistical Guardrails

- Agresti, A. (2013). *Categorical Data Analysis* (3rd ed.). Wiley. – Foundations for proportion estimates and uncertainty.
- Agresti, A., & Coull, B. A. (1998). Approximate is better than "exact" for interval estimation of binomial proportions. *The American Statistician*, 52(2), 119–126. – CI choice for aggregated binary inputs.
- Clopper, C., & Pearson, E. S. (1934). The use of confidence or fiducial limits... *Biometrika*, 26(4), 404–413. – Reference for conservative intervals.
- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 15. – Taxonomy for integrity/flagging systems.

D.3 Privacy by Design and Publication Thresholds

- Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 557–570. – Basis for thresholds and anti-reidentification.
- Dwork, C. (2006). Differential Privacy. In *ICALP 2006* (pp. 1–12). Springer. – Foundational privacy framework; informs the Platform's approach to threshold-based publication safeguards.
- European Union. (2016). Regulation (EU) 2016/679 (GDPR). – Roles (Controller/Processor), lawful bases, data-minimization; see §§ 5.4 & 6.2.
- NIST. (2020). SP 800-53 Rev. 5: Security and Privacy Controls. – Catalog for security controls (hosting/SLA alignment).
- ISO/IEC 27001. (2022). Information Security Management. – Governance benchmark for managed hosting.

D.4 Human Rights and Public Interest Basis

- United Nations. (1948). Universal Declaration of Human Rights (Art. 19). – Expression and access to information.
- UN General Assembly. (1966). International Covenant on Civil and Political Rights (Arts. 19, 25). – Participation in public affairs; expression.
- Council of Europe. (1950). European Convention on Human Rights (Art. 10). – Freedom of expression.

D.5 Neutrality, Transparency and Media Use

- Tufte, E. R. (2001). *The Visual Display of Quantitative Information* (2nd ed.). Graphics Press. – Clarity over spin; avoid deceptive visuals.
- Groves, R. M., et al. (2009). *Survey Methodology* (2nd ed.). Wiley. – Limits of episodic polling (motivates continuous, low-friction signals).
- Meyer, P. (2002). *Precision Journalism* (4th ed.). Rowman & Littlefield. – Standards for reporting quantitative findings (CI, uncertainty, reproducibility).
- Council of Europe, Committee of Ministers. (2004). Recommendation Rec(2004)16 on the right of reply in the new media environment. – Normative basis for the right of reply and transparent notes, favouring disclosure over takedowns while protecting individuals.

D.6 Governance, Tokens and DAO (Non-Financial, Scoped)

- Buterin, V. (2021). *The Most Important Scarce Resource is Legitimacy*. (essay). – Legitimacy in decentralized governance (conceptual backdrop; not financial).

- Hassan, S., & De Filippi, P. (2021). Decentralized Autonomous Organizations. *Internet Policy Review*, 10(2). – Overview of DAO governance patterns and risks.
- Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. – Early articulation of on-chain governance boundaries.

Note: Token here is governance-utility only (non-financial, no personal data), per §6.6.1, Section 9, and Appendix A.7.

D.7 How to Cite this White Paper

- In text: "Teisond White Paper (v10.0, 2026-08-09), Section N.M."
- Bibliography entry: Teisond White Paper, v10.0 (2026-MM-DD). AGPT Ltd. CC BY-ND 4.0.

D.8 Versioning Note

This bibliography is maintained with the method. When publication rules, thresholds, or security controls materially change, the bibliography and cross-references are updated in the next minor version.

APPENDIX E: GOVERNMENTAL AUTHORITY – DETAILED POSITION ESTIMATES BY LEVEL

This Appendix provides detailed breakdowns of official positions at each of the four authority levels described in Section 2.2. Estimates are based on publicly available institutional data from consolidated democracies and represent ranges reflecting the diversity of administrative structures found among them. These figures serve as reference material for database construction and coverage planning; the Platform's actual database is populated progressively from official registries and institutional directories.

All estimates refer to a typical mid-sized democracy unless otherwise noted. Actual counts vary significantly by country size, administrative tradition, and institutional structure.

E.1 Level 1: National Authority

Executive Branch (60–80 officials per country)

Head of State and/or Head of Government: 1–2 positions. Deputy Heads of Government: 1–4 positions, varying by system. Cabinet Ministers: 15–25 ministers leading major government departments, including Interior/Home Affairs, Defence, Economy/Finance, Foreign Affairs, Justice, Education, Health, Transportation, Environment, Labour, and Agriculture. Junior Ministers and Secretaries of State: 30–50 senior political appointees; each ministry typically has 1–3 junior ministers handling major policy areas. Heads of major national agencies (politically appointed): 10–20 officials, including intelligence services, transportation authorities, national railways, airports authority, postal services, and broadcasting corporations.

Legislative Branch (520–560 officials per country)

Lower chamber (primary legislative body): 300–400 members in a mid-sized country. Upper chamber (if bicameral): 200–250 members. Legislative leadership – speaker, deputy speakers, committee chairs: 30–50 officials. Party leaders and parliamentary group leaders: 8–15 officials.

Other National Positions (5–15 officials per country)

Supreme or Constitutional Court justices (where appointments are political): 10–15 justices. Ombudsman and similar oversight institutions: 1–3 officials. Heads of major regulatory agencies (if politically appointed): 3–8 officials, including securities regulator, competition authority, telecommunications regulator, and energy regulator.

Level 1 Summary

Typical count per democracy: 250–800 officials, depending on population and institutional structure. National official counts scale sublinearly with population: legislative chambers do not triple when population triples, and the largest national assemblies in consolidated democracies are rarely more than seven or eight times the size of the smallest.

E.2 Level 2: Regional Authority

Regional Executives (50–70 officials per country)

Regional heads (governors, regional presidents, premiers): 12–18 officials. Deputy regional heads and senior councillors: 30–50 officials. In federal and devolved systems, these include regional equivalents of cabinet ministers; in centralised systems, senior administrators.

Regional Legislators (1,200–1,300 officials per country)

Regional assembly or state legislature members: 1,100–1,200 representatives. Size varies – larger regions may have 100+ members, smaller regions 50–80. Regional assembly leadership and committee chairs: 50–100 officials.

Provincial/Intermediate Governance (where applicable, 50–100 officials per country)

Some jurisdictions maintain an intermediate tier between regional and municipal levels: provincial governors, council leaders, or provincial administrative directors.

Level 2 Summary

Typical count per country: 400–2,500 officials, depending on administrative structure. Federal and strongly devolved systems have substantially more regional officials per capita than centralised unitary systems. The number of first-tier administrative subdivisions ranges from three to around twenty across consolidated democracies of comparable size.

E.3 Level 3: Municipal Authority

Municipal Structure Variation

Municipal structure shows the greatest variation of all. Some jurisdictions have many thousands of small municipalities; others have consolidated their local government into fewer than a hundred larger units. Municipal autonomy also varies: some traditions grant strong municipal authority, while centralised systems retain more control at regional and national levels.

For a mid-sized country, the approximate distribution is: major cities (over 500,000 population): 5–10; mid-size cities (100,000–500,000): 30–60; small cities (20,000–100,000): 200–400; towns (5,000–20,000): 1,000–2,000; small towns (under 5,000): 2,000–3,000.

Municipal Executives

Mayors: one per municipality, totalling 3,000–5,000 officials. Deputy mayors and municipal managers: approximately 1,000–2,000 officials.

Municipal Legislators (Councillors)

Total varies enormously based on municipal structure and council size regulations. Major cities: 25–60 councillors each (150–600 total). Mid-size cities: 15–30 each (450–1,800 total). Small cities: 11–21 each (2,200–8,400 total). Towns: 7–15 each (7,000–30,000 total). Small towns: 5–9 each (10,000–27,000 total). Potential total: 20,000–70,000 municipal legislators in a mid-sized country.

Municipal Administrators

Municipal secretaries and managers: 2,000–4,000. Department directors in larger municipalities: 1,000–3,000.

Level 3 Summary

Typical count per mid-sized democracy: 25,000–80,000 officials, with a wide range depending on municipal structure.

E.4 Level 4: Local Officials and Appointed Administrators

Education Sector (15,000–25,000 officials per country)

School principals and directors (public schools): 10,000–18,000 officials across primary and secondary schools. Each principal exercises authority over disciplinary decisions, teacher assignments, curriculum implementation, school policies, budget allocation, and parent-teacher relationships. School district administrators and inspectors: 500–1,500 officials. University and college administrators: 200–500 officials (where publicly managed). Regional education directors: 200–500 officials.

Law Enforcement and Public Safety (8,000–15,000 officials per country)

Local and municipal police chiefs: 3,000–6,000 officials, exercising authority over traffic enforcement, community policing, response protocols, and personnel deployment. National or state police local commanders: 1,000–3,000 officials. Fire department chiefs: 1,000–2,000 officials. Emergency services directors: 500–1,500 officials. Prison directors (where publicly managed): 200–500 officials.

Regulatory and Inspection Services (10,000–20,000 officials per country)

Building inspectors and urban planning officials: 3,000–7,000 officials, with authority over permit approvals, building code compliance, and construction authorisation. Health and safety inspectors: 2,000–4,000 officials. Environmental inspectors: 1,000–3,000 officials. Labour inspectors: 1,000–2,000 officials. Consumer protection officials: 500–1,500 officials. Licensing and permit officials: 2,000–4,000 officials.

Social Services and Public Welfare (8,000–15,000 officials per country)

Social services directors and supervisors: 4,000–8,000 officials, with authority over benefit eligibility, service allocation, case management, and emergency assistance. Child welfare

supervisors: 1,000–3,000 officials. Public housing administrators: 1,000–2,500 officials. Disability services administrators: 1,000–2,000 officials. Employment service directors: 1,000–2,000 officials.

Healthcare Administration (3,000–7,000 officials per country)

Public hospital directors: 500–1,200 officials (where healthcare is publicly managed). Health centre directors: 2,000–5,000 officials. Regional health service directors: 50–150 officials. Emergency medical services directors: 200–800 officials.

Administrative and Financial Services (8,000–15,000 officials per country)

Tax office local directors: 1,000–3,000 officials. Social security and pension office directors: 1,000–3,000 officials. Vehicle registration office directors: 500–1,500 officials. Land registry officials: 2,000–4,000 officials. Municipal finance directors: 1,000–2,000 officials. Pension and benefits administrators: 2,000–3,000 officials.

Judicial and Legal Services (5,000–10,000 officials per country)

Local and regional court judges: 4,000–8,000 judges across civil, criminal, administrative, and family courts, with authority over case decisions, sentencing, and custody determinations. Magistrates and justices of the peace: 1,000–3,000 officials. Public prosecutors at local level: 500–1,500 officials.

Transportation and Infrastructure (3,000–7,000 officials per country)

Public transit authority directors: 500–1,500 officials. Municipal public works directors: 2,000–4,000 officials. Port authority directors: 50–150 officials. Airport directors: 30–100 officials (where publicly managed).

Environmental and Utilities Services (2,000–5,000 officials per country)

Water utility directors: 500–1,500 officials. Waste management directors: 500–1,500 officials. Parks and recreation directors: 500–1,500 officials. Environmental protection officers: 500–1,500 officials.

Cultural and Community Services (3,000–6,000 officials per country)

Library directors: 1,000–2,000 officials. Museum directors: 500–1,200 officials. Community centre directors: 1,000–2,000 officials. Sports facility directors: 500–1,500 officials.

Level 4 Summary

Typical count per mid-sized democracy: 50,000–150,000 officials – by far the largest category of officials exercising governmental authority.