Isle of Man Government

DIGITAL ISLE OF MAN

CONSULTATION PAPER

A Data Governance Framework

Data Asset Foundations

October 2026

Digital Isle of Man | Department for Enterprise



CONSULTATION PAPER

NOT FOR LEGAL RELIANCE

This Consultation Paper is issued in connection with the Foundations (Amendment) Act 2026 and the implementing instruments made or to be made under it. It is explanatory. It does not constitute legal advice, is not a statement of current law, and is not the authoritative record of the Regime. Matters identified as recommended or proposed have not been given legal effect and remain subject to change through the regulatory process.

Issued by:

Digital Isle of Man
Department for Enterprise
Isle of Man Government

Author:

Aga Strandskov
Head of Data Strategy
Digital Isle of Man

Date issued:

October 2026

Contents

Part 1: Context **6**
1.1 The Data Asset Foundations regime 6
1.2 What the Data Governance Framework covers 6
1.2.1 Building on DCAM and CDMC 7
1.3 The three categories of the framework 8
1.4 Scope of the consultation 9
1.5 Who this affects 10
Part 2: Design principles **12**
2.1 Designed coexistence with data protection law 12
2.2 Distributed governance 12
2.3 Constitutive, not behavioural 13
2.4 Proportionality 14
2.5 Phased capability 14
2.6 Bounded commitment 15
Part 3: The architecture of the framework **16**
3.1 The instrument family 16
3.1.1 Headline instruments 17
Above the categories: the enabling instrument 17
Category 1: Obligations of the DAF Council 17
Category 2: Other Actors in the Ecosystem 18
Category 3: Data Asset Boundary and Material Change 19
3.2 The role architecture 20
3.2.1 Proposed allocation of functions across the roles 22
3.2.2 Bodies outside the statutory role architecture 23
3.3 The seven loci of governance 23
3.3.1 DCAM and CDMC in the locus model 25
3.4 The Asset Boundary Profile and two-axis classification 25
3.4.1 The two-axis classification 26
3.4.2 Governance signals 27
3.5 The accreditation ladder 28
3.5.1 Mandatory Level 3 in the highest classification cells 29
3.5.2 Design features of the ladder 30
3.5.3 Three modulators 30
Part 4: How the framework works in practice **32**
4.1 Establishing a data asset foundation 33
4.2 Dedicating and registering a data asset 35
4.2.1 The dedication instrument 35

4.2.2 Application and provisional registration 35
4.3 Full registration and the property right 36
4.3.1 Completing registration 36
4.3.2 What the property right is 37
4.3.3 Interoperability with other registers: the position at launch 37
4.4 Utilisation under the governance wrapper 38
4.4.1 Use outside the wrapper 38
4.4.2 Third-party rights within a dedicated asset 39
4.5 Material change and Tier 2 amendments 40
4.6 Accreditation lapse and remediation 41
4.6.1 Accreditation is binary 41
4.6.2 The remediation pathway 41
4.6.3 Preservation during remediation 42
4.6.4 Suspension, and lapse of a mandated Level 3 assessment 42
4.7 Reversion or removal 42
4.8 Worked examples 43
4.8.1 Example A: An anonymised clinical research dataset 43
4.8.2 Example B: An AI training corpus 44
4.8.3 Example C: A telemetry asset as collateral 45
Part 5: The data protection interface 47
5.1 Two regimes, two objects 47
5.2 The non-derogation principle 48
5.3 Controllership 48
5.4 Dedication is not a lawful basis 51
5.5 Data subject rights and the register 52
5.5.1 Erasure and rectification are not the enemies of register integrity 52
5.5.2 The data subject rights amendment pathway 52
5.5.3 Amendment and the validity of the accreditation 52
5.5.4 Compliance and the protection against unauthorised use 53
5.6 Register publicity and data minimisation 53
5.7 Parallel enforcement 54
5.8 The anonymisation boundary 54
5.9 Working with the Information Commissioner 55
Part 6: Assurance and accreditation 57
6.1 Introduction: who checks? 57
6.2 The Accredited Assurance Provider scheme 58
6.2.1 Accreditation of providers by the Department 58
6.2.2 Appointment by foundations and the provider's function 59
6.2.3 Conduct standards, independence and the integrity of attestation 59
6.2.4 Changing provider, continuity and appeals 60

6.2.5 Liability, insurance and the limits of an attestation 61
6.3 The assurance ladder 62
6.3.1 Mapping the ladder to the statute 64
6.3.2 Signals, and the naming discipline 64
6.4 Accreditation and register standing: the statutory position 64
6.4.1 Accreditation is binary 64
6.4.2 The remediation pathway 64
6.4.3 Reversion and preservation during prohibited-use periods 65
6.4.4 Suspension 65
6.4.5 Signals and standing: the two layers restated 66
6.5 The Level 3 mandate 66
6.5.1 The mandate and its trigger 66
6.5.2 How the mandate binds 66
6.5.3 What the mandate means in practice 66
6.6 The Departmental recommendation for the initial cohort 67
6.7 Phasing and market readiness 67
6.8 Recognised equivalent standards 68
6.9 International interoperability: a phased path 69
Part 7: Oversight and the actors in the ecosystem 70
7.1 Oversight without a regulator 70
The normal response pathway and direct duties 71
The boundary around private-law offices 71
7.2 The data enforcer (sections 86 and 87) 72
The nature of the office 72
The functions proposed 72
What the office is not 73
Independence, qualification and liability 73
Protected disclosure to the data enforcer 74
7.3 The data asset registrar (section 77) 75
7.4 The Department 75
7.5 The Verification Agent 76
7.6 The High Court (section 91) 76
7.7 The oversight pathway end to end 77
Part 8: Roadmap 80
Annex A: Proposed Asset Boundary Profile Schema 82
A.1 Purpose and status of this Annex 82
A.2 General rules for drawing the boundary 82
A.3 The proposed seven attributes 83
A.3.1 Definitional scope 83

A.3.2 Temporal scope 84
A.3.3 Provenance scope 84
A.3.4 Classification coordinates 85
A.3.5 Derivation rule 85
A.3.6 Governance status 86
A.3.7 Identity-preserving change envelope 86
A.4 What the Profile does not contain 87
Annex B: Index of DGF Framework Instruments 89
B.1 About this Annex 89
B.2 The framework instruments 90
B.3 Private instruments 94

Part 1: Context

1.1 The Data Asset Foundations regime

The Foundations (Amendment) Act 2026 introduces the data asset foundation: a new type of Manx foundation whose purpose is the holding and stewardship of data as a recognised asset. Data is formally dedicated to the foundation through a dedication instrument, recorded on the Data Asset Register, and — on full registration — becomes the subject of a personal property right vested in the foundation. The foundation is governed by a council; reviewed by a specialised Data Enforcer; and, in respect of its assets, subject to independent assurance by an Accredited Assurance Provider.

The design of the Data Asset Register is set out in the Department's white paper Data Asset Register and Data Asset Registrar: Architecture, Governance, Classification, Operation and Technical Design, in its earlier consultation and policy papers, and in the technical materials describing the Register's architecture. This paper does not repeat that ground. Its subject is section 69 of the Act, which requires the Department to make regulations establishing a data governance framework that imposes minimum requirements to be met by data asset foundations and their councils. This paper is the consultation on the design of that framework.

1.2 What the Data Governance Framework covers

The framework the Act calls the “data governance framework” is a term of art. It requires explanation, because in industry usage the phrase “data governance” has a narrower meaning than the meaning the Act gives it.

In the specialist vocabulary of data professionals, data governance is a discrete organisational discipline concerned with authority and control over data assets: the appointment of data owners and stewards, the setting of policies and standards, the definition of metadata, the operation of an internal governance council. It is one component of a broader data management practice that also covers architecture, quality, security, access and lifecycle operations. Established frameworks reflect this division: the EDM Association's Data Management Capability Assessment Model (DCAM) identifies it as one of eight core components; its Cloud Data Management Capabilities framework (CDMC) treats governance and accountability as one of six components of a controls-based framework; DAMA-DMBOK identifies data governance as one of eleven knowledge areas. In each, data governance is bounded, and it sits alongside separate treatments of corporate governance (the governance of the organisation itself), of process governance (the governance of business processes), and of data management (the operational disciplines around the data).

The Act uses the phrase differently. Section 69 requires minimum requirements for the operation of data asset foundations in respect of their data assets. Those requirements cannot be confined to the discipline that industry names data governance; the foundation is a legal entity with fiduciary duties, the register is a constitutive record with a lifecycle, the ecosystem contains supervisory and assurance roles that industry frameworks do not envisage, and the interface with data protection law is central. The

framework the Act mandates is necessarily broader than the industry term, and covers each of the following.

The governance of the foundation itself. What industry would call corporate governance: the council's constitution, qualifications, duties, decision making processes and fiduciary obligations, adapted to the data holding purpose of the foundation.

The governance of the processes by which data is dedicated, registered, amended and (where applicable) removed. What industry would call process governance, applied to the constitutive lifecycle events of a registered asset: provisional and full registration, Tier 2 amendments, remediation, reversion. Most of these provisions are covered under the DAR regulations.

Data governance in the industry sense. The description, classification, ownership and stewardship of data assets — carried, in this regime, by the Asset Boundary Profile, the two-axis classification, the governance signals and the recorded governance terms.

Data management in the broader sense. Quality, security, access, records, lifecycle operations — the operational disciplines that data professionals expect a data management framework to cover. In this regime, most of these are set at the standards tier and applied through the accreditation ladder.

The regulatory interface. The coexistence of the regime with data protection law, sectoral regulation and other applicable frameworks.

The assurance architecture. The Accredited Assurance Provider scheme, the accreditation ladder, the Verification Agent and the supervisory arrangements that give the register its credibility. Treated at Part 6.

A data professional reading the framework should understand that it is broader than what the name would suggest. A lawyer or council member reading it should understand that it is more technical than a purely corporate governance framework would be. Both are correct, and the breadth is a consequence of the regime it supports: a legal form whose purpose is the governed holding of data as an asset must operate across the whole span from foundation constitution to technical operation of the register.

The Department has considered whether an alternative name would reduce the terminological confusion. The name is fixed by section 69 of the Act, and this paper does not propose to depart from it; but the Department's intention throughout the framework's supporting instruments is to be explicit about what the phrase means in this context, and to avoid drafting that assumes the industry narrow meaning.

1.2.1 Building on DCAM and CDMC

The breadth of the statutory term does not mean that the framework has been designed from first principles. The Department has drawn deliberately on two frameworks published by the EDM Association. DCAM describes the capabilities an organisation needs in order to manage its data with the discipline it would apply to any other asset of value. CDMC sets out the key controls for managing sensitive data in cloud environments, with an emphasis on controls that are evidenced and, wherever possible, automated. Much of what this framework requires of a registered data asset will be familiar to anyone who knows either.

The relationship operates in three distinct ways.

Design. The principles of DCAM and CDMC are embedded throughout the framework, modified for its distributed design. Accountability for data, authoritative sources and lineage, cataloguing and classification, purpose bound entitlements, security, data quality, retention, cross-border movement and the monitoring of control compliance are each carried into the framework. What changes is who carries them. In an enterprise they sit within a data management programme that the organisation builds for itself; here they are carried by the register, the Asset Boundary Profile, the classification matrix, the governance wrapper and the assurance ladder, with the foundation's own operational layer performing what remains. Part 3.3.1 sets out where each principle sits and how it has been adapted.

Recognition. DCAM and CDMC are proposed as the first schemes on the Recognised Standards list, so that an assessment under either may be recorded as a Level 3 external assessment. Either may also be credited as evidence within Levels 1 and 2 where its scope is relevant, on terms set in the Verification and Accreditation Framework (Part 6.8).

Market. The assurance and oversight roles draw on the EDM Association's existing professional community. Current Authorised Partner status is the qualifying route to competence for Accredited Assurance Providers at launch (Part 6.2.1), and the Department proposes to leverage the EDM Association's training programme in the accreditation of data enforcers (Part 7.2).

What the framework does not do is make a DCAM or CDMC assessment the test for the statutory data asset accreditation. Levels 1 and 2 are assessed against the framework's own attestation profiles and DAR Code controls, set at standards tier, for two reasons. Their object is the registered asset, whereas DCAM and CDMC assess the capability and the control environment of an organisation. And several functions that both frameworks place within the organisation are performed here by the register, the Verification Agent or an independent provider, so an assessment of the foundation's own arrangements would not reach them (Part 3.3.1).

The Department acknowledges with thanks the work of the EDM Association, and of the practitioners who developed DCAM and CDMC, which provided the building blocks of this framework.

1.3 The three categories of the framework

For navigation, the instruments that make up the Data Governance Framework are organised into three categories. The categories reflect what each set of instruments does rather than the technical domain each covers. This means that a reader looking for a particular topic — for example, records retention — will find it grouped with the instruments dealing with the council's duties, even though records retention would in an industry taxonomy sit under information governance or lifecycle management.

Category 1 — Obligations of the DAF Council. The instruments that set out what the foundation itself must do. These are the operational content of section 88 of the Act and of the framework's minimum requirements imposed on foundations and their councils. The category includes Practice Direction 1 (Obligations of the Data Asset

Foundation). It is where a prospective council member, an administrator, or a legal adviser will look first.

Category 2 — Other Actors in the Ecosystem. The instruments that set out the functions and conduct of the actors other than the foundation itself: the Data Enforcer, the Accredited Assurance Provider, the Registrar (included by reference to the DAR regulations), the Verification Agent, and the Information Commissioner at the data protection interface. It is where a reviewer, an assurance provider or a regulator will look first.

Category 3 — Data Asset Boundary and Material Change. The instruments that describe what a registered data asset is and how it changes. The category includes the Classification and Metadata Standard, the Data Quality Standard, the Sector and Residency signals, and the elements of the DAR Regulations dealing with the amendment regime. It is where a data professional working on the technical description, classification and governance of a specific asset will look first.

Two further statutory instruments belong to the family. Model foundation rules for data asset foundations may be prescribed by regulations (section 74, with section 92(3)(v)); where the rules of a foundation are silent on a matter for which the model rules provide, and do not exclude it, the model provision is deemed included, and an amendment to the model rules does not affect a foundation established before it takes effect. Regulations may also add to the documents and records a foundation must keep at its business address (section 89, supplementing section 41 of the 2011 Act), which is the anchor for the Records Retention Standard in Category 1. Above the three categories sit the DGF Regulations themselves — the principal subordinate instrument, providing the enabling powers for the Standards and Practice Directions and the definitions that apply across the framework.

The categories are for navigation, not for exclusive assignment. Several instruments carry content that speaks to more than one category. The Verification and Accreditation Framework sits primarily in Category 2 because it defines the AAP role, but it is read against Category 1 when a council is engaging with its accreditation duties, and against Category 3 when an AAP is attesting the correspondence of an asset to its registered description. The category into which an instrument is placed indicates its principal subject; it does not exclude relevant content from adjacent categories, and readers are directed across categories where the interlock is significant.

1.4 Scope of the consultation

The consultation will cover the design of the Data Governance Framework as a body of subordinate legislation and supporting standards. The Department will consult on the proposed structure, the allocation of governance functions across the statutory roles, the architecture of the supporting accreditation ladder and the data protection interface.

The following will not be within the scope of the consultation. The Foundations (Amendment) Act 2026 itself has been enacted; the policy decisions reflected in the primary legislation are settled. The establishment of the Data Asset Register and the appointment of the Data Asset Registrar are in delivery phase, following the previous consultation. Statutory powers under the Act are retained by the Department for

Enterprise, which delegates their exercise as appropriate either to the registrar, whose function is administrative and operational, or to Digital Isle of Man, to which policy and architecture development for the regime is delegated. The third implementing instrument, the minimum viable enforcement regulations, will provide the internal reconsideration procedure required at launch. Its commencement is a launch dependency. The wider design of civil penalties and supervisory enforcement against contraventions of the framework will be the subject of a separate consultation; this paper is silent on the form sanctions will take, save for the principle of no double penalisation with the Information Commissioner where the same conduct engages both regimes.

The Department's working position throughout this paper is the proposed position; consultation responses will shape the final framework. Where this paper expresses certainty, it does so because the position rests on the Act or on settled architectural decisions; where it expresses openness, it does so because the matter is properly for consultation.

1.5 Who this affects

The framework will have direct effect on the following:

Foundations established or intended to be established as data asset foundations, and their councils. The framework sets the minimum requirements to be followed in the conduct of the foundation's affairs in respect of its registered data assets; it shapes the qualifications expected of council members; and it provides the operational content that gives section 69 of the Act effect. The instruments primarily relevant to this audience are those in Category 1.

Accredited Assurance Providers. The framework determines what AAPs assess against, on what cycle, and how their attestations are recorded against the register. AAP accreditation criteria, attestation profiles and the formal levels of the accreditation ladder are set out in the Verification and Accreditation Framework in Category 2.

Data Enforcers. The framework determines the standards against which the Enforcer supervises the council's conduct in respect of the governance terms recorded on the register.

The Data Asset Registrar. The framework shapes the operational interface between the Registrar and the foundations whose assets are recorded; the Registrar's own functions are set in the Act and in the subordinate registration regulations made under it. The instruments in Category 3 most closely engage the Registrar's remit.

Indirect effects extend further. Lenders, licensees, custodians and counterparties relying on the register will read what the framework requires the register to record, and will calibrate their commercial positions accordingly. Controllers of personal data within registered assets will find that the framework shapes the interface with the Information Commissioner. Recognised standards bodies — notably the EDM Association in respect of DCAM and CDMC, and ISO in respect of relevant management system standards — are part of the regime's interoperability architecture through the recognition mechanism at Part 6.8.

The Department's intention is that the framework is read first by those it directly affects, with the more specialist sections (Part 5 on data protection; Part 6 on assurance) holding the detail their respective audiences will look for. Each Part is drafted so as to be capable of being read on its own, with cross-references where the content interlocks.

Part 2: Design principles

The framework rests on six principles. They are stated here so that readers can hold the architecture in Parts 3 and 4 against them, and so that consultation responses can engage with the principles as well as with the operational detail.

2.1 Designed coexistence with data protection law

The first and most important principle: the regime is designed to operate alongside the Data Protection Act 2018 and the Applied GDPR, not in displacement of either. Nothing in the framework limits, conditions or displaces any right of a data subject under that legislation, any obligation of a controller or processor or any function of the Information Commissioner. Where the framework's recording or governance requirements might otherwise pull against data protection law in any particular situation, the framework provides explicit resolution pathways — designed in, not bolted on.

The framing is deliberate. The Department recognises that the introduction of a property concept for data is read by some as an assertion of ownership over personal information, in tension with the principle that personal data is not the controller's commercial property. The framework treats that reading as resolvable. The personal property right vested in a data asset foundation by section 80(4) is in the composite of the data together with its recorded governance terms — the asset and its wrapper, considered together. No right of a data subject is assigned, waived or diminished by dedication of an asset; the foundation remains a controller of personal data within the asset, and every data subject right is exercisable against it as against any other controller. The register records governance state; it does not record, certify or substitute for consent or any other lawful basis.

The Department has worked through the points where the framework and data protection law touch the same facts and has identified resolution mechanisms for each. The substantive content of those mechanisms — the proposed controllership map, the data subject rights as amendment pathway, the parallel enforcement protocol and the test applied at the anonymisation boundary — is the subject of Part 5 and of the Data Protection Interface Statement that accompanies this paper. The Department's view is that, as drafted, the relationship is one of designed coexistence and not of conflict.

The Department's intention is that the framework provides the level of clarity that controllers, data subjects' representatives and the Commissioner can each rely on. Questions on the interface are at the heart of the consultation.

2.2 Distributed governance

The framework's organising idea is that data governance is the joint product of many parts, not the work of a single office. No single body “does data governance” for a registered data asset. Instead, each governance function — describing the asset, classifying it, verifying its conformity to that description, attesting its controls, reviewing its use, deciding remediation — is allocated to the part of the regime best placed to perform it.

Seven loci are identified. At the most binding end, the legislation and the framework's regulations and standards set the rules of general application: what every data asset foundation must do, and the minimums below which no foundation may go. The foundation's own constitutive documents and organs then carry the rules that the foundation itself adopts in addition to those minimums. The register records the asset and the rights and permissions attaching to it, in a form that is constitutive: what the register says is what the asset is for legal purposes. An automated Verification Agent verifies, by machine, those conditions that are mechanically checkable. An Accredited Assurance Provider attests the conditions that require professional judgement or site work. The Registrar maintains the integrity of the data asset register, and the Information Commissioner and the courts supervise. And the foundation's own operational layer — the council and any administrators or service providers it engages — is what remains: the residual work that cannot and should not be encoded.

The model is described in Part 3.3, with a table identifying each locus and its mechanism. The architecture supplies a common catalogue, classification scheme, policy framework, assurance record and escalation pathway. The foundation and its appointed providers remain responsible for operating the controls that discharge the recorded commitments, including access control, security, records, incident response and lifecycle management. Registration and independent assurance make that work visible; they do not perform it for the council. The model adapts established practice rather than departing from it: the capabilities described by DCAM and the key controls set out in CDMC are carried into the framework, but allocated across the loci rather than concentrated in a single organisation (Parts 1.2.1 and 3.3.1).

2.3 Constitutive, not behavioural

Enterprise data governance treats governance as behaviour: policies adopted, roles staffed, routines followed, adherence audited. That is the right model where governance is something an organisation builds for itself, against its own commercial purposes. It is not the model the regime adopts.

The regime treats governance as a property of the registered asset itself. The recorded description of the asset — what this paper calls, after the design materials, the Asset Boundary Profile — and the recorded governance terms are not records of governance performed elsewhere. They are conditions of the asset's existence as a registered composite. An asset that loses conformity does not merely breach internal policy; its register state, and the legal and commercial protections that flow from registration, are directly in question. Governance status is something the asset has, not something the foundation reports.

A counterparty can read the asset's registered description, accreditation status and supporting evidence, distinguishing declarations from independently assessed facts. Registration supplies the statutory property right; evidence and reliance have only the effects expressly assigned to them. Registration and assurance do not warrant data quality or create an automatic entitlement to compensation. Security registration and priority are later capabilities, as explained in Part 4.8.3.

The constitutive design also has implications for what the framework asks of foundations. Where governance is constitutive, it is not enough for the foundation to

assert that it is meeting requirements; the requirements must be met in a form the register can record and external assurance can verify. Where governance is behavioural, the foundation chooses its own evidence base; where governance is constitutive, the framework chooses it for the foundation, in the interest of every party who relies on the register.

2.4 Proportionality

The framework does not impose a single, maximalist set of requirements on every data asset foundation. Requirements scale with the asset's classification — its position on the two-axis matrix of Distribution Scope and Data Sensitivity — and with any applicable governance signals (commercial intent, AI-use, sectoral overlay and residency signals). A foundation holding a small, well-bounded, low sensitivity asset faces requirements proportionate to that asset. A foundation holding a large, broadly distributed, high sensitivity asset faces correspondingly heavier requirements.

The proportionality controls operate through several mechanisms. The classification of an asset, applied at registration, drives the mandatory minimums for governance, access controls, accreditation level and cycle, and supervisory attention. All asset classes require both Level 1 verification of registered information and Level 2 controls attestation for full registration; what classification varies is the depth of the attestation profile applied and the frequency of the refresh cycle. Sectoral overlays attach additional governance requirements where the nature of the data engages another regulatory regime — financial services, gambling, life sciences and others. The framework's standards making process allows the calibration of these levels and cycles to be refined as the regime matures, without primary legislation.

The Department recognises that proportionality is itself something on which consultation responses will be informative. A framework that is too permissive at the lower end will be read as undermining the credibility of registration as a governance signal; a framework that is too demanding at the lower end will deter the smaller foundations that the regime should be capable of accommodating. The Department's working calibration is set out in Part 4 (the lifecycle walkthrough) and in the supporting Standards.

It is not the framework's intention that proportionality operate as a self-disapplication route. Section 69 of the Act mandates minimum requirements; foundations are not at liberty to declare a requirement inapplicable to their own circumstances. Where a requirement does not apply on its face to a particular asset class — for example, requirements that engage only on the presence of personal data — the relevant Standard says so. The route to legitimate variation is the proportionality of the classification driven minimums, not unilateral disapplication.

2.5 Phased capability

The Verification Agent is a staged, Registrar-hosted capability and will not be available when the Register opens. At launch, AAP work and prescribed foundation evidence support the required checks. Initial automation will address integrity, existence and parameter checks to the extent supported by the inputs actually available; continuous semantic conformity is a later target. Metadata-only access cannot substantiate

content inspection or prove the absence of personal data. Each deployed check must identify its inputs, scope, observation time and limitations.

The framework is drafted so that no register state carries legal meaning that the capability of the day cannot support. Conditions the Verification Agent cannot yet verify automatically are attested by Accredited Assurance Providers, and migrate from attestation to automation as the agent's capability advances. The accreditation ladder (Part 3.5) is designed expressly to carry this migration: individual checks within Level 1 and Level 2 can move from AAP performance to Agent performance as the technical specification matures, without changing the register-facing meaning of the attestation. The result is a predictable path for the assurance market, and a regime that can advance technically without re-legislation.

The Department is open about the phasing. The first version of the regime is exactly that: a first version. The framework is built so that it can grow into its full technical form without confidence in the first version being misplaced. Phase one is what is being consulted on; the criteria for moving to phase two will be a matter for subsequent consideration as the technical specification develops.

2.6 Bounded commitment

The framework distinguishes between what should be committed in Regulations and what should be left to Standards and Guidance. Functions, recording mechanisms, the existence of roles and the legal effect of register state are committed in Regulations — they engage rights, duties and powers, and they should be slow to change. Thresholds, technical specifications, attestation profiles and cycles are matters for lawfully authorised Standards; Guidance explains them without creating obligations, where they can mature with the assurance market, with the development of the Verification Agent, and with the practice of classification, without requiring re-legislation each time.

This is more than an administrative convenience. The data and assurance landscape will move in the years after commencement of the regime, in ways that are not now fully predictable. A framework that hard-coded today's understanding of, for example, the right cycle for re-verification of a high-sensitivity asset would risk being wrong within two years. A framework that hard-coded a particular taxonomy of asset classes would invite boundary gaming as the assurance market and the classification practice developed. By contrast, a framework that locks in the existence of the requirement and the legal effect of compliance, while leaving the operational detail to standards updateable through a transparent process, can move with the practice without losing its statutory grip.

The standards making process by which Practice Directions and Standards are made, approved and revised is itself part of the framework. Without that process, every Standard would be exposed to a challenge that it had been made without proper authority. The process is set out in Part 3.1 and in the DGF Regulations. The Department's commitment is that bounded commitment in the Regulations is matched by transparent process at the standards tier.

Part 3: The architecture of the framework

This Part sets out the architecture of the Data Governance Framework: the family of instruments through which it operates, organised by tier and by the three categories introduced at Part 1.3; the roles by which the framework is discharged; the loci across which governance functions are distributed; the recorded description by which each data asset is fixed; and the accreditation ladder through which assurance is provided. Together these are the structural choices that give the principles in Part 2 their operational effect. Part 4 then walks through how the architecture works in practice across the lifecycle of a foundation and its assets.

3.1 The instrument family

The Data Governance Framework is not a single document. It is a body of subordinate legislation and supporting instruments, each carrying the content appropriate to its tier and organised into the three categories introduced at Part 1.3. Two organising cuts operate together: by tier, and by category.

By tier — how binding each instrument is. Three tiers are used.

Regulations carry the binding rules: enforceable duties, conferred powers, definitions of statutory terms, and anything giving effect to a delegating section of the Act. The Department makes the Regulations under section 92 of the Act, in discharge of the duty in section 69 to establish a data governance framework, and subject to the Tynwald procedure specified there. Section 69 requires the framework to set minimum requirements for data stewardship, including provision about technical, ethical and security standards in respect of data assets (section 69(a)), to specify the role of the Information Commissioner in relation to the supervision of data asset foundations in respect of their processing of personal data (section 69(b)), to set minimum requirements for data asset accreditation (section 69(c)), and to make provision about any other matter the Department considers necessary or expedient (section 69(d)). Regulations are the slowest layer of the framework to change: they engage rights, duties and powers, and amendments require the same process as the original making.

Practice Directions and Standards carry the operational and technical detail: forms, evidence formats, taxonomies, verification specifications, accreditation procedures. They are made by the Department under the standards making process set out in the Regulations, which provides for consultation with affected stakeholders, approval, publication, versioning and transitional savings on revision. Practice Directions and Standards are the responsive layer of the framework: they can be updated as the assurance market matures, as the Verification Agent develops, and as classification practice evolves, without re-legislation. The making instrument identifies the category of each new instrument.

Guide Notes carry the explanatory and interpretive content: worked examples, plain language summaries, joint guidance with the regulators where appropriate. They are not binding; they are aids to navigation and interpretation. The Department may issue Guide Notes at any time.

The boundary between the tiers is not arbitrary. The Department applies a consistent test in deciding where to place new content: if the content creates, alters or extinguishes a legal right, duty or power, it sits in Regulations; if it provides operational or technical content within an enabling power conferred by the Regulations, it sits in a Practice Direction or Standard; if it is purely explanatory, it sits in a Guide Note. The test is what allows the framework to commit firmly at the level that matters legally while remaining adaptable at the level that matters operationally.

By category — what each instrument does. Within the tiers, the substantive instruments are grouped into the three categories introduced at Part 1.3: (1) Obligations of the DAF Council; (2) Other Actors in the Ecosystem; and (3) Data Asset Boundary and Material Change. The DGF Regulations sit above these categories as the principal subordinate instrument, providing enabling powers and definitions that apply across the framework. The category into which an instrument is placed indicates its principal subject; it does not exclude relevant content from adjacent categories, and cross-references are made throughout the framework where content interlocks.

A complete index of DGF instruments — those made, those in draft, and those planned — is at Annex B, arranged by category. The headline instruments are introduced at 3.1.1 below.

3.1.1 Headline instruments

The framework is delivered through the following principal instruments, grouped by category. The list is not exhaustive; the full index at Annex B identifies further instruments dealing with specific obligation areas. Cross-references between instruments are given where content interlocks. The allocation of each concept shared with the Register white paper — the Asset Boundary Profile, classification, governance signals, accreditation and amendment — across these instruments is set out in the DAR–DGF Interface Schedule, published alongside this paper. This section remains subject to change.

Above the categories: the enabling instrument

Instrument	Tier	Content
DGF Regulations	Regulations	The principal subordinate instrument: definitions, outcome duties, scope of application, transitional and review provisions, enabling powers for the Standards and Practice Directions, and the standards-making process itself.

Category 1: Obligations of the DAF Council

The instruments that set out what the foundation itself must do in the conduct of its data-related affairs.

Instrument	Tier	Content
Practice Direction 1 — Obligations of the Data Asset Foundation	Practice Direction	Operational content of the foundation's residual duties and the foundation side discharge of its constitutive obligations. Read against the Verification and Accreditation Framework (Category 2) for accreditation duties, and against the Category 3 instruments for asset side obligations.
Access Control and Information Handling Standard	Standard	Access controls aligned to the Distribution Scope axis of classification; security duties protecting register integrity and reliance. Read against the Classification and Metadata Standard (Category 3) for the classification driving control requirements.
Records Retention Standard	Standard	The retention schedule for records of control maintained by the foundation. Read against the lifecycle content in the DAR Regulations (Category 3) for records associated with material change events.
Publication Matrix Standard	Standard	Reporting and publication thresholds; the form and content of the foundation's annual report to the Data Enforcer. Read against the Data Enforcer review standard (Category 2) for the receipt and use of reports.

Category 2: Other Actors in the Ecosystem

The instruments that set out the functions and conduct of the actors other than the foundation itself.

Instrument	Tier	Content
Verification and Accreditation Framework	Standard	The AAP scheme, accreditation criteria, attestation profiles, the accreditation ladder (including the mandatory Level 3 provision at 3.5.1), and the Verification Agent specification. Incorporates the Capability Model Standard applied by AAPs. Read against Practice Direction 1 (Category 1) for the foundation's accreditation duties.
Data Enforcer review standard	Standard	The Data Enforcer's functions, conduct, standing, and escalation pathways. Read against Practice Direction 1 (Category 1) for the foundation's cooperation duties.

Instrument	Tier	Content
Data Protection Interface Statement	Guide Note	Designed coexistence with data protection law; indicative controllership map; resolution pathways across the interface points identified at Part 5. Read against Practice Direction 1 (Category 1) for the foundation's controller side duties, and against the DAR Regulations (Category 3) for the data subject rights amendment ground.
Joint Guidance	Guide Note	Operational coordination between the Registrar and the regulators as appropriate; driven by the no double penalisation principle and greater clarity on the interaction with adjacent regimes.

Category 3: Data Asset Boundary and Material Change

The instruments that describe what a registered data asset is and how it changes over time.

Instrument	Tier	Content
Classification and Metadata Standard (Practice Direction) / Register Data Dictionary	Standard	The two-axis classification taxonomy; the field architecture of the register; the versioned data dictionary; the cells in which a Level 3 assessment is a condition of issue or renewal of the accreditation. Read against the Access Control Standard (Category 1) for controls driven by classification.
Asset Boundary and Material Change Standard [working title]	Standard	How each attribute of the Asset Boundary Profile, including the growth parameter declarations, is declared, and how a change to a registered asset is assessed against the categories in the DAR Regulations. Its proposed schema is in Annex A. Read against the Data Quality Standard for quality and material drift.
Data Quality Standard	Standard	Quality dimensions and metrics; fitness for purpose criteria; material drift definitions. The Asset Boundary Profile schema, including the growth parameter declarations, sits in the Asset Boundary and Material Change Standard. Read against the Verification and Accreditation Framework (Category 2) for the attestation of quality conformance.

Instrument	Tier	Content
Sector and Residency Overlay Standard	Standard	Operational rules for sectoral overlays (financial services, gambling, life sciences and others) and for residency overlays. Read against Practice Direction 1 (Category 1) for the foundation's compliance with applicable overlays.
DAR Regulations — amendment regime	Regulations	Not an instrument of this framework. The DAR Regulations are made under the Act and deal with the Register: the amendment grounds and processes, provisional and full registration, and disposal and reversion on removal. They are cross-referred from across the framework but are not adopted into it: register mechanics and legal effects sit with the DAR Regulations, and the substantive standard the asset and its foundation must meet sits with this framework.

Each instrument is read consistently with the others. Where this paper expresses a position that is to be given effect through a Standard or Practice Direction, the instrument is named at the relevant point. Where a position is to be given effect through the Regulations themselves, that is also identified.

3.2 The role architecture

The Act creates a deliberate, non-overlapping role architecture for the DAF ecosystem. Each role has a defined remit, with clear escalation pathways between them. The architecture is designed on the principle that every detectable non-conformity should have one role with the duty to respond first, one escalation actor, and one terminal venue for enforcement. The principle exists to avoid the diffusion of accountability that defeats governance in less structured arrangements, and it allows the regime to operate without a dedicated standing supervisor for data assets: supervision is distributed across the Enforcer, the assurance market, the Registrar's narrow register integrity remit and the competence of the existing regulators. This section addresses the roles established by the Act; the instruments giving those roles operational content are grouped in Category 1 (the council) and Category 2 (all others).

The roles, with the section of the Act establishing each:

Council of the data asset foundation (section 88). The fiduciary organ of the foundation and the home of every function requiring judgement. The council carries the foundation's statutory duties, makes strategic decisions within the foundation's objects, oversees access to and use of the asset, decides remediation in response to qualifications or alerts, and is collectively accountable for compliance with the framework. The Act requires at least two members of the council of a data asset foundation to meet qualification requirements set out in the framework (section 88(1));

the routes by which those qualifications may be met are addressed in the Qualification Routes Standard. Section 88(3) provides that the personal liability of council members for fraud, wilful misconduct or gross negligence cannot be relieved or excused by any instrument or contract. The council's operational duties are set out in Category 1 instruments.

Data Enforcer (sections 86 and 87). A specialised version of the existing foundations law enforcer, adapted to the data context. The data enforcer must review, at the prescribed intervals and against the prescribed scope, the council's conduct of the foundation's affairs relating to its data assets; and must act, on reasonable grounds, where a departure comes to its attention, whether through that review or otherwise. A data enforcer is not liable for failing to detect a matter that a review conducted in accordance with the prescribed scope and intervals would not have revealed. A data enforcer reviews conduct; it does not direct strategy, hold assets, or substitute its judgement for the council's within the recorded terms. The Enforcer is treated as a person with sufficient interest in respect of a data asset foundation for the purposes of the Act (section 86(8)). The Enforcer's functions are set out in the Data Enforcer review standard (Category 2).

Accredited Assurance Provider (section 84). An independent professional firm — a specialist data assessment provider — accredited by the Department to issue and renew data asset accreditations. The AAP attests the conditions that require professional judgement or site access: implementation of controls, conformity of use with declared purpose, provenance of derivation claims, and others. Accreditation status is recorded on the register as a register state under section 85(3), and not as a governance signal; its lapse, qualification, suspension or revocation is reflected in that state and engages the remediation pathway under section 85. A foundation must appoint an AAP and provide reasonable assistance for the AAP's performance of its functions (section 84(3)). The AAP scheme is set out in the Verification and Accreditation Framework (Category 2).

Data Asset Registrar (section 77). Appointed by the Department, with responsibility for register integrity: maintaining the register, recording amendments, verifying the integrity of new asset states following amendment, and recording asset accreditation status and related register-facing consequences. The Registrar does not adjudicate data protection compliance, does not manage assets and does not direct foundations; its remit is the register, and the register is the artefact through which governance is constituted. The Registrar's operations engage instruments across all three categories, with the amendment regime (Category 3) being the primary substantive interface. The registrar's remit is defined by object rather than by stage: it is the registrar of the data asset register, not of data asset foundations. Part 4.1 describes how the division operates at establishment and the single point at which the two interlock.

Verification Agent. A machine component, operating in trusted execution environments, that verifies asset state against the recorded description. The Verification Agent is not a statutory office; it is infrastructure deployed under the Verification and Accreditation Framework (Category 2), with its specification and operational rules sitting in the standards tier. Its outputs feed register state (where verification confirms continuing conformity) and the escalation pathway (where it does not). Capability is phased: phase

one performs basic integrity and existence verification; continuous semantic conformity is a phase two target (see Part 2.5).

Information Commissioner. The supervisor of data protection law in respect of personal data within registered data assets. The Commissioner's role, powers and independence are unchanged by the regime. The interface between the framework and the Commissioner's supervisory functions is addressed at Part 5 and in the Data Protection Interface Statement (Category 2).

3.2.1 Proposed allocation of functions across the roles

The table below sets out, for each of the principal governance functions, the role with primary responsibility and the roles with supporting or interface responsibilities. The allocation is non-overlapping in respect of primary responsibility: every function has exactly one role identified as primary, with other roles in supporting positions. The table is illustrative; the full detail sits in the relevant Standards, distributed across Categories 1 and 2.

Function	Council	Enforcer	AAP	Registrar	Agent	ICO
Asset strategy within objects	Decides	Oversees conformity with terms	—	—	—	—
Defining and amending the asset description (ABP)	Proposes / approves	May challenge non-conforming change	Attests basis where required	Records; verifies integrity of new state	Verifies continuity of state	—
Classification (two-axis)	Applies at registration	Reviews accuracy at the prescribed intervals	Attests in higher-sensitivity cases	Validates completeness at registration	Flags drift signals	—
Access, entitlements, purpose of use	Grants within wrapper terms	Reviews grants at the prescribed intervals	Attests purpose conformity	—	Logs where in scope	Supervises lawful basis (personal data)
Security and integrity controls	Implements (via providers)	Reports known deficiencies	Attests implementation	Receives attestation status	Verifies integrity vs ABP	—
Data subject rights (incl. Art. 17)	Gives effect as controller	Verifies effect given	—	Records Tier 2 amendment; verifies new asset state	Confirms erased state conformity (later stage)	Supervises and issues guidance
Lifecycle: retention, archiving, destruction	Executes per schedule	Confirms execution	Attests defensible destruction where required	Records material change	Verifies state transitions (later stage)	Supervises personal data aspects
Breach or non-conformity response	Remediates	First escalation point	Re-attestation post-remediation	Receives notifications and information; records the consequence	Signal downgrade	Notified where personal data engaged

Function	Council	Enforcer	AAP	Registrar	Agent	ICO
Ethics of access, use, outcomes	Decides; owns judgement	Reviews against wrapper purpose limits	—	—	—	Relevant where overlapping with data protection principles

The pattern visible in the table is the regime's structural answer to self-certification: any function the council itself performs is, where possible, evidenced by a body other than the council. Strategy decisions are the council's; their conformity with the recorded governance terms is independently monitored. Access grants are the council's; their conformity with the wrapper is monitored by the Enforcer and attested by the AAP. The judgement remains where it must — with the organs of the foundation — but the evidence base does not depend on the foundation's own assertion.

3.2.2 Bodies outside the statutory role architecture

Two categories of body have a bearing on the operation of the framework without forming part of the statutory role architecture. External standards bodies — including the EDM Association as owner of the DCAM and CDMC schemes, ISO, and the owners of other schemes on the Recognised Standards list — own and administer the assessment schemes that may satisfy a Level 3 requirement. Additionally, Authorised Partners licensed by the EDM Association conduct assessments under the accreditation framework. Neither has a function under the Act, and neither is subject to direction by the Department; their position in the regime arises from the Department's recognition of their schemes, which is a decision of the Department and is revisable through the standards making process. The recognition mechanism is set out at Part 6.

3.3 The seven loci of governance

The role architecture explains who does what. The locus model explains where the doing happens — that is, which mechanism gives each governance function its effect. The model is the operational expression of the distributed governance principle introduced at Part 2.2, and it is orthogonal to the three category grouping: any category may draw content from any locus, and locus allocation is a design property of specific functions rather than of instruments as a whole.

Seven loci are identified, in descending order of bindingness:

Locus	Name and mechanism	How it works in the regime
L1	Normative — the Act, the DGF Regulations, the Standards	Binding rules of general application: what every data asset foundation must do, and the minimums below which no foundation may go. The legislative and regulatory floor.

Locus	Name and mechanism	How it works in the regime
L2	Entity embedded — foundation instrument and rules, council, Data Enforcer	Governance encoded in the constitutive documents of the foundation and discharged as legal duties of its organs. Travels with the entity, survives personnel change, and is reviewed by the Enforcer.
L3	Register embedded — the Data Asset Register entry as the authoritative description of the asset	The Register records asset identity and governance commitments with the effects assigned by the Act and operative instruments. Declaration, independently assessed fact and statutory status remain distinct; the entry does not itself prove that operating controls are effective.
L4	Automated — the Verification Agent	Machine performed verification of mechanically checkable conditions, to the capability of the deployed agent. The output feeds register state and the escalation pathway; the Agent does not exercise judgement.
L5	Attested — the Accredited Assurance Provider scheme	Independent professional assurance of conditions that require judgement or site access. Attestations are recorded on the register; false attestation engages professional and statutory consequences.
L6	Continued monitoring — Registrar, Information Commissioner, courts	Supervisory bodies and venues that detect departures the other loci surface. Institutional separation is preserved: the Registrar oversees register integrity; the Commissioner oversees data protection, the courts enforce.
L7	Residual organisational — the foundation's own operational layer	Council directed operational data management, performed by the foundation or its appointed providers. Includes access control, security, records, incident response, lifecycle management and the council's strategic, ethical and remediation decisions.

The model rests on a design rule: each governance function is allocated to the lowest numbered locus at which it becomes self-executing or independently verifiable, and no lower. Constitutive (L3) is preferred to automated (L4); automated is preferred to attested (L5); attested is preferred to organisational (L7) — but only where the function is genuinely rule shaped. Forcing judgement-shaped functions (strategy, ethics, remediation decisions) into rules produces brittle rules and fictitious compliance. The rule operates as a discipline at the design stage; it does not constrain the council's ability to discharge its own judgement-laden duties at L7.

The framework supplies a common catalogue, classification, rules, assurance record and escalation structure. The foundation remains responsible for the operational controls beneath those records. The register, automated checks and professional assurance provide evidence of defined matters; none substitutes for the council and its providers operating the required controls.

The locus model therefore separates the setting and recording of requirements, their operational performance, and assurance over that performance.

The council retains accountability for the foundation's continuing compliance, including where it delegates operational tasks to service providers. The assurance record states what was assessed, when and with what limitations.

3.3.1 DCAM and CDMC in the locus model

DCAM and CDMC are both written for an organisation governing its own data: DCAM assesses whether the organisation has the capabilities to do so, and CDMC specifies the key controls it should operate. The locus model takes the substance of both and reallocates it. A function that an enterprise would discharge through its own data office is allocated, under the design rule above, to the locus best placed to carry it: often the register itself, sometimes the Verification Agent or an Accredited Assurance Provider, and only residually the foundation's operational layer.

The Department has mapped each of the capabilities in DCAM and CDMC against the framework, asking of each whether it bears on the foundation or on the asset, whether the regime can supply it in standard form, and whether it can be verified automatically. Those questions correspond closely to the locus model: what the regime supplies in standard form sits at L1 and L3, what can be verified automatically at L4, what bears on the asset at L5, and what bears on the foundation at L7 and, as a whole, at Level 3.

The object of assurance shifts from the organisation to the asset. Functions are distributed: where a function is rule shaped, what an enterprise framework expects the organisation to do for itself is done here by the register/registrar, the Verification Agent or an independent provider. And in some instances the governance becomes constitutive: a control that DCAM or CDMC expects an organisation to evidence becomes, here, a condition of the asset's registered existence. Where none of the reasons for the loci applies, the framework follows DCAM and CDMC as closely as it can, so that a foundation, a provider or a counterparty familiar with either will recognise what is being asked.

3.4 The Asset Boundary Profile and two-axis classification

Every registered data asset is described by an Asset Boundary Profile (ABP). The ABP is the recorded description that fixes what the asset is and how it is to be governed. It is the artefact at the centre of the register entry, and it is the reference point against which conformity is assessed: by the Verification Agent (state continuity), by the AAP (correspondence with reality, controls implementation), by the Data Enforcer (council conduct), and by the Registrar (recording and integrity of amendments). The instruments defining the ABP and the classification that attaches to it sit in Category 3.

The ABP comprises seven identity defining fields: definitional scope, temporal scope, provenance scope, classification coordinates, derivation rule, governance status and identity-preserving change envelope. The DAR Regulations will establish this legal allocation; the Asset Boundary and Material Change Standard [working title] will specify the permitted declarations and technical detail within that authority, with the proposed schema in Annex A. The Register Data Dictionary and DAR Field List specify register representation and are versioned with the Standard as a coordinated release. Neither the schema nor the Dictionary can override the Act or Regulations. Four matters sit outside the ABP: governance signals; accreditation status; fitness for purpose criteria; and integrity and verification method metadata. Asset-side canonicalisation and integrity methods are declared and recorded separately from the Registrar's technical algorithms and infrastructure. Changes to evidence metadata or governance signals remain recorded and assured where required, even where no ABP amendment results. A cryptographic commitment evidences a represented state; a changed commitment does not of itself create a different legal asset.

3.4.1 The two-axis classification

The classification of a data asset is applied at registration and reviewed continuously. The framework uses a two-axis classification matrix as the mandated taxonomy. The axes are Distribution Scope and Data Sensitivity.

Distribution Scope describes the range of parties who have, or may have, access to the asset under the recorded governance terms. The axis has four classes, which are the canonical labels and codes used throughout the regime: I — Internal, where the asset is restricted to the foundation itself; C — Controlled-Share, where it is shared with a defined, contracted set of external partners each of whom the foundation can identify; F — Federated, where it is pooled within a formal multi-party consortium, data trust or federated research arrangement; and D — Distributed, where it is made available under licence on defined terms or openly available. The scope is a property of the recorded governance terms; it is not affected by the technical means of distribution chosen by the foundation.

Data Sensitivity describes the data protection status of the data within the asset: whether and how personal data is present, and the nature of any special category personal data. The scale runs from assets containing no personal data — data that was never personal, or data established to be anonymous in its relevant context, including synthetic data only where that conclusion is supported — through pseudonymised and aggregated personal data, to identifiable personal data including special categories. The axis is drawn by reference to data protection law rather than independently of it, so that the boundary between its levels moves with that law and neither this framework nor the DAR Regulations restates the test.

The axis therefore describes what the asset contains. It does not describe how sensitive the asset is in a commercial or operational sense. Operational sensitivity is real and it does bear on the assurance an asset should carry, but it is a function of the sector and context in which the asset sits rather than of the data protection status of its contents, and the framework already has an instrument for it: the sectoral overlay signal described at 3.4.2, which triggers the operational rules set out in the Sector and Residency Overlay Standard (Category 3). An asset containing no personal data but relating to critical

national infrastructure is Data Sensitivity level 1 and carries the critical infrastructure overlay; the overlay, not the axis, is what raises its assurance requirement.

The classification a foundation applies determines the mandatory minimums for governance: the attestation profile applied and the accreditation cycle, the access controls expected, the records of control to be maintained, and the supervisory attention the asset will receive. Levels 1 and 2 are required for full registration of every asset, because together they constitute the data asset accreditation; what classification determines is the depth at which each is performed and how often it is refreshed. Assets in the highest cells attract a mandatory Level 3 assessment as an additional accreditation condition (see 3.5.1). The exact taxonomy on each axis, the points at which classification thresholds are crossed, and the consequences of each class are matters for the Classification and Metadata Standard.

The classification scheme is mandated by the framework. It is not for each foundation to design or vary. This is deliberate: a register on which each foundation invented its own classification would be a register on which counterparties could not rely.

3.4.2 Governance signals

The two axes are supplemented by a set of governance signals — recorded attributes on the register that convey particular governance properties of the asset, additional to its classification. Four categories of signal are envisaged at commencement, corresponding to the Commercial Intent, AI Use Tier, Regulated Sector and Residency Tier attributes described in the Register white paper:

Sectoral overlay signals indicate where the nature of the data engages a sectoral regulatory regime — financial services (Financial Services Authority), gambling (Gambling Supervision Commission), life sciences, and others. An overlay signal triggers operational rules set out in the Sector and Residency Overlay Standard (Category 3).

Residency overlay signals indicate cross-border data flow constraints — sovereignty requirements, hosting location commitments, or destination restrictions imposed by the dedication instrument or by the governance terms. Personal data movement remains additionally subject to the requirements of the Applied GDPR.

AI-use signals indicate the permitted or prohibited use of the asset in the training or operation of artificial intelligence systems. The control consequences attached to AI tiers are specified in the AI-Use Tier Governance Standard, are kept light and principles based at commencement pending the Department's wider AI strategy, and may be phased; the descriptive examples given in the Register white paper do not independently create minimum requirements.

Commercial intent signals indicate the basis on which the asset is exploited, from public good and internal pre-commercial use through active commercialisation to marketplace trading. The signal describes how the asset is used rather than what it contains; it is declared by the council and maintained through the amendment regime. Accreditation status is not a governance signal. The level, scope, assessor, date and expiry of a current accreditation are recorded in the attestation record described at 6.3.2, and the validity of the accreditation is a register state recorded by the registrar under section 85(3). The distinction is developed at 4.6.1 and 6.4.5 and it matters: the attestation record

describes the depth of assurance behind an asset, while register standing determines whether it may be utilised at all.

Further signal categories may be added through the standards-making process as the regime matures. The Department's preference is to keep the signal set small and stable enough that counterparties can read the register confidently, while leaving room for evolution where the practice clearly requires it.

3.5 The accreditation ladder

Neither the registrar nor the register warrants or independently validates data quality. Where this framework requires quality controls or fitness for purpose criteria, conformity is assessed through the applicable assurance process and the resulting assurance state is recorded on the register. Accreditation is the framework's transparency instrument. It is a graduated set of assurance products, the results of which are recorded against the register entry as the attestation record, so that the depth of verification behind any asset is visible to its market. Four levels are used. Levels 1 and 2 together constitute the statutory data asset accreditation; Level 0 denotes provisional registration under section 79, with no accreditation, independent assurance claim or section 80(4) property right, and Level 3 is a recognised external capability assessment. The full ladder, with its criteria, profiles and cycles, is set out at Part 6.3 and in the Verification and Accreditation Framework (Category 2); it is not repeated here.

Level	What is verified	Register effect
Level 0 — Provisional Registration	Registrar validation of completeness and formal integrity of the application through the staged registration process. Carries no assurance claim about correspondence to reality.	"Provisionally registered" status. Not an accreditation and not to be presented as one.
Level 1 — Registered Information Verification	An AAP confirms that the registered information corresponds to reality: the asset exists; the boundary is as described in the ABP; the classification is accurate; custody and hosting arrangements are as declared.	Level 1 evidence is recorded with its scope, assessor, date, accepted currency and limitations. Levels 1 and 2 support one accreditation with one expiry; evidence changes are handled under Part 6.4.
Level 2 — Controls Attestation	Implementation of controls proportionate to classification, plus conformity of actual use with the declared purpose in the governance wrapper. Scope is drawn from the applicable attestation profile.	Controls entry in the attestation record, including the profile applied and any qualifications.

Level	What is verified	Register effect
Level 3 — Recognised External Assessment	Full data management capability assessment under a recognised approved scheme (such as Data Management Capability Assessment Model (DCAM) or Cloud Data Management Capabilities (CDMC) by EDM Association) of the foundation and its operating arrangements.	External assessment entry in the attestation record, naming the scheme, version and assessor. Mandatory for assets in the highest cells of the two-axis classification matrix; optional and market-driven elsewhere. Treated further at Part 6.

Levels 1 and 2 constitute the assurance components of the data asset accreditation and are sufficient for full registration of an asset under section 80 of the Act. For designated asset classes, the framework additionally requires evidence of a current recognised Level 3 external assessment before an AAP may issue or renew the statutory accreditation. Level 0 is the provisional registration that precedes full registration: it carries no assurance claim and is not to be presented as accredited status.

3.5.1 Mandatory Level 3 in the highest classification cells

The Department's position is that, for the small number of asset profiles where the combination of broad distribution and high data sensitivity creates the highest risk, the regulatory minimum should include independent assessment of the foundation's data management capability as a whole, not only attestation of the asset's controls and purpose conformity. For these profiles, a Level 3 assessment under a recognised approved scheme (DCAM or CDMC) is therefore required, in addition to Levels 1 and 2, as a condition of full registration.

Two design choices are reflected in this position. The first is that the trigger for mandatory Level 3 is the constitutive classification of the asset itself. The Department has considered, and rejected, the alternative of defining a separate “high-risk category” concept alongside the two-axis matrix: such a concept would have to be defined, maintained and consistently applied alongside the existing classification, and would invite definitional disputes that the classification system is designed to settle. By making the trigger mechanical and visible — the asset's position on the matrix, recorded on the register at provisional registration — the obligation is predictable from the moment of dedication, and the framework does not carry a parallel taxonomy.

The second is that the precise cells of the matrix that trigger Level 3 mandation are set in the Classification and Metadata Standard (Category 3) rather than in this paper. The Department's working position is that mandation should attach on two limbs: to the cells in which broadly distributed assets contain identifiable special category personal data, and to assets carrying a sectoral overlay signal designated for that purpose in the Sector and Residency Overlay Standard at or above a specified distribution scope. The second limb is how operational sensitivity enters the mandate, for the reasons given at 3.4.1. The Department is consulting on both the principle of mandation and the threshold.

The implications for foundations are practical. A foundation considering dedication of an asset whose classification would fall in the mandated cells will need to plan, at the

establishment stage, for an external assessment in addition to AAP attestation. Recognised schemes (DCAM and CDMC in the initial phase and any others as they become approved) are administered by their respective scheme owners; the assessment is conducted by an Authorised Partner of the scheme — which, where the AAP holds the necessary licence, may be the same firm that conducts the Level 1 and 2 work.

3.5.2 Design features of the ladder

Two design features of the ladder warrant comment in this Part.

The naming discipline matters. Level 1 is a verification of registered information; it is not an attestation of controls, and is not to be presented as one. If a counterparty could read "accredited" on the register and assume Level 2 substance, or Level 2 and assume Level 3, the transparency mechanism would become a misrepresentation vector. The signal vocabulary, and any public facing rendering of it, must make the level impossible to miss. The Verification and Accreditation Framework sets out the naming and presentation conventions to be observed.

The ladder is built to carry the Verification Agent's phased capability. Items within Levels 1 and 2 are specified so that they can migrate from AAP performance to Verification Agent performance as the Agent's specification advances. An item performed by the Agent ceases to consume attestation effort but continues to feed the same signal. The register-facing meaning of the level is stable while its production cost falls. This progression is consistent with the direction of industry practice, and in particular with CDMC's emphasis on automating key controls wherever they can be evidenced by machine: judgement items (purpose conformity, custody adequacy, certain provenance claims) remain attested indefinitely; mechanically checkable items move to automation as capability allows. Level 3 sits outside this migration: it is a capability assessment of the foundation, not a check of the asset, and is not subject to automation.

3.5.3 Three modulators

Three modulators govern how accreditation requirements vary in practice.

Classification and applicable governance signals drive the mandatory assurance profile and refresh requirements. Levels 1 and 2 are required for every full registration. The Level 3 mandate applies to designated profiles as described at 3.5.1; other legal obligations continue to apply independently of classification.

Asset class drives the content of attestation profiles, not the existence of obligations. The nature of the asset — personal data bearing, financial records, telemetry, AI training corpora — determines what a Level 1 or 2 engagement actually checks. Profiles live in the standards tier, derivable from ABP content, so that they can mature without re-legislation.

Purpose drives product profiles. The declared use in the governance wrapper supports purpose specific attestation products — most immediately a collateral grade profile for assets used as security in lending arrangements. This converts the foundation as custodian role from an asserted feature into a verifiable, register marked one.

The ladder is the connecting tissue between the architecture (the register, the role allocations, the locus model) and the market on which the regime depends. It is what makes the framework's distinctive claim — that registration is a substantive governance signal, not a bare administrative fact — operationally true.

Part 4: How the framework works in practice

Parts 2 and 3 described the architecture of the framework: the distributed model, the instruments through which it is delivered, the roles that operate it, and the classification and accreditation machinery that makes governance visible on the register. This Part walks through the life of a data asset from the establishment of the foundation that will hold it to the eventual removal of the asset from the register, showing at each stage which obligations attach, which actor carries them, and which instrument supplies the detail. It is written for the reader who wants to understand what participation in the regime actually involves, rather than how the regime is constructed.

The walkthrough follows the lifecycle the Act itself defines. Nothing in this Part creates obligations: every requirement described here is anchored in the Act, the Regulations or a named framework instrument, and where this Part simplifies for readability, the instrument prevails. Where the Department is describing a proposal rather than a settled position, this Part says so.

The three categories introduced in Part 1 provide the navigation. Obligations of the DAF Council dominate the stages at which the foundation is acting — establishment, utilisation, remediation. The instruments in Other Actors in the Ecosystem govern the actors the foundation deals with at each stage — the Registrar, the Accredited Assurance Provider (AAP), the Data Enforcer. The instruments in Data Asset Boundary and Material Change carry the stages at which the asset itself is defined or redefined — dedication, registration, amendment, and removal. The table below shows the correspondence; cross-references are given through the text where the categories interlock.

Lifecycle stage	Statutory anchor	Primary instrument category
Establishment	s.68, s.88	Obligations of the DAF Council (with the Qualification Routes Standard); Other Actors for the appointments the foundation must make.
Dedication and provisional registration	ss.76, 78, 79	Data Asset Boundary and Material Change (dedication instrument, Asset Boundary Profile, classification).
Full registration	s.80	Data Asset Boundary and Material Change, with Other Actors supplying the AAP accreditation machinery.
Utilisation	s.85(1), s.88(2)	Obligations of the DAF Council (the continuing duties under the governance wrapper).
Material change	s.83	Data Asset Boundary and Material Change (Tier 2 amendment grounds and process).

Lifecycle stage	Statutory anchor	Primary instrument category
Remediation	s.85	Obligations of the DAF Council, with Other Actors governing the Registrar and AAP steps.
Reversion or removal	s.81	Data Asset Boundary and Material Change.

4.1 Establishing a data asset foundation

A data asset foundation begins life as an ordinary Isle of Man foundation under the Foundations Act 2011, to which the Act attaches additional requirements. Under section 68, the foundation instrument must declare the foundation to be a data asset foundation, and its objects must relate to the utilisation of its data assets. The declaration signed by the class 4 licenceholder on establishment must state both matters. A foundation that is not a data asset foundation cannot hold data assets: section 68(4) provides that a purported dedication of a data asset to any other foundation is void. The name of the foundation must end in the words "Data Asset Foundation" or "DAF" (section 71), so that the foundation's status is apparent on its face to anyone dealing with it.

The additional requirements that make a foundation a data asset foundation in substance, rather than merely in name, are set out in this framework. At establishment the founder should have four matters in hand.

Council composition. Section 88(1) requires the council of a data asset foundation to have at least two members who meet the qualification requirements set out in this framework. The routes by which the qualification requirements may be met — professional qualification, recognised certification, demonstrated experience, or completion of a recognised course — are set out in the Qualification Routes Standard, which is designed so that the requirement can be satisfied through more than one pathway and does not create an artificial bottleneck in the supply of qualified council members. The foundation rules must also include the information required by this framework (section 73), and must set out the council's responsibilities in relation to the section 88 requirements (section 75).

Registered Agent. As with any Isle of Man foundation, a class 4 licenceholder must be appointed as Registered Agent. The Act strengthens this requirement for all foundations: failure to have a Registered Agent appointed in accordance with the 2011 Act is an offence, and a structured resignation process ensures that a foundation is not left without one inadvertently: not less than eight weeks' written notice to the foundation and to the Registrar (section 28A(2)(a)), a copy filed within one week (section 28A(4)), and the resignation effective only on entry of the final notice in the register (section 28A(6)). Where a registered agent resigns during a period of remediation, the eight weeks runs alongside the remediation clock and the council should plan the replacement accordingly.

Data Enforcer. Every data asset foundation must appoint a Data Enforcer (section 86(1)). The Data Enforcer is the regime's independent review presence within the foundation's

own governance: it reviews the council's conduct against the foundation instrument and the recorded governance terms, at the prescribed intervals and against the prescribed scope, and is the first escalation point when matters are not resolved by the council. The criteria the Data Enforcer must meet, and the functions it performs, are set out in this framework; the Data Enforcer review standard supplies the operational detail. The council must cooperate with and provide reasonable assistance to the Data Enforcer (section 86(4)).

Accredited Assurance Provider. The foundation must appoint an AAP to issue and renew data asset accreditation (section 84(3)). Assurance providers are accredited by the Department, which must be satisfied that the provider meets the criteria and qualifications prescribed in the Regulations (section 84(1) and (2)); the Regulations also establish the public register of accredited providers from which founders (and/or the council) can identify them. The appointment need not be in place at establishment, but it must be in place before full registration of any asset can complete, and in practice a founder will want the provider engaged early, because the provider's Level 1 verification work is performed against the registered particulars the founder (or a dedicator) is preparing. Part 6 describes the provider market, the independence requirements applying to appointments, and what happens to a foundation's attestations if its provider changes or withdraws.

None of this is novel machinery for the Island's professional services sector. The establishment stage of a data asset foundation resembles the establishment of any governed vehicle — a regulated fund, a licensed trust structure — in which the constitutive documents, the governing body and the appointed officers must be settled before the vehicle can take on the assets it exists to hold. What is distinctive is what comes next: the asset itself passes through a registration process that no conventional asset class requires, because the data asset register is what makes the asset.

Two registers are engaged across the lifecycle, and the division between them is by object. Entity requirements sit with the central Registry: the declaration that the foundation is a data asset foundation, the name requirement under section 71 and the objects requirement under section 72 are checked by the Registry on establishment, in the ordinary course of the establishment filing. Asset requirements sit with the data asset register: the data asset registrar's remit begins at the application for registration of an asset under section 78 and runs through the amendment, remediation and removal machinery described in the rest of this Part. The division is not quite watertight, and deliberately so. A foundation is a data asset foundation only if, among other things, it meets the additional requirements for data asset foundations set out in this framework and otherwise in regulations (section 68(1)(c)). Compliance with the framework is therefore constitutive of data asset foundation status, not merely a standard of conduct within it, and section 68(5) attaches an asset consequence to a failure that is not remedied within the period the registrar specifies. That is the route by which a framework failure serious enough to put the entity's character in question reaches the assets, and it is discussed further at 7.1. A founder whose declaration or objects are defective will therefore be caught at establishment, before any asset is dedicated. The two responsibilities meet at one point only: where a foundation ceases to meet the section 68 requirements and does not remedy the failure within the period the data asset registrar specifies by notice, the data asset registrar may remove that foundation's data assets from the data asset register (section 68(5)) — an entity failure

with an asset consequence, applied by the registrar of the register on which the consequence falls.

4.2 Dedicating and registering a data asset

Data becomes a data asset through dedication and registration. The two steps are distinct and the distinction matters. Dedication is the act by which the dedicator transfers or grants to the foundation the rights and permissions pertaining to the data (section 67). Registration is the act by which the register records the resulting asset and, on completion, constitutes the property right in it. Dedication without registration confers no registered status; registration cannot proceed without an executed dedication.

4.2.1 The dedication instrument

Section 76 requires the dedication to be recorded in a data asset dedication instrument in the form prescribed by the Regulations. The instrument is executed by the dedicator or founder and accepted by the council. Its required content is worth setting out in full, because the instrument is where the most consequential drafting decisions in the life of the asset are made. It must describe the dedicated data sufficiently to support the registration application; describe the nature of the rights and permissions the foundation holds in the data; identify any restrictions, limitations or conditions on those rights, including rights reserved to the founder or dedicator; and confirm the reversion position — that the data and all rights in it revert to the dedicator if there is no data asset accreditation or if the foundation fails to complete registration (section 76(2)(f)).

The description of rights transferred must identify reserved rights and third-party interests clearly. The dedication form will implement the statutory requirements and the intended lifecycle treatment: initial failure to complete registration must be distinguished from subsequent accreditation lapse, during which section 85 preserves the registered property right while remediation proceeds. The Department's drafting baseline is that lawful custody, preservation and remediation remain possible during all relevant prohibited-use periods, without premature reversion defeating the cure process. The interaction of section 76(2)(f) with sections 81 and 85 and the enabling route for that treatment are being referred to the Attorney General's Chambers. This is the policy basis for drafting, not confirmation that the legal construction has been approved; see 6.4.3.

4.2.2 Application and provisional registration

The council applies to the data asset registrar under section 78, providing the prescribed particulars, the executed dedication instrument and the prescribed fee. The particulars include the Asset Boundary Profile (ABP) — the structured description of the asset introduced in Part 3 — and the asset's classification under the two-axis matrix (Distribution Scope × Data Sensitivity), applied by the council at registration. Where the asset bears governance signals at admission — commercial intent, AI-use, sectoral overlay and residency signals — these are declared in the application.

If the registrar is satisfied that the application has been properly made, it must accept it, and the asset is recorded on the register as “provisionally registered” (section 79). Provisional registration is a genuine register status but a deliberately modest one: it

confirms that a complete and formally valid application exists, and nothing more. It corresponds to Level 0 on the assurance ladder described in Part 6.3, carries no assurance claim about correspondence to reality, and is never to be presented as an accreditation. The registrar may at this stage notify the council of outstanding requirements that must be met before full registration.

For personal data bearing assets, one point cannot be stated too often and is developed fully in Part 5: neither dedication nor registration confers a lawful basis for processing. The foundation is a controller under the Applied GDPR in the ordinary way, and every processing purpose in the foundation's objects must rest independently on a lawful basis. The classification applied at registration drives data protection touchpoints constitutively — high-sensitivity classes carry data protection impact assessment expectations at the point of establishment rather than after it.

4.3 Full registration and the property right

4.3.1 Completing registration

Provisional registration opens a window within which the council must complete registration (section 80). Completion requires the council, within the period prescribed by the Regulations, to submit confirmation of a data asset accreditation issued by the foundation's appointed AAP, and to meet any outstanding requirements notified by the registrar at the provisional stage.

The Act speaks of a single "data asset accreditation" (section 67). The assurance ladder in Part 6 supplies its content: Levels 1 and 2 together constitute that accreditation. Level 1 is verification that the registered information corresponds to reality — that the asset exists, that its boundary is as the ABP describes it, that the classification is accurate, and that custody and hosting are as declared. Level 2 is attestation of the implementation of the controls proportionate to the asset's classification that are set at standards tier — referred to throughout this paper as the DAR Code controls — and of the conformity of actual use with the declared purpose. Neither is sufficient alone. They support one accreditation identifier, scope and expiry date. Their evidence may have different assessment dates, but the AAP must ensure it remains adequate for the accreditation period; neither component is independently valid as an accreditation. A pending renewal does not extend the stated expiry.

For assets whose classification falls within the mandated cells of the matrix, a current Level 3 recognised external assessment is additionally required, and the accreditation expiry must not extend beyond that assessment's accepted currency. The mandate binds through the accreditation criteria rather than as a separate duty: the framework's minimum requirements for data asset accreditation under section 69(c) will include the Level 3 assessment for those assets, so that a provider cannot be satisfied for the purposes of section 84(4) without it. For all other assets Level 3 remains a market instrument, with the Department's recommendation for the initial cohort described at Part 6.6.

If the registrar is satisfied that the requirements are met, the asset is recorded as "fully registered". If the registrar is not satisfied, the provisional registration is removed and the registration process is void (section 80(3)) — at which point the reversion confirmation in the dedication instrument operates and the dedicator's rights are

restored. The staged process is deliberate: it lets the register accept an application quickly, exposes the asset's intended particulars to verification while the asset is not yet constituted, and reserves the constitutive step for the point at which verification and attestation are in place.

4.3.2 What the property right is

On full registration, a personal property right in the data asset vests in the foundation (section 80(4)), notwithstanding that the asset may be neither a thing in possession nor a thing in action. This is the provision on which the regime's commercial utility rests, and it is worth being precise about what it does and does not do.

The right is constitutive: it is created by registration and exists because of registration, not because the common law has been persuaded to recognise a new category of property. The object of the right is the composite asset — the data together with its governance wrapper — as recorded on the register. The right is extinguished when the asset is removed from the register (section 81(8)). It follows that the register is not a record of ownership established elsewhere; it is the source of the ownership it records. The practical consequences run through the rest of the lifecycle: an unregistered copy of the data is not the asset, and dealings in the asset are dealings in the registered composite.

Equally important is what the right does not do. It does not confer ownership of personal data as such, and no right of a data subject is assigned, waived or diminished by registration — the position is developed in Part 5 and in the Data Protection Interface Statement. It does not override third-party intellectual property or contractual rights in the underlying data: the dedication instrument must identify those interests, and the asset the foundation owns is the bundle of rights actually dedicated, no more. And it does not, of itself, supply a remedy against a third party who uses the asset without authority; that is the subject of the proposal described at 4.4.

4.3.3 Interoperability with other registers: the position at launch

Section 82 allows the Department, by Regulations, to specify a register established under the law of another jurisdiction as an equivalent data register, so that assets registered there may be admitted here without repeating the accreditation process. The Department does not propose to bring that mechanism into use at launch. Equivalence is a judgement about another jurisdiction's entire assurance architecture — its establishing law, the accreditation required before registration, the functioning of its registrar, the information its register makes available and the oversight applied to it (section 82(4)) — and there is at present no comparable register against which that judgement falls to be made. The regime launches with the domestic register only, and every asset enters through the accreditation pathway described at 4.3.1.

The interoperability instrument the Department does propose to develop, for phase two, is the data asset passport. It packages this register's assurance for verification elsewhere and it is described at Part 6.9 and is not set out again here.

4.4 Utilisation under the governance wrapper

Once fully registered, the asset may be utilised — held, managed, processed, exploited, licensed, disclosed or otherwise used in furtherance of the foundation's objects (section 67). Utilisation is subject to two continuing conditions: there must be a valid data asset accreditation in respect of the asset at all times (section 85(1)), and use must remain within the terms of the recorded governance wrapper. A third constraint is in development. The Department is designing a framework identifying utilisations that may not be carried on in respect of a registered data asset, and utilisations permitted only where prescribed conditions are satisfied, to be given effect through the DAR Regulations and, where a sectoral regime is engaged, in coordination with the regulator responsible for it. The design is not settled and is not described further here. Two points are settled: compliance will be declared and attested rather than supervised, and the consequences of a prohibited utilisation will attach to the register entry rather than take the form of a determination by the registrar as to the lawfulness of the underlying conduct.

The governance wrapper is the operative concept of this stage. It is the set of governance terms recorded against the asset: the purposes for which the asset may be used; the entitlements the council may grant and the conditions attaching to them; derivation and sub-licensing rights; provenance obligations; lifecycle terms including retention and destruction; and the security and hosting commitments proportionate to classification. The wrapper travels with the asset. A counterparty taking a licence, a lender taking security, or an escrow agent taking custody deals with the asset on the wrapper's terms, and can read those terms — through the register's governance signals and attestation record — without conducting its own governance due diligence from a standing start.

Within the wrapper, decisions belong to the council. The council grants access, sets commercial terms, manages service providers and exercises the judgement the framework deliberately leaves with the foundation's fiduciary organ — the residual layer described in Part 2. The council's continuing duties under section 88(2) frame this stage: all activity involving the asset must directly support the foundation's objects; the foundation must comply with this framework; and the council must oversee effective access control mechanisms for the asset. The obligations are Category 1 territory — Obligations of the DAF Council — and Practice Direction 1 is the instrument that operationalises them.

4.4.1 Use outside the wrapper

Use of the asset without a grant under the wrapper, or in excess of one, is a contravention of this framework by the foundation that permits it, and, where a licence is in place, a breach of that licence by the party that exceeds it. Those consequences follow from the framework and from contract, and they are available on day one.

The Department's further intention is that unauthorised use of a registered data asset should be actionable by the foundation against the party responsible, without the foundation having to establish a contractual relationship with it. That is a proposal, and this paper is deliberate in saying so.

The difficulty is not whether a registered data asset is capable of being property. Section 80(4) settles that for assets on the register, and it does so in terms that track the third category of personal property now confirmed for England and Wales by the Property (Digital Assets etc) Act 2025 — a thing capable of being the object of personal property rights although it is neither a thing in possession nor a thing in action. The Island's provision is, if anything, ahead of that development rather than behind it, because it constitutes the right rather than leaving its recognition to be worked out case by case. The difficulty is that property status does not of itself supply a remedy against a stranger. The 2025 Act expressly leaves the rights attaching to third category things to be developed by the courts, and the established torts protecting property depend on possession, which a data asset cannot support. A foundation whose asset is used without authority therefore has a property right and, at present, no settled cause of action by which to vindicate it against a party with whom it has no contract.

The Department proposes to close that gap through the Regulations. The Attorney General's Chambers will be consulted on the vehicle, on the extent of the regulation making power in section 92, and on whether a cause of action of this kind can properly be created by subordinate legislation at all. Respondents should read every reference in this paper to interference with a registered data asset — including the data protection carve out at Part 5.2 — as describing an intended protection whose availability and final form depend on that advice.

Whatever form the remedy finally takes, the default position at the level of governance is deny. The wrapper states what is permitted; anything not granted is not permitted; and the register makes the grant position legible to counterparties rather than leaving it to be asserted. The Data Enforcer polices the boundary from within — monitoring grants against the wrapper's terms and escalating departures the council does not resolve — and the AAP's periodic Level 2 attestation provides external verification that actual use conforms to declared purpose.

One boundary is drawn deliberately. What a licensee or consumer does inside its own organisation with data lawfully received under the wrapper is governed by the wrapper's terms and by general law, not by this framework. The regime governs the asset and the terms of access to it; it does not follow the data into every counterparty's internal data management arrangements.

4.4.2 Third-party rights within a dedicated asset

A data asset is often built on rights the foundation does not own outright: licensed inputs, database rights, content subject to third-party intellectual property, or material whose use is limited by the terms on which it was acquired. The dedication instrument records those interests, because section 76(2)(d) and (e) require it to describe the rights and permissions the foundation holds and to identify any restriction, limitation or condition attaching to them. Recording an interest is not the same as governing it, and the framework accordingly places a continuing duty on the council in respect of assets carrying third-party rights.

The proposed duty has three limbs. The first is the consent chain: the council must be able to demonstrate, for each stratum of the asset, the chain of rights by which the foundation holds what it purports to hold, and must maintain that evidence for as long as the asset is registered. The second is grant discipline: no entitlement granted under

the governance wrapper may exceed the rights actually dedicated, and where a head licence restricts sub-licensing, derivation or a category of use, the wrapper terms must carry that restriction through to every grant made under them. The third is contamination control: where material enters an asset whose rights position is unresolved, or where a head licence is terminated or varied, the council must isolate the affected stratum and treat the change as a material change to the asset boundary.

The third-party rights evidence standard will specify evidence proportionate to each asset class. At launch, rights and restrictions are declared through the dedication material, asset description, provenance and assurance records using the lawful locations prescribed for those fields. Section 3 of the register record remains inoperative until the later charges and priority machinery commences; recording a rights declaration at launch does not register a security interest or establish priority. Conformity with the duty falls within the applicable Level 2 profile. The detailed field allocation will be completed with the Dictionary.

4.5 Material change and Tier 2 amendments

Data assets are inherently dynamic. Data is added or removed; boundaries are redrawn; anonymisation degrades or improves; hosting moves; purposes evolve; classification ceases to be accurate. A register whose entries could not change would quickly become a register of fictions; a register whose entries changed informally would forfeit the reliability that makes it worth consulting. The amendment regime is the mechanism that reconciles the two, and it embodies a principle stated in Part 3 and worth repeating: register integrity means auditability of state transitions, not immutability of content.

Class A covers changes preserving asset identity. Tier 1 covers routine content changes within the declared envelope, recorded in the foundation's evidence trail as required; Tier 2 covers material changes to the registered description or governance state. Reclassification alone is Tier 2. Changes beyond the identity-preserving envelope are Class B events requiring a fresh application, sometimes described as Tier 3; they are not amendments within Class A. Class C covers transmission of the same asset between foundations through the legally operative process. Class D consolidation and division are deferred from launch. A material amendment retains the identifier and original registration date, but the treatment of rights, licences and assurance follows the applicable law and terms. Changed states must remain within the scope of valid accreditation before use. The DAR Regulations supply legal event effects; the Standard supplies authorised criteria. Neither a changed hash nor widening the declared envelope can conceal a substantive change of identity.

A foundation must give effect to a valid data subject rights request without prior Registrar approval. It then assesses the effect on the asset and assurance coverage. Routine corrections within the envelope follow the applicable internal evidence rules; material changes are notified and recorded through the amendment process. The DAR Regulations must reconcile the data subject rights ground with the routine-change exception. No Class B event arises merely because a valid right was exercised. The Registrar records the resulting change without adjudicating the request; the Data Enforcer checks performance within its remit. Part 5.5 sets out the approach.

Alongside the amendment machinery sits the duty of accuracy. The council must notify the registrar without undue delay on becoming aware of a mistake in the register relating to the foundation's data (section 83(4)); the Data Enforcer bears a parallel duty in the performance of its functions (section 83(5)); and the register records an asset as "under review" while the registrar assesses the accuracy of its record (section 83(3)). Failure to comply with the notification duties is an offence under the Act. Third parties may apply to update the register in the circumstances and through the process prescribed in the Regulations, with internal reconsideration at launch under the minimum viable enforcement regulations. No statutory alternative dispute resolution process is assumed at launch.

4.6 Accreditation lapse and remediation

4.6.1 Accreditation is binary

Accreditation is not a one-time gate but a continuing condition of utilisation, and it is binary. A foundation must not utilise a data asset unless there is a valid data asset accreditation in respect of it (section 85(1)). An accreditation that has expired, or been revoked, is not a downgraded governance signal; it is the absence of the condition on which lawful utilisation depends, and it puts the asset on a statutory clock. This is a point on which the framework's earlier working drafts and the Act have to be reconciled squarely, and Part 6.4 does so: governance signals convey depth of assurance, and register standing conveys whether the asset may be used at all. The two must not be confused, in this paper or in the instruments.

4.6.2 The remediation pathway

Where an accreditation is revoked or has expired, the registrar must update the register to record that the asset is subject to remediation (section 85(4)). Three things are then simultaneously true. First, the prohibition on utilisation continues to apply (section 85(5)(a)). Second, the personal property right vested on full registration remains in effect (section 85(5)(b)) — remediation suspends use, not ownership, which matters considerably to any lender or counterparty whose position depends on the asset's continued existence. Third, the clock runs: the council must, within the remediation period, provide the registrar with confirmation of a valid accreditation. The remediation period is 90 days, or such other period as the Regulations prescribe for specific categories of asset (section 85(6)), extensible once by up to a further 90 days on written application if the registrar is satisfied that there are reasonable grounds (section 85(7)). If a valid accreditation has not been provided when the period expires, the registrar must follow the process prescribed in the Regulations to remove the asset from the register (section 85(8)) — at which point the disposal and reversion provisions described at 4.7 take over.

In practice, remediation is a council-led process with the rest of the architecture in support. The deficiency will typically have been surfaced by an AAP qualification or a verification alert; the council decides and executes the remediation, drawing on the remediation procedure that Practice Direction 1 requires it to maintain; the AAP re-attests after material remediation; and the Data Enforcer reviews, with standing to escalate if the council does not act.

4.6.3 Preservation during remediation

The drafting baseline is to permit lawful custody, security, preservation, compliance with data protection law and acts strictly necessary to obtain accreditation during all relevant prohibited-use periods, including suspension and remediation, while prohibiting commercial exploitation. The broad definition of utilisation in section 67 and the interaction of sections 76(2)(f), 81 and 85 require legal confirmation. Part 6.4.3 explains the Attorney General referral and the proposed legislative fallback.

4.6.4 Suspension, and lapse of a mandated Level 3 assessment

Suspension is recorded under sections 85(2) and (3). The framework's design is that utilisation is prohibited during suspension, subject to a legally effective preservation route. Suspension does not itself trigger the statutory remediation clock, which attaches to revocation or expiry. The DGF Regulations must specify grounds, competent decision-makers, review, maximum duration and lifting or revocation conditions; the DAR Regulations record the resulting status and process. Automatic conversion must not be inferred without an operative rule.

The framework uses one statutory accreditation and one expiry. Where Level 3 is mandatory, that expiry must fall no later than the end of the external assessment's accepted currency. Scheduled expiry therefore follows the ordinary section 85 pathway. An earlier adverse finding or withdrawal of supporting evidence is referred promptly through the prescribed review, suspension or revocation process; it is not silently treated as a second expiry date. Where Level 3 is optional, its lapse is an evidence update and has no automatic section 85 consequence.

Questions of penalty for contravention are outside the scope of this paper. The consequence structure described here is the Act's own — prohibition on use, register status, and ultimately removal — and the separate sanctions instrument described at 1.4 will address civil penalties and their coordination with the Information Commissioner's powers.

4.7 Reversion or removal

An asset leaves the register in one of a small number of ways: the foundation is wound up, dissolved or otherwise removed from the register of foundations; the asset is removed by the registrar following failed remediation or otherwise under the Regulations; or the foundation itself removes the asset for the purpose of utilising it in accordance with its objects — for example, on a sale in which the asset is transferred to another data asset foundation through the simplified application process the Regulations may provide under section 80(5).

Except in the last case, section 81 governs what happens to the asset, and it establishes a strict order of priority. The asset and all rights pertaining to it are disposed of, or revert, first in the manner specified in the dedication instrument; second, if the dedication instrument is silent, in the manner specified in the foundation rules; third, if the rules are also silent, the property right is extinguished and all dedicated rights and permissions revert to the dedicator, provided the dedicator exists and can reasonably be ascertained; and finally, only if no dedicator can be ascertained, the asset is treated as bona vacantia. The Act expressly displaces the ordinary rule that a dissolved

foundation's assets vest in the Treasury: a data asset reaches the Treasury only at the end of the chain, never at its beginning.

The order of priority returns the reader to the point made at 4.2: the dedication instrument is where the exit is designed, at the moment of entry. A dedicator who wants the data returned, destroyed, transferred to a successor foundation or released under an open licence on the foundation's failure specifies that outcome in the dedication instrument, and the specification binds. Where an asset is removed but the foundation survives, the council must take all necessary steps to effect the disposal or reversion in the statutory order. On removal, the personal property right is extinguished (section 81(8)) — the right that registration created, removal ends — though the underlying data, and any continuing rights and obligations in it under general law, of course persist.

Where the asset contains personal data, disposal and reversion are executed subject to data protection law in the ordinary way: reversion transfers the dedicated rights and permissions, and the recipient's ability to process any personal data within the asset depends on its own lawful basis. Part 5 addresses the interface.

4.8 Worked examples

Three worked examples follow. They are illustrative only: they show how the machinery described in this Part combines in realistic scenarios, and they simplify deliberately. They do not state the Department's position on how any actual case would be determined, and nothing in them qualifies the instruments they illustrate.

4.8.1 Example A: An anonymised clinical research dataset

A research consortium holds a longitudinal clinical dataset, anonymised to a standard the consortium considers robust, and wishes to place it under independent, durable governance so that access can be granted to researchers on consistent terms beyond the life of any single funding cycle. The consortium establishes a data asset foundation whose objects relate to the curation of the dataset and the grant of research access, dedicates the dataset, and applies for registration.

The consortium claims non-personal status, but that classification must be supported before it can justify reduced safeguards. The assessment considers the methodology, its implementation, the intended recipients and access conditions, and plausible linkage or re-identification. If supported, the asset is Sensitivity Level 1 with controlled research access; the health sector overlay may still raise assurance requirements. Pending adequate support, the foundation uses conservative controls and restricts release; this does not deem the data personal as a matter of law or supply a lawful basis for processing.

A competent independent reviewer substantively assesses the claim, and the AAP evaluates and incorporates the conclusion into its accreditation decision. A suitably qualified AAP team member may perform that work; otherwise specialist support is required. Existing independent evidence can be reused where current and properly scoped, with targeted testing for greater exposure, consequences or uncertainty. The council remains accountable for its claim and continuing controls. The register distinguishes the declaration from the assessed conclusion and publishes a safe

summary of scope, date, context and limitations rather than an unconditional guarantee of anonymity.

The classification and the overlay together drive the governance minimums — the DAR Code controls attested at Level 2, the accreditation refresh cycle, and the data protection touchpoints appropriate to an asset whose non-personal status depends on a boundary that can move.

Assuming the claim is supported, the asset is low on the personal-data sensitivity axis despite its clinical origin. Whether Level 3 is mandatory depends on both the applicable matrix cells and any designated sectoral overlay, not on restricted distribution alone. If no mandate applies, the foundation obtains the single accreditation supported by Levels 1 and 2 and considers the Department's recommendation for optional external assessment. If a mandate applies, the accreditation period is constrained by the required Level 3 assessment's accepted currency.

Two years on, a published reidentification technique weakens the anonymisation claim for a subset of the records. The foundation's continuing review surfaces the issue and triggers prompt containment and reassessment, without waiting for the annual cycle. Any expansion of recipients, linkage or purpose also requires reassessment before the changed release. Reclassification is a recognised Tier 2 amendment ground: the council notifies the registrar, the asset's classification is amended, and the changed classification carries changed minimums — a shortened attestation cycle and, because part of the asset must now be treated as personal data, the full engagement of the controller obligations described in Part 5, including the handling of any data subject rights requests through the amendment pathway at 4.5. The register throughout tells the truth about the asset's state: prospective licensees see the reclassification and the refreshed attestation, not a stale claim.

4.8.2 Example B: An AI training corpus

A media and technology business assembles a training corpus from three sources: content it created and owns outright; content licensed in from third-party rights holders on terms permitting model training but restricting sub-licensing; and content in the public domain. It wants to license the corpus to model developers, and it knows its market: buyers of training data increasingly pay for provenance, because their own regulatory and litigation exposure turns on it. The business establishes a data asset foundation and dedicates the corpus.

The dedication instrument carries the load in this example. It describes the three provenance strata; it records that the rights dedicated in respect of the licensed stratum are subject to the head licence terms, including the sub-licensing restriction; and it identifies the reserved rights. The Asset Boundary Profile reflects that structure, and the third-party interests are visible on the register as characteristics of the asset. The wrapper's terms translate the head licence restrictions into entitlement conditions: the council may grant training use licences, but no grant may exceed what the dedicated rights support.

At registration, the Level 2 component of the accreditation covers, alongside the DAR Code controls, the asset class items the attestation profile specifies for training corpora: provenance and derivation evidence, and the conformity of the licensing terms actually

offered with the rights actually held, assessed against the third-party rights evidence standard identified in the Instrument Map. The forthcoming worked attestation profile in Annex D will illustrate its construction. This is where the regime's external story is strongest: lineage is a property of the asset, verified and register marked, rather than a representation in a licence schedule. When a model developer's counsel asks the question every such counsel now asks — what is this trained on, and who says so — the answer is a register entry, an attestation signal naming the assessor, and a wrapper whose purpose limits are recorded rather than negotiated afresh. A licensee that exceeds its grant — training a model class the entitlement excludes, or sub-licensing the restricted stratum — is in breach of its licence, and would additionally be answerable to the foundation under the cause of action proposed at 4.4.1 if that proposal is carried through.

When the business later adds a fourth content stratum to the corpus, the council assesses the addition against the declared envelope. If identity is preserved, it is a Tier 2 amendment with prompt reassessment of affected provenance evidence; if the addition exceeds the envelope, Class B requires a fresh application. Assurance for the changed scope must be adequate before use. The corpus grows; the governance record grows with it.

4.8.3 Example C: A telemetry asset as collateral

An industrial operator generates a continuous telemetry dataset — machine performance data across a large installed base — with demonstrable revenue attached: it is licensed to insurers and to the equipment manufacturer's analytics arm. The operator wants to raise asset finance against the data. Its lender's difficulty is conventional: the dataset is valuable but legally amorphous — no possession, no document of title, no reliable way to know that what is charged today still exists, ungoverned copies notwithstanding, tomorrow.

The regime's answer is the structure this Part has described, deployed for a financing purpose. The operator establishes a data asset foundation as custodian and dedicates the telemetry asset; the dedication instrument and foundation rules are drafted with the financing in view, including the disposal provisions the lender requires. On the register, the lender can see the asset's classification, its accreditation status and its governance signals. The primary stratum contains no personal data, so it sits at the lowest level of the Data Sensitivity axis; any operator personnel data is separately identified and classified. The asset's commercial sensitivity is not a coordinate on that axis and does not need to be: what protects it is the Distribution Scope coordinate, which records that the asset is not broadly distributed, together with the recorded governance wrapper and, where the operator's sector engages one, the applicable sectoral overlay. The foundation obtains the collateral grade attestation profile described in Part 6 — the Level 2 component plus defined scope items on custody arrangements, escrow conditionality and enforcement pathway — converting the foundation as custodian claim from an assertion into a verified, register marked characteristic. The lender takes its security over an asset that is a personal property right by statute, whose continued conformity is periodically attested, and whose state transitions are auditable. One point of sequencing should be stated, because the example depends on it. The Act contains no charges or priority machinery for data assets; registration of security interests is proposed design resting on the general regulation-making powers, and it is a later

release rather than a launch capability. Until it is available, security is taken and perfected by the ordinary means and the register supplies the asset's governance state rather than its priority position.

The lapse architecture is part of what the lender is relying on, and it is a double-edged reliance that the paper states honestly. If the foundation's accreditation lapses mid-facility, the asset enters remediation: utilisation is suspended, but the property right persists while the council cures the deficiency (4.6.2). The security's continuing effect depends on its terms and applicable law; registration does not guarantee its value or enforceability. What the lender must also price is the far end of that pathway: if remediation fails within the statutory period, the registrar must remove the asset, and removal extinguishes the property right over which the security was taken. The remediation window is therefore a covenant event of the first order, and the register makes it visible as it happens rather than at the next reporting date. The preservation carve out at 4.6.3 matters to the same audience for the opposite reason: a lender needs the custodian to be able to keep the asset safe during remediation, not merely to be prohibited from exploiting it.

The telemetry contains a modest stratum of personal data relating to equipment operators, and during the facility's life the foundation receives valid erasure requests. It gives effect to them, notifies the registrar, and the amendments are recorded through the pathway at 4.5. The lender has no complaint: the carve-out proposed at Part 5.2 provides that an act done in compliance with data protection legislation is not, by reason only of that compliance, a contravention of the Regulations or an interference with a registered asset. Nor is the lender surprised in fact — the collateral grade attestation profile discloses data subject rights volatility as an asset characteristic, and the facility was priced with it in view. The carve out protects the data subject; the disclosure protects the credit decision; and the foundation is never squeezed between the two.

Part 5: The data protection interface

Most data assets that matter contain, have contained, or may come to contain personal data. Any framework for the governance of data assets must therefore address clearly how it interacts with data protection law. This Part sets out the proposed relationship between the Data Asset Foundations regime, the Data Protection Act 2018 and the Applied GDPR.

The Department's position is that the Data Asset Foundations regime is intended to operate alongside the Data Protection Act 2018 and the Applied GDPR, without displacing or modifying the requirements of either. Where the regimes apply to the same facts, the framework is intended to provide a clear means of identifying and managing the relevant interface. We refer to this approach as designed coexistence.

This Part identifies the main points of interaction between the regimes and explains the proposed approach at each. The purpose is to enable respondents to assess whether those arrangements are sufficiently clear, coherent and workable, and to identify any additional interface points that may need to be addressed.

This Part is also intended to support detailed scrutiny by those with expertise in data protection law and practice. Nothing in this Part constitutes legal advice or states, implies or presumes the position of the Information Commissioner.

5.1 Two regimes, two objects

The Applied GDPR regulates the processing of personal data. It attaches obligations to controllers and processors, and confers rights on data subjects, wherever and however personal data is handled. Its object of regulation is the processing.

The Data Asset Foundations regime constitutes property in a governed data asset: the data asset together with its recorded governance terms — the asset and its wrapper, considered together. The object of the right is that composite, never underlying personal data as such. The register records governance state; it does not record, certify or substitute for consent or for any other lawful basis.

Because the two regimes operate on different objects, they are capable of applying simultaneously to the same facts without contradiction. A foundation holding a dedicated data asset that contains personal data is, in respect of that personal data, a controller under the Applied GDPR in the ordinary way. Dedication changes the property and governance position of the asset; it changes nothing about the data protection position of the personal data within it. Every data subject right is exercisable against the foundation exactly as against any other controller. No right of a data subject is assigned, waived or diminished by dedication.

The Department does not pretend that the two regimes never pull against each other at first sight. They touch the same facts at defined points — we identified eight — and at each point an obligation or expectation under one regime can appear, on a first reading, to strain against the other. The Department's claim is not that no tension exists; it is that each tension is resolved by design, without derogation from any data subject right and without qualification of the Information Commissioner's competence. Sections 5.2 to 5.8 work through the resolutions.

One point of framing deserves to be met head on, because it is the objection most often raised against any property concept for data: that dedicating an asset containing personal data asserts ownership over data subjects' information, contrary to the principle that personal data is not a proprietary commodity of the controller. The framework's answer is structural, not rhetorical. The property right is in the composite of asset and wrapper; it confers no processing entitlement; and the controller's obligations and the data subject's rights are untouched by registration. What registration changes is who accountably holds the asset, on what recorded terms, and with what visible governance — which is a strengthening of the data subject's practical position, not a dilution of it.

5.2 The non-derogation principle

The relationship described at 5.1 is not left to inference. A single anchoring provision at Regulations tier puts it beyond argument. The proposed working text is as follows:

Relationship with data protection legislation

(1) Nothing in these Regulations, or in any instrument made under them, limits, conditions or displaces — (a) any right of a data subject under the Data Protection Act 2018 or the Applied GDPR; (b) any obligation of a controller or processor under that legislation; or (c) any function of the Information Commissioner.

(2) An act done in compliance with the Data Protection Act 2018 or the Applied GDPR is not, by reason only of that compliance, a contravention of these Regulations or an interference with a registered data asset.

(3) These Regulations are to be read, so far as possible, consistently with the legislation referred to in paragraph (1).

The provision does three jobs. Paragraph (1) is the general non-derogation rule: the framework takes data protection law as it finds it. Paragraph (2) is the compliance carve out, whose significance for the proposed protection against unauthorised use is developed at 5.5.4. Paragraph (3) imports a consistent construction rule, so that any residual ambiguity in the framework is resolved in favour of data protection law without recourse to amendment of the primary Act.

The statutory hook is already in the Act: section 69(b) requires the data governance framework to specify the role of the Isle of Man Information Commissioner in relation to the supervision of data asset foundations in respect of their processing of personal data. The non-derogation provision, the controllership map at 5.3, the demarcation at 5.7 and the guidance at 5.9 together discharge that requirement. Consistent with the framework's instrument discipline, interface mechanisms should be delivered through subordinate legislation and guidance where the Act permits. The reversion and preservation issue at 6.4.3 remains subject to legal confirmation and, if necessary, the proposed primary-legislation amendment route.

5.3 Controllership

The regime introduces roles whose data protection responsibilities must be mapped by processing activity. The map below describes the intended operational allocation and

remains subject to the applicable data protection laws; controller, joint-controller and processor status follows applicable law and the actual purposes and means of processing, not a label in the foundation instrument or a contract.

The Central Registry's entity-register operations and the Data Asset Registrar's asset-register operations are distinct. The Registrar-hosted verification design also requires separate mapping of any authorised content inspection, gateway operation, independent assurance and service-provider processing. The map must identify accountable legal entities and data flows before deployment; software is not itself a controller or processor.

Actor	Personal data in scope	Role*	Notes
Foundation	Personal data within the dedicated asset	Controller	All data subject rights exercisable against it in the ordinary way
Council and internal allocations (data steward functions and the like)	As organs of the foundation	Discharge the foundation's accountability obligations	Not separate controllers by virtue of office alone
Data enforcer	Personal data processed in discharging its functions: records of its enquiries and enforcement, material obtained under section 86(4), escalations	Controller (its own functions)	Not a processor of the foundation; not a controller of asset contents by virtue of office. Statutory disclosure gateway to the registrar at section 86(5)
Accredited assurance provider	Personal data processed in forming and issuing an accreditation opinion, and its working papers	Controller (its own functions)	Independent professional judgement; accredited by the Department under section 84(1). Statutory disclosure gateway to the registrar at section 84(5)
Data asset registrar	Register metadata, applicant and officer information; any personal data processed in authorised verification activities	Controller for its register functions; verification roles assessed by activity	No categorical exemption for asset contents inspected in a Registrar-hosted service; identify actual purposes, means and responsible entities before deployment

Actor	Personal data in scope	Role*	Notes
Central Registry	Establishment and entity filings for data asset foundations	Controller (Foundations Act 2011 register operations only)	Included for completeness; its processing is governed by the 2011 Act regime in the ordinary way and is not altered by the framework
Service providers (hosting, storage, operational support)	Asset contents processed on the foundation's instructions	Processors where acting solely on the controller's instructions	Article 28 contracts in the ordinary way; reflected in attestation profiles. Distinct from the data enforcer and the assurance provider, neither of which acts on instruction
Verification Agent (when deployed)	Asset state data within the trusted execution environment	Software; processing attributed to the responsible legal entities	Registrar-hosted design; map metadata checks and any content inspection separately. TEE isolation does not remove data protection obligations

**this map is indicative and remains subject to the actual function and applicable laws*

The foundation remains accountable for its own processing and cannot transfer that accountability by registering the asset. The Registrar's register functions and any hosted verification processing must be analysed separately. Office alone does not create controllership of all asset contents: a council member ordinarily acts as an organ of the foundation, while independent assurance and review bodies are responsible for the personal data they process in performing their own functions. The actual arrangement governs any joint-controller or processor relationship.

Those two rows will be the unfamiliar ones, and they are worth explaining, because the intuitive classification is the wrong one. The data enforcer and the accredited assurance provider are each appointed by the foundation and paid by it, which invites the assumption that each processes on the foundation's behalf under an Article 28 contract. Neither does. A processor acts on the controller's instructions, and the whole point of both roles is that they do not. The data enforcer monitors the council's conduct against the foundation instrument and the registered governance wrapper, may act against the foundation, has standing to put a matter before the registrar or the court, and carries a liability floor at section 87 that no contract can exclude. The assurance provider forms an independent professional judgement on whether the asset meets the requirements of the framework, determines the scope and manner of its own enquiry, and holds an accreditation granted by the Department under section 84(1) rather than a mandate given by the foundation. Each therefore determines the purposes and means of the

personal data it processes in discharging its own functions, and each is a controller of that processing.

Three practical consequences follow, and founders should note them. First, the foundation cannot discharge its accountability for what it hands to either party by putting a processor contract in place: the disclosure is controller to controller, and it needs a lawful basis of its own. The statutory duties to cooperate and to give reasonable assistance — section 86(4) for the enforcer and section 84(3)(b) for the provider, the latter offence-backed at section 84(6) — are directly relevant to that analysis. Second, onward disclosure to the data asset registrar is expressly provided for by section 86(5) and section 84(5); those are statutory gateways, and neither party needs the foundation's permission to use them. Third, the scope of each party's controllership is its own functions and no more — its monitoring records, working papers, correspondence and escalations — not the asset itself.

The AAP should minimise access to personal data. Independent substantive anonymisation assessment under 5.8 may use properly scoped existing evidence, controlled samples or specialist testing; a documentary existence check alone is insufficient. Where inspection of personal data is necessary, it requires an applicable lawful basis and, where relevant, an Article 9 condition, with access and retention limited to the assessment's needs. TEE protection does not turn personal-data processing into non-processing.

The map is explanatory; it does not create controllership, which is always a question of fact under the Applied GDPR. Its function is to remove ambiguity for founders and to give the Information Commissioner a stable account of where Applied GDPR obligations bite within the structure. A one line anchor at Regulations tier will confirm that registration does not of itself alter controllership.

5.4 Dedication is not a lawful basis

The point in this section is short, and the framework states it plainly and repeatedly because experience with novel legal structures suggests it will otherwise be assumed away: dedication confers no lawful basis for processing. Registration confers no lawful basis for processing. Recording a purpose in the foundation instrument, the dedication instrument or the governance wrapper confers no lawful basis for processing. Every purpose of a data asset foundation that involves the processing of personal data must rest independently on an Article 6 basis and, where applicable, an Article 9 condition under the Applied GDPR — established by the foundation as controller, in the ordinary way, and supervised by the Information Commissioner in the ordinary way.

What the framework does do is channel founders towards data protection compliance at the point of establishment rather than after it. Classification on the Data Sensitivity axis drives mandatory governance minimums constitutively, and for high-sensitivity classes those minimums include data protection touchpoints — data protection impact assessment expectations engage at establishment, not as an afterthought once processing has begun. A founder cannot bring a personal data bearing asset through registration without the framework having asked the data protection questions on the way in. The register does not certify the answers — that is not its function, and 5.1

explains why it cannot be — but the architecture ensures the questions are asked at the moment they are cheapest to answer well.

5.5 Data subject rights and the register

5.5.1 Erasure and rectification are not the enemies of register integrity

The most intuitive objection to a constitutive, integrity assured register is that it appears to resist change: Articles 16 and 17 of the Applied GDPR require rectification and erasure on valid request, and a register whose reliability depends on the stability of its entries looks, at first sight, like a structure with an incentive to resist both. The objection rests on a misreading of what register integrity means, and the framework's answer to it is the principle stated in Part 3 and applied throughout Part 4: register integrity means auditability of state transitions, not immutability of content. A register that could not change would be a register of fictions; a register that changes on defined grounds, through a recorded and verified process, tells the truth about the asset over its whole life. Compliance with data subject rights is not a threat to that kind of integrity — it is an instance of it working.

5.5.2 The data subject rights amendment pathway

The foundation determines and gives effect to a valid request without prior Registrar approval. It then assesses whether the change is routine within the declared envelope or a material amendment, records the necessary evidence and makes the notifications required by the DAR Regulations. Material changes are recorded and their integrity checked by the AAP at launch and by deployed automation only within its capabilities. The amendment rules must reconcile the data subject rights ground with the routine-change exception; exercising a valid right is not itself a Class B trigger.

The allocation of judgement in that sequence is deliberate. The data asset registrar at no point adjudicates the validity of the underlying request: whether a request is well founded is a controller level question, subject to the Information Commissioner's supervision, and it stays there. The registrar's role is confined to recording the amendment and verifying the integrity of the resulting state. The data enforcer, for its part, verifies that effect has in fact been given — an independent check, internal to the regime, that the foundation's data protection compliance is real and not merely asserted. The framework's insistence that the register tell the truth is backed by duty as well as by design: where a council or a data enforcer becomes aware of a mistake in the register, section 83(4) and (5) require notification without undue delay. Failure to notify is an offence, committed by the foundation where the duty is the council's (section 83(9)) and by the data enforcer where the duty is its own (section 83(10)). An entry left describing an asset as it was before an amendment took effect is capable of being such a mistake. The end-to-end sequence, with indicative timescales, is to be set out operationally in the Registrar Practice Direction on data subject rights amendments and in the guidance.

5.5.3 Amendment and the validity of the accreditation

The data asset accreditation is not a transparency signal that can lapse quietly. Under section 85(1) a foundation must not utilise a data asset unless there is a valid accreditation in respect of it, and the machinery at section 85(4) to (8) makes expiry or

revocation existential: the asset is recorded as subject to remediation, a 90-day period runs (extendable once), and if valid accreditation is not restored the data asset registrar must remove the asset from the register. Levels 1 and 2 together constitute that accreditation, as Part 6 explains.

The question is what a data subject rights amendment does to it. An accreditation is issued on the asset as described at the time it is issued. A Tier 2 amendment giving effect to an erasure request may change the asset materially enough that the Level 1 verification — that the asset exists and its boundary is as described in the Asset Boundary Profile — no longer holds good of what remains. If the amendment displaces the accreditation, a foundation that has complied promptly with Article 17 finds itself prohibited from utilising the asset until it has been re-attested. That would be a perverse result, and a familiar one in a new guise: the framework would have closed the chilling effect at 5.5.4 and reopened it through the accreditation door.

The Department's approach is to preserve the single accreditation where the amended asset remains within its assured scope. The council records the impact and obtains prompt reassessment of affected evidence where material, rather than automatically deferring it to the next annual cycle. A routine correction need not trigger a complete new audit. Where the changed asset can no longer satisfy the applicable requirements, the prescribed review, suspension or revocation process applies; statutory expiry and remediation continue to follow section 85. Nothing in that process delays compliance with the data subject's valid request.

5.5.4 Compliance and the protection against unauthorised use

Paragraph (2) of the provision at 5.2 provides that an act done in compliance with the Data Protection Act 2018 or the Applied GDPR is not, by reason only of that compliance, a contravention of the framework or an interference with a registered data asset. The carve out is drafted to attach to the protection in whatever form it emerges; if it does not emerge at all, the carve out costs nothing and the position is unchanged. The Department's intention is that a foundation which erases personal data in discharge of a valid Article 17 request should have, as against every holder of an interest in the asset, a complete answer.

The commercial exposure that remains is managed transparently rather than suppressed. An asset containing personal data carries an irreducible susceptibility to change through the exercise of data subject rights; the framework's approach is to make that characteristic visible at origination rather than contested at the point of compliance. Collateral grade attestation profiles disclose data subject rights volatility as an asset characteristic, so that a lender prices the risk when taking the asset as security instead of litigating it when a data subject exercises a right. Part 4's Example C illustrates the position from the lender's side.

5.6 Register publicity and data minimisation

The Register publishes metadata and governance state, not the underlying asset. Access is tiered using the DAR Regulations' names: Level 1 access tier, Level 2 access tier and Level 3 access tier. These must always be distinguished from Levels 0–3 of the assurance ladder. The schema applies data minimisation to asset descriptions,

instrument extracts and assurance records. Public history and evidence summaries remain subject to lawful redaction, restriction and retention; auditability is not a promise of permanent public access to personal data.

Three further safeguards operate at the schema's edges. Free text fields, which are where personal data most often arrives uninvited, are constrained. The data asset registrar has power to require redaction of personal data from publishable particulars, so that an application drafted carelessly does not become a publication problem. And the registrar's own processing of applicant and officer information — one of its processing activities, per the map at 5.3 — is governed by its privacy notice in the ordinary way. The publishable particulars schedule sits in the Regulations; the redaction procedure sits in the Registrar Practice Direction.

5.7 Parallel enforcement

A data asset foundation answers to two regimes: to the Information Commissioner in respect of its processing of personal data, and to the data asset registrar in respect of its register, attestation and governance wrapper obligations. The same conduct can, on some facts, engage both. Unmanaged, that raises two familiar concerns — double jeopardy, and forum confusion, in which a foundation facing a problem does not know whom it answers to first.

The framework's first answer is demarcation by subject matter. Processing contraventions are for the Information Commissioner; register, attestation and governance wrapper contraventions are for the data asset registrar. Neither absorbs the other's remit: the registrar does not adjudicate data protection compliance (a point the controllership map and the amendment pathway both reflect), and the Information Commissioner's functions are untouched by the framework (a point the non-derogation provision puts at Regulations tier). The institutional separation is not an accident of drafting; it is the design.

The second answer is coordination where the boundary is crossed. A coordination protocol between the data asset registrar and the Information Commissioner should provide for referral where a matter arising in one regime discloses a contravention in the other, for information sharing within the statutory gateways, and for sequencing where the same conduct engages both regimes. A no double penalisation principle for the same conduct is to be stated in the guidance, and the Department proposes that the forthcoming sanctions instrument should require the registrar to have regard to any penalty imposed by the Information Commissioner in respect of the same facts. The form of that instrument is a matter for the separate consultation described at 1.4.

5.8 The anonymisation boundary

The boundary between personal and non-personal data is the single point on the interface where the greatest weight rests on a claim of fact. An asset dedicated as non-personal on the strength of an anonymisation claim escapes, if the claim holds, the controller obligations that would otherwise follow the personal data — and if the claim is weak, degrades over time, or fails against evolving reidentification techniques, the asset is misclassified and every governance minimum calibrated to its classification is

miscalibrated with it. A framework that took anonymisation claims at face value would have built its most consequential judgement on its least examined input.

At launch, a non-personal claim that depends on anonymisation must have substantive independent support before it can justify reduced governance safeguards. The council declares the claim and remains accountable for it. A competent independent reviewer assesses the methodology, evidence of implementation and intended access or release context; the AAP evaluates and incorporates the conclusion and retains responsibility for its statutory satisfaction. A reviewer may be a suitably qualified member of the AAP team or an independent specialist, subject to the independence requirements at 6.2.3. A separate firm is not mandatory, but a competence gap requires specialist support, not a weaker conclusion.

Proportionality governs the work required. For data with no personal origin or apparent linkability, the AAP checks the basis for the classification, provenance and plausible linkage; it need not invent an anonymisation process that never occurred. For anonymised or synthetic data whose non-personal claim reduces safeguards, existing independent evidence may be reused if current and scoped to the asset, transformation, recipients and use. Greater exposure, consequences or uncertainty require targeted specialist testing of credible failure routes. Synthetic origin alone does not establish non-personal status. Pending adequate support, the claim cannot justify reduced safeguards or expanded release: conservative controls and restricted release are required, and full registration or changed use cannot proceed if valid accreditation cannot be supported. This is an assurance rule, not a legal deeming of uncertain data as personal.

The applicable legal test remains that under data protection law; the framework does not create its own definition of anonymity or presume the Information Commissioner's approval. The register records the claim separately from the independently assessed conclusion, including scope, reviewer competence and identity, assessment date, context, limitations, review triggers and current status. A safe public summary describes the claim as independently assessed in the stated context; technical attack details and linkage material remain restricted. Neither the AAP nor the register gives an unconditional guarantee that identification is impossible.

The foundation reassesses before a material expansion of recipients, linkage opportunities, purpose or transformation, and on credible re-identification evidence. Periodic confirmation is supplemented by targeted reassessment of changed elements; routine refreshes covered by a validated process need not trigger a complete new study. A live concern requires prompt containment and notification where required, without waiting for the annual cycle. Reclassification alone remains a Tier 2 amendment; the applicable controls and accreditation coverage must be reassessed before changed use. Personal-data obligations apply wherever the legal test is met.

5.9 Working with the Information Commissioner

The mechanisms described in this Part resolve the interface at the level of design. Making the interface work day to day is an operational matter, and the framework's chosen vehicle is guidance issued by the data asset registrar and the Information Commissioner. Issuing the substance jointly would serve the design directly: it would

demonstrate institutional alignment rather than asserting it, while preserving the Information Commissioner's independence — the guidance binds neither party's statutory discretion, and nothing in it qualifies the Commissioner's functions.

The Department proposes that the guidance be scoped collaboratively during the implementation phase, with the proposed Data Protection Interface Statement as the opening document for that conversation.

Part 6: Assurance and accreditation

6.1 Introduction: who checks?

Every substantive claim this paper has made about the framework leads, sooner or later, to the same question: who checks? Part 2 explained that governance under the framework is supplied by the architecture rather than built separately by each foundation. Part 3 described the register, the classification matrix and the accreditation ladder through which governance is made visible. Part 4 walked through the lifecycle, at almost every stage of which an accreditation, attestation or verification event appears. Part 5 showed how anonymisation claims and data subject rights volatility are evidenced rather than asserted. This Part sets out the machinery that makes all of that true in practice: the accredited assurance market, the levels of assurance and what each does and does not claim, the statutory consequences that follow when accreditation lapses, the circumstances in which the highest level is mandatory, the Department's recommendation for foundations outside the mandate, and the mechanisms by which external standards and registers are recognised.

The design principle running through this Part was stated in Part 2 and bears restating here. In a conventional enterprise, assurance over data governance is internal: an audit function of variable quality, reporting to the body whose conduct it audits. The framework externalises assurance. Any governance condition whose discharge can be verified mechanically or attested professionally is not evidenced by the body that performs it: the council decides and implements; the register, the Verification Agent and the Accredited Assurance Provider evidence. The result recorded on the register is available to every counterparty, which is what converts governance from a private assertion into a marketable property of the asset.

Accreditation under the Act is not one input among many to a governance picture: it is a condition of the asset's lawful use and, ultimately, of its continued registration. Section 85(1) prohibits a data asset foundation from utilising a data asset unless there is a valid data asset accreditation in respect of it, and section 85(8) requires removal from the register where accreditation is not restored within the remediation period. The assurance architecture described in this Part must therefore be read in two layers: the statutory layer, in which accreditation is binary — it is valid or it is not, and the consequences of its absence are prescribed by the Act — and the standards layer, in which governance signals convey the depth, currency and qualifications of the assurance behind an accreditation. Signals enrich the statutory position; they never soften it.

The statutory anchors for this Part are sections 69(c), 80, 84 and 85 of the Foundations (Amendment) Act 2026, together with the regulation making powers at section 92(3)(g) to (i). Section 69(c) requires the data governance framework to set minimum requirements for data asset accreditation. Section 84 requires every data asset foundation to appoint an Accredited Assurance Provider (AAP) and requires the Department to accredit those providers. Section 80 makes confirmation of a data asset accreditation a condition of full registration. Section 85 makes a valid accreditation a condition of lawful utilisation and prescribes the remediation and removal machinery that follows lapse.

6.2 The Accredited Assurance Provider scheme

6.2.1 Accreditation of providers by the Department

An Accredited Assurance Provider is a person or body accredited by the Department where the Department is satisfied that the applicable criteria and qualifications have been met (section 84(1) and (2)(a)). Those criteria and qualifications are set out in this framework, in the Verification and Accreditation Framework (Category 2), consistently with the division at 3.1.1: the substantive standard a provider must meet belongs with the framework, while the DAR Regulations carry register mechanics and legal effects. The Regulations will also specify the process for granting, suspending or revoking a provider's accreditation and will establish a public register of AAPs (section 84(2)(b) and (c)), so that any counterparty can verify that a named provider held accreditation at the date of a given engagement.

The institutional allocation is deliberate and should be read precisely. The Department accredits providers and owns the criteria by which they are admitted to and removed from the market. The statutory power remains with the Department, although, consistently with the Department's general allocation of its functions under the Act, operational functions under the scheme may be delegated to the Registrar and policy functions to Digital Isle of Man. The Data Asset Registrar does not accredit providers in its own right and does not adjudicate the quality of their work; the Registrar's own role in the assurance architecture is confined to the register consequences that the Act attaches to accreditation events — recording suspension, revocation and expiry (section 85(3)), marking remediation status (section 85(4)) and, at the end of the road, removing an asset whose accreditation is not restored (section 85(8)). Providers are, however, connected to the Registrar by an information gateway: information received by an AAP from a foundation in the course of its duties may be disclosed to the Registrar for the purposes of the Act (section 84(5)).

Admission to the scheme tests two things, and tests them separately. The first is competence: whether the provider can carry out the assessments to the required standard. At launch, current Authorised Partner status with the EDM Association is the qualifying route to accreditation and the evidence of competence on which the Department relies; the Department does not re-assess the skill that the authorisation evidences. The second is fitness and propriety: whether the provider, and those who own, run and sign for it, can be trusted to hold a statutory assurance role. That is a judgement the Department makes for itself, and no private authorisation substitutes for it. Both tests would be prescribed as criteria for accreditation under section 84(2)(a), so neither requires a new primary power.

The proposed process is conventional. The applicant applies in the prescribed form, with declarations from the firm and from each relevant person, and the Department carries out its own checks: criminal record certificates, sanctions screening, director disqualification registers, and regulatory and professional references. The Department grants, grants with conditions or refuses, giving reasons in each case, and its decision is open to the reconsideration and court routes described at 6.2.4. Fitness and propriety is a continuing requirement, not a hurdle at entry. An accredited provider must notify the Department within a prescribed period of any material change — a new relevant person, a change of control, a conviction, an insolvency event, or the lapse of its Authorised

Partner status or indemnity cover — and must give an annual declaration of continuing fitness and propriety; it is fully reassessed on renewal, and the Department may reassess at any time on reasonable grounds. Failing either test is a ground for suspension or revocation under section 84(2)(b). The Department proposes that loss of Authorised Partner status should suspend the provider's accreditation until it is restored.

6.2.2 Appointment by foundations and the provider's function

Every data asset foundation must appoint an AAP to issue the data asset accreditation supporting any registration application, and to issue renewals (section 84(3)(a)). The foundation must provide all reasonable assistance to the provider for the performance of its functions, and failure to do so is an offence (sections 84(3)(b) and 84(6)). The provider may issue or renew a data asset accreditation if satisfied that the data asset meets the requirements set out in the data governance framework (section 84(4)). An accreditation issued without that satisfaction would not answer the statutory definition, which requires an accreditation to meet the criteria set out in the framework and to be issued in accordance with the process set out in it (section 67); the binding therefore runs through the definition and through section 69(c) as much as through section 84(4). The framework's minimum requirements for accreditation are themselves a statutory obligation of the Regulations under section 69(c), and the form, procedure, criteria for issue, renewal, suspension and revocation of accreditations, together with audit, reporting and renewal-period requirements, are within the regulation making powers at section 92(3)(g), (h) and (i).

The scheme therefore has three legs, each in its proper place: the Act supplies the offices and the consequences; the Regulations supply the criteria, procedures and cycles; and the standards tier supplies the attestation profiles — what a particular engagement actually checks for a given kind of asset — where content can mature with the assurance market without re-legislation. Consistent with the bounded-commitment discipline described in Part 2, the white paper proposes to hard-commit in Regulations only the levels of the ladder, the recording mechanism and the consequences of lapse; profiles, thresholds and cycles belong in the standards tier.

The provider's satisfaction extends to the basis of the asset's classification. Where an asset is derived from personal data and its non-personal classification depends on a claim of anonymisation, the accreditation extends to that claim, and the provider forms its view on the substantive independent assessment described at 5.8; the council declares the claim and remains accountable for it.

A note on where providers will come from. The Department expects the AAP cohort to be drawn substantially from established assurance practices, namely the EDM Association's existing Authorised Partner network. A single provider will therefore commonly deliver Levels 1 and 2 and Level 3, within one engagement relationship.

6.2.3 Conduct standards, independence and the integrity of attestation

Externalised assurance is only worth more than internal audit if the external party is genuinely external. The Department therefore proposes conduct standards for providers, set in the Verification and Accreditation Framework and made criteria for accreditation under section 84(2)(a), so that a breach is a ground for suspension or

revocation under section 84(2)(b). Independence comes first, and the Department proposes the following working position for consultation. A provider must not attest arrangements that it, or an entity in the same group, designed, implemented or operates: an AAP that supplies a foundation's hosting, administration or data management services cannot attest the controls over those services, because the self-review threat is not manageable by disclosure. Where a group has separate practices, the separation must be structural rather than declared. The provider and its relevant persons must hold no material interest, and the engagement partner and team no financial or personal interest, in the foundation, the asset, its founder or dedicators, its council members or, and the engagement partner and team must be free of financial or personal interest in the foundation, its dedicators and its principal counterparties. Fee arrangements are a further threat, and two standards address them. On remuneration, fees are fixed in advance, and no fee may be contingent on or linked to the outcome of an engagement, including the level achieved or the completion of registration. On concentration, a provider must disclose to the Department where a single client group or introducer accounts for more than a prescribed share of its engagements, and may not exceed a higher prescribed share.

Two supporting mechanisms are proposed. First, disclosure: each attestation records the provider's other engagements with the foundation and its group, so that a counterparty reading the register can see what else the attesting firm does for the entity it attests. Second, rotation and cooling-off, following established audit practice: the engagement lead rotates after a prescribed number of consecutive accreditations of the same asset, and no individual assesses a foundation for which they have worked within a prescribed period, with the periods set at standards tier where they can be calibrated against market capacity. Consultees are invited to comment on both, and in particular on the rotation and cooling-off periods.

The consequences of a defective or false attestation run through two channels, and the distinction matters. The provider-facing channel is the Department's process for suspending or revoking a provider's accreditation under section 84(2)(b), with the public register of providers under section 84(2)(c) recording the outcome; a provider whose accreditation is withdrawn cannot issue or renew data asset accreditations, and the foundations it serves must appoint another. The asset-facing channel is the accreditation itself: an accreditation obtained on a defective attestation is liable to suspension or revocation in the circumstances the framework specifies under section 85(2), engaging the remediation machinery at 6.4 for the asset concerned. Financial and other sanctions are a matter for the separate sanctions instrument, which is outside the scope of this paper; the framework's own contribution is that both channels are visible on public registers, so a provider's record and an asset's status are equally checkable.

6.2.4 Changing provider, continuity and appeals

The obligation to appoint an AAP under section 84(3)(a) is continuous, but it does not tie a foundation to one provider. A foundation may change provider at any time — on rotation, on dissatisfaction, on a change in the asset's assurance needs, or because the incumbent's own accreditation has been withdrawn — and the framework's concern is only that the change does not create a gap. Two propositions follow. The accreditation itself is unaffected by a change of provider: it attaches to the asset, not to the firm, and runs to its expiry. The incoming provider performs a handover verification within a

defined window, establishing the basis on which it will renew and identifying anything the outgoing provider's work leaves unresolved; the change and the handover are recorded in the assurance evidence and event history, so that a pattern of provider churn is visible to counterparties rather than concealed by it. Where a provider resigns or its accreditation is suspended or withdrawn mid-cycle, the foundation has a defined period to appoint a replacement, and failure to do so is referred through the prescribed review, suspension or revocation process. It does not silently create a second expiry date.

The third implementing instrument, the minimum viable enforcement regulations, will provide the internal reconsideration procedure required at launch. This is a commencement dependency independent of the later development of the wider sanctions regime. Registrar decisions will carry reasoned notices and access to reconsideration by an officer uninvolved in the original decision, with ordinary and expedited deadlines and any lawful interim measures specified in that instrument. The process for the Department's decisions on a provider's own accreditation, specified under section 84(2)(b), will likewise give reasons and access to internal reconsideration. Section 91 is an original High Court jurisdiction, not a statutory appeal; judicial review and urgent court relief remain distinct and available where applicable. No statutory ADR scheme under section 92(3)(n) or appeal under section 92(3)(o) is assumed at launch. A provider's professional refusal to issue or renew is not automatically within Registrar reconsideration; applicable contractual and court routes remain available. A challenge does not itself extend an accreditation, stop the remediation clock or permit prohibited use. Future appeal or ADR arrangements require the appropriate instrument.

6.2.5 Liability, insurance and the limits of an attestation

An attestation is worth what stands behind it. A counterparty relying on a Level 2 attestation, and a lender pricing a facility on the strength of it, are relying on a professional judgement formed by a private firm. The framework should be explicit about the consequences of that judgement being wrong and about the resources available to meet them.

On insurance, the Department proposes that the accreditation criteria under section 84(2)(a) require a provider to hold and maintain professional indemnity cover to a minimum set at standards tier, scaled to the levels the provider is accredited to deliver and to the classification of the assets it attests. A provider that allows its cover to lapse ceases to meet the criteria on which its accreditation was granted, engaging the Department's process for suspension or revocation under section 84(2)(b).

On liability, the Department's working position is that the Regulations should identify the heads of liability rather than leave the position to be settled case by case, and that a provider should owe a duty in respect of its attestation to the foundation that appoints it and to the data asset registrar. Whether that duty should extend to third parties who rely on a register signal without any relationship with the provider is the harder question. An unlimited class of claimants would be uninsurable and would deter entry to a market the regime needs; a duty owed only to the appointing foundation gives the relying counterparty nothing. The Department's provisional preference is a duty owed to the foundation and to the registrar, with a proportionate cap set at standards tier by reference to the level and the scope of the engagement, and no relief for fraud, wilful

misconduct or gross negligence — the floor the Act itself applies to data enforcers at section 87(2) and to council members at section 88(3).

Two limits on what an attestation claims follow, and both belong on the register rather than in inference. An attestation speaks as at its date and to the scope of the profile applied; it is not a continuing warranty of conformity, and the assurance record at 6.3.2 records date, scope and qualifications precisely so that a reader can see what has and has not been examined. And an attestation is not an assumption of the council's duties: the provider evidences, the council remains accountable.

6.3 The assurance ladder

The framework organises assurance into a ladder of four levels. The ladder is the regime's transparency instrument: the results of each level are marked on the register, so that the depth of verification behind any asset is visible to its market rather than asserted by its holder. It is also the assurance bridge for the phased Verification Agent described in Part 7.5: work the Agent cannot yet perform is carried by professional attestation, and migrates to automation, item by item, as the Agent's specification matures — without the register-facing meaning of any level changing.

Level	What is verified	Form and cycle	Register effect
Level 0 — Provisional registration (baseline)	Registrar validation of the completeness and formal integrity of the application through the staged registration process (ss. 78–79). Carries no assurance claim about correspondence to reality and is not an accreditation.	Once, at acceptance of the application; revisited on amendment.	"Provisionally registered" status (s. 79(3)(a)). Never to be presented as an accreditation.

Level	What is verified	Form and cycle	Register effect
Level 1 — Registered information verification	An AAP verifies registered information within the applicable profile: existence, ABP correspondence, classification basis, custody and hosting. A classification depending on anonymisation requires the substantive independent assessment described at 5.8; the AAP evaluates the conclusion and may use appropriately scoped specialist work. Documentary existence checks alone do not establish the claim.	Point-in-time evidence, refreshed as required by classification and material change; its accepted currency supports the single accreditation period. Checks may migrate to deployed automation within its stated capability.	Component of one accreditation. Record evidence scope, assessor, date, accepted currency and limitations separately from the single statutory expiry.
Level 2 — Controls attestation	Implementation of DAR Code controls proportionate to classification, plus conformity of actual use with the declared purpose in the governance wrapper. Scope drawn from the applicable attestation profile at standards tier.	Periodic evidence supporting the single accreditation period; reassessment after material remediation or change.	Component of the data asset accreditation. Controls signal recorded, including profile applied and any qualifications.
Level 3 — Recognised external assessment	Full data management capability assessment of the foundation and its operating arrangements under a scheme on the Recognised Standards list — DCAM and CDMC being the first candidates for recognition.	On the recognised scheme's own cycle; deliverable only by an assessor holding the authorisation the scheme requires (for DCAM, EDM Association Authorised Partner status). Mandatory in the defined matrix cells described at 6.5; otherwise optional and market-driven, subject to the Departmental recommendation at 6.6.	External assessment entry in the attestation record, naming the scheme, version and assessor. The register field is scheme generic; recognition of particular schemes sits in the standards tier.

6.3.1 Mapping the ladder to the statute

Levels 1 and 2 together constitute the single data asset accreditation for sections 80(1)(b), 84(4) and 85(1). The AAP issues one accreditation identifier, scope and expiry date when satisfied on both components. Separate evidence dates do not create separately valid accreditations or independent expiry clocks. Level 0 is provisional registration only. For designated assets, a current Level 3 assessment is an additional condition and the accreditation expiry must not extend beyond its accepted currency. Earlier adverse findings or withdrawal of evidence use the prescribed review, suspension or revocation process. Optional Level 3 lapse is an evidence update without an automatic statutory consequence. A pending renewal does not extend accreditation beyond its stated expiry.

6.3.2 Signals, and the naming discipline

Every assurance event records the level, scope or profile, assessor identity and accreditation reference, assessment date, accepted currency, and qualifications or limitations. The register separately records the statutory accreditation's identifier, scope, status and single expiry. Level 1 evidence must not be presented as controls assurance, and neither component alone may be labelled an accreditation. Evidence updates do not silently change statutory status; expiry, suspension and revocation are recorded through their prescribed processes. Governance signals remain the separate commercial-intent, AI-use, sector and residency declarations described in Part 3.4.2.

6.4 Accreditation and register standing: the statutory position

6.4.1 Accreditation is binary

Section 85(1) is categorical: a data asset foundation must not utilise a data asset unless there is a valid data asset accreditation in respect of that asset. There is no graduated state in which an asset with a lapsed accreditation may continue in qualified use, and the framework does not create one. The Act treats accreditation as existential twice over. Prospectively, an asset cannot complete registration — and so cannot attract the personal property right under section 80(4) — without confirmation of an accreditation (section 80(1)(b)); the dedication instrument carries the reversion confirmation required by section 76(2)(f), whose interaction with post-registration remediation is addressed at 6.4.3. Retrospectively, an asset whose accreditation is revoked or expires enters a prescribed remediation pathway at the end of which, absent restoration, the Registrar must remove it from the register (section 85(8)) — upon which the property right is extinguished (section 81(8)) and the disposal and reversion cascade in section 81(3) applies.

6.4.2 The remediation pathway

Where an accreditation is revoked or expires, the sequence prescribed by section 85 is as follows. The Registrar updates the register to record the suspension, revocation or expiry (section 85(3)) and, on revocation or expiry, marks the asset as subject to remediation (section 85(4)). While the asset is in remediation: the prohibition on utilisation continues to apply (section 85(5)(a)); the personal property right vested

under section 80(4) remains in effect (section 85(5)(b)); and the foundation must, within the remediation period, provide the Registrar with confirmation of a valid accreditation (section 85(5)(c)). The remediation period is 90 days, or such other period as the Regulations prescribe for specific categories of asset (section 85(6)); the Registrar may extend it once, by up to a further 90 days, on written application by the council where satisfied there are reasonable grounds (section 85(7)). If a valid accreditation has not been provided when the period, including any extension, expires, the Registrar must follow the prescribed process to remove the asset from the register (section 85(8)).

Three features of this design deserve emphasis for consultees. First, the preservation of the property right during remediation (section 85(5)(b)) is what makes the pathway a genuine cure period rather than a cliff edge: title is undisturbed while use is suspended, without guaranteeing the continuing effect or value of any security interest, and the register makes the asset's status transparent to anyone pricing it. Second, the fixed period with a single bounded extension gives every counterparty a calculable worst case. Third, the endpoint is not discretionary: section 85(8) is expressed as a duty, and the framework will not present continued registration without accreditation as an available state. The commercial significance of accreditation currency — and of choosing renewal cycles that a foundation can actually sustain — follows directly.

6.4.3 Reversion and preservation during prohibited-use periods

The Department's drafting baseline distinguishes initial registration failure from subsequent accreditation lapse and preserves lawful custody and remediation during all relevant prohibited use periods, including suspension. Section 76(2)(f)'s reversion confirmation must be reconciled with the preservation of the registered property right under section 85 and the disposal rules under section 81. The intended treatment permits acts strictly necessary for custody, security, integrity, compliance with data protection law and obtaining accreditation, while preventing commercial exploitation. The Attorney General's Chambers will be consulted on the legal construction, dedication wording and enabling route; this paper proceeds on the policy assumption that the treatment can be given effect, without presenting that advice as received. If the route is not confirmed, the Department intends to include the necessary primary-law change in the twelve-month amendment programme, subject to the scope and timing of section 92(6) and the required legislative process. Guidance cannot narrow the Act, and the intended exception must have legal effect before operational use relies on it.

6.4.4 Suspension

Section 85(2) provides that an accreditation may be suspended or revoked in the circumstances set out in the data governance framework, and the register records suspension (section 85(3)); the High Court may also order suspension or revocation (section 91(2) and (5)). The Act attaches the remediation machinery to revocation and expiry but not, in terms, to suspension. The framework will treat suspension for what it is: a state in which the accreditation is not valid — so the section 85(1) prohibition applies, subject to the preservation carve-out proposed at 6.4.3 — but which is designed to be lifted by the suspending authority on defined conditions rather than cured by re-accreditation. The DGF Regulations will specify suspension grounds, competent decision-makers, review, maximum duration and lifting or revocation conditions, with the

DAR Regulations recording the resulting events and consequences, so that suspension cannot become an indefinite twilight state.

6.4.5 Signals and standing: the two layers restated

The register distinguishes registration status, accreditation status and assurance evidence. Accreditation may be valid, suspended, revoked or expired; expiry and revocation engage the section 85 remediation pathway, while suspension has its own prescribed review process. Evidence records and governance signals may change without a change in statutory status. An expired or suspended accreditation must never appear as valid, and a scheduled expiry must be reflected from the recorded date rather than waiting for a council report. Prompt authenticated event notifications support accurate status recording.

6.5 The Level 3 mandate

6.5.1 The mandate and its trigger

For most assets, Level 3 is a market instrument: obtained where counterparties value it, priced accordingly, and signalled on the register. For a defined set of assets it is mandatory. The Department proposes that data assets whose classification falls within defined cells of the two-axis matrix — broadly, widely distributed assets containing identifiable special category personal data, together with assets carrying a designated sectoral overlay signal at or above a specified distribution scope — must hold a current assessment under a scheme on the Recognised Standards list as a condition of their accreditation. The schemes proposed as the first entries on the Recognised Standards list are the DCAM assessment and CDMC. The trigger is deliberately the constitutive classification itself, not a separate “high-risk” designation: the matrix already applies to every registered asset, is set at registration, maintained through the amendment regime, and leaves no uncertainty about whether an asset falls within the mandate.

6.5.2 How the mandate binds

For designated assets, Level 3 is an additional accreditation condition under the framework's section 69(c) requirements. The AAP must set the single accreditation expiry no later than the end of the required assessment's accepted currency. If renewal is not completed by that date, ordinary expiry and the section 85 remediation pathway apply. Earlier withdrawal or adverse evidence is notified promptly and handled through the prescribed review, suspension or revocation decision. There is no separate Level 3 statutory expiry clock and no automatic extension while renewal or a dispute is pending.

6.5.3 What the mandate means in practice

A foundation in a designated profile must plan for a recognised external assessment (DCAM or CDMC), allow for the assessor's timetable and budget for it alongside Levels 1 and 2. The AAP must align the single accreditation period to the accepted currency of all required evidence. Example A illustrates how classification and any designated health overlay must both be considered; restricted distribution alone does not settle whether Level 3 is mandatory.

6.6 The Departmental recommendation for the initial cohort

For foundations whose assets fall outside the mandated cells, Level 3 remains formally optional. The Department nonetheless makes an active recommendation: foundations in the initial cohort are strongly encouraged to obtain a recognised external assessment under a scheme on the Recognised Standards list within their first accreditation cycle.

The reasoning is candid. The regime is new. Its central claim — that a registered data asset carries governance a counterparty can rely on — will be tested first by the earliest assets and the earliest foundations, and the credibility of the whole register rides on those early tests. An external assessment under an internationally recognised scheme, conducted by an authorised assessor and marked on the register, is the strongest available answer to the counterparty who asks why an Isle of Man register entry should be trusted before the regime has a track record. The recommendation is a credibility mechanism for the regime's early years, not a permanent feature: the Department expects to review it at the statutory three year review point under section 94, described in Part 7.4, by which time the register's own record should carry the weight.

The recommendation is a steer, not a rule, and the Department is aware that its calibration is contestable from both directions. Some respondents will argue that if external assessment matters for credibility it should be mandatory for the entire initial cohort; others will argue that any Departmental steer distorts a mechanism designed to be market driven, and that counterparties can price the presence or absence of a Level 3 signal for themselves.

6.7 Phasing and market readiness

A mandate must be serviceable by the market that satisfies it — and, for this regime, that market already exists. Level 3 work under the first candidate schemes is conducted by assessors holding the scheme's own authorisation, and the EDM Association maintains an established international network of around fifty Authorised Partners licensed to deliver DCAM assessments and engagements.

Phasing is therefore a matter of onboarding rather than market creation, and onboarding includes the Department's fitness and propriety assessment of each provider (6.2.1). Before the mandate commences, the Department must have accredited an initial cohort of AAPs under section 84, the attestation profiles at standards tier must be in operation, and Authorised Partner capacity must be committed to Isle of Man engagements alongside existing client work. The commencement date for the mandate will be set in the Regulations, informed by the consultation responses, in particular by evidence from assessment firms on capacity and timetable. Until the mandate commences, assets in the mandated cells register on the statutory floor (Levels 1 and 2) with the Departmental recommendation applying with particular force, and the register signal makes the position transparent to counterparties in the ordinary way. Transitional treatment of the first cohort follows the same logic: assets registered before the mandate commences, and before the Verification Agent is deployed, take their first annual renewal on the calendar described in the forthcoming worked attestation profile in Annex D with the interim checks the deployed capability of the day can support. The same phasing logic governs the Verification Agent: under the phased capability path described at Part 7.5, items within Levels 1 and 2 migrate from professional attestation to machine verification

as the Agent's specification at standards tier advances, without the register facing meaning of either level changing.

6.8 Recognised equivalent standards

Foundations, dedicators and their advisers do not always arrive at the regime empty handed: many hold, or operate under, existing certifications and assessments. The framework recognises this in two distinct ways, and the distinction matters. For Level 3, recognition operates at scheme level: the Recognised Standards list will name the external assessment schemes whose results may be recorded as a Level 3 signal, with DCAM and CDMC proposed as the first entries. For Levels 1 and 2, recognition operates at evidence level: attestation profiles at standards tier will specify the extent to which current certifications and assessments — ISO/IEC 27001 for information security management, the ISO 8000 series for data quality, SOC 2 reporting on relevant trust criteria, DCAM and CDMC for data management capability and controls — may be credited as evidence within an engagement, reducing duplication of assessment effort without outsourcing the provider's statutory satisfaction under section 84(4).

The distinction between the levels is one of object, not of standard family. Level 1 assures facts: the registered information corresponds to reality. Level 2 assures controls: DAR Code controls are implemented and operating for the asset. Level 3 assures capability: the foundation's data management operating arrangements as a whole. External standards are evidence inputs to those objects, not definitions of them, and each candidate sits closer to one object than another: an ISO/IEC 27001 certification evidences the security slice of Level 2's controls scope; a SOC 2 report evidences control operation over a period against defined criteria; ISO 8000-family conformity evidences data quality items within an attestation profile; a DCAM assessment addresses whole-of-organisation capability and so belongs at Level 3. Like an ISO/IEC 27001 certification, however, it may also be credited within Level 2 profiles for the organisation-wide controls it covers, and at Level 1 it may support the provider's reliance on the foundation's own records; it does not verify the facts of a particular asset or the operation of controls over it. An assessment of a service provider may be credited in the same way, to the extent that its scope covers the arrangements serving the asset. CDMC deliberately spans the line — it is a controls framework assessed and certified at business level — and is treated accordingly: credited as evidence within Level 2 profiles where a current certification covers the relevant controls, and recognised at Level 3 where deployed as a whole-of-business assessment. Because the levels are defined by object, crediting a standard at one level says nothing about the others, and the boundary between the levels does not move as the list evolves.

Neither form of recognition substitutes for the data asset accreditation. A foundation certified to ISO/IEC 27001 still requires Levels 1 and 2; a foundation holding a DCAM assessment still requires them; recognition determines what an engagement may take as read/evidence, not whether the engagement happens. For each credited standard, the attestation profiles in the Verification and Accreditation Framework will state the scope, version and currency on which an engagement may rely and, for a capability assessment such as DCAM, the minimum rating required for each relevant capability. The Recognised Standards list and the crediting rules will be maintained through the standards making process described in Part 3.1, so that the list can track the evolution of

the standards landscape — additions, new versions, withdrawals — without amendment of the Regulations.

The list, like the crediting rules, is also expected to track the emerging AI assurance landscape. Consultees are invited to comment on which AI assurance standards should be considered for foundations whose assets serve AI training and deployment, and on whether they are better recognised at Level 3 or credited as evidence within Levels 1 and 2.

6.9 International interoperability: a phased path

The Act contains, at section 82, a mechanism for recognising data registers established under the laws of other jurisdictions as equivalent data registers, whose assets may enter the Isle of Man register on an expedited basis. The Department does not propose to bring that mechanism into use at launch. Equivalence is a judgement about another jurisdiction's entire assurance architecture — its establishing laws, the accreditation required before registration, the functioning of its registrar, the information its register makes available and the oversight applied to it (section 82(4)) — and there is at present no comparable register against which that judgement falls to be made. The mechanism remains on the statute book as the long-term interoperability route; no equivalence designation will be made in the first phase, the regime launches with the domestic register only, and every asset enters through the accreditation pathway described in this Part.

The interoperability instrument the Department does propose to develop, for launch in phase two, is the data asset passport: a portable, machine-readable representation of a registered asset's governance state — its classification, accreditation status, governance signals and attestation history — that a counterparty, lender or overseas register can consume without interrogating the Isle of Man register directly. The passport inverts the equivalence question. Rather than asking whether another register's assurance can be trusted here, it packages this register's assurance so that it can be verified elsewhere, carrying the regime's assurance story outward in a form other frameworks and markets can consume. Specification work on the passport sits naturally in the standards tier alongside the Verification Agent roadmap.

Part 7: Oversight and the actors in the ecosystem

The preceding Parts have described a regime in which most of the work of data governance is done constitutively: by the register, the classification system, the Asset Boundary Profile, the governance wrapper and the accreditation requirement, rather than by an authority telling foundations what to do. This Part completes the picture. It describes how conformity with those constitutive requirements is observed, how departures from them are detected and responded to, and which actors carry those functions.

The starting point deserves to be stated plainly, because it is a deliberate design decision and not an omission: the Act creates no new regulator. There is no supervisory authority for data asset foundations, no licensing body for their activities, and no public office with a general discretion to direct or discipline them. Oversight is instead distributed across a set of actors, each holding a defined and limited function: the council of the foundation itself, as the normal first responder, subject to independent notification and urgent-action duties; the data enforcer, a mandatory private law office within each foundation's own governance; the data asset registrar, an administrative custodian of the register; the Department, as steward of the framework; automated verification infrastructure, within its published capability; the accredited assurance providers described in Part 6; the Information Commissioner, whose existing supervision of personal data processing is unchanged and is described in Part 5; and, as the terminal venue for contested matters, the High Court.

In the three category presentation of the framework's instruments introduced at Part 3, this Part is the consolidating treatment of Category 2 — Other Actors in the Ecosystem. Two Category 2 subjects have already received dedicated Parts because they carry distinct external interfaces: the Information Commissioner (Part 5) and the Accredited Assurance Provider (Part 6). This Part addresses the remaining actors — the data enforcer, the registrar, the Department, the Verification Agent and the court — and then shows how all of them, together, produce oversight of the whole.

7.1 Oversight without a regulator

Three considerations drive the decision not to create a regulator, and they are worth setting out.

First, the regime already sits within a supervisory landscape. Personal data processing by a data asset foundation is supervised by the Information Commissioner in exactly the way it would be for any other controller; nothing in the regime dilutes that supervision, and section 69(b) of the Act requires the framework to specify the Commissioner's role expressly. Creating a second public supervisor whose remit overlapped the Commissioner's would blur, rather than strengthen, accountability — the demarcation position is set out in Part 5. Where a foundation's activities engage other regulated perimeters (for example financial services), the relevant existing regulator's jurisdiction is likewise untouched.

Second, foundations law already supplies an oversight tradition that does not depend on a regulator. The Foundations Act 2011 polices the conduct of foundations through a combination of internal offices with legal duties, persons with sufficient interest who

may bring matters before the court, a registrar with administrative functions and the supervisory jurisdiction of the High Court. The data asset foundation regime extends that model rather than departing from it: the data enforcer is a specialisation of the existing enforcer concept, and section 91 extends the court's powers to the specific subject matter of data assets.

Third, the architecture reduces the need for supervision by design. Where a conventional regime relies on a supervisor to discover whether an organisation is doing what it should, this regime makes the material facts observable: registration status, accreditation status, remediation status and classification are register states, visible to the persons who deal with the foundation. A counterparty, lender or dedicator does not need a regulator's opinion of a foundation's governance; the register discloses it. Much of what supervision exists to achieve — the alignment of conduct with stated commitments, visible to those affected — is delivered by transparency and by the accreditation requirement in section 85, which makes utilisation of an unaccredited asset unlawful without any authority needing to intervene.

The absence of a regulator does not mean the absence of consequence. The Act attaches specific offences to specific failures — failure to have a registered agent and resignation in contravention of the statutory process (sections 28(5) and 28A(7) of the 2011 Act), failure to notify a mistake in the register (sections 83(9) and 83(10)), and failure to give the accredited assurance provider reasonable assistance (section 84(6)) — section 85 suspends the ability to utilise an asset whose accreditation is not valid, the registrar's removal processes operate on prescribed statutory grounds, and the High Court may make orders and give directions under section 91. There is also a route by which a framework failure serious enough to put the entity's character in question reaches the assets: compliance with this framework is constitutive of data asset foundation status (section 68(1)(c)), and where a failure of those requirements is not remedied within the period the registrar specifies, the registrar may remove that foundation's data assets from the register (section 68(5)). What the design withholds is a general supervisory discretion vested in a public office; what it provides instead is a defined pathway for every detectable failure.

The normal response pathway and direct duties

The council is the normal first responder and the Data Enforcer the normal escalation actor where the council does not resolve a matter. This sequence does not delay statutory notification or urgent protective action. Section 83 duties to notify mistakes without undue delay apply independently of any council cure period. Direct recourse remains available where an actor is unavailable, conflicted or implicated. Accreditation-status events are notified promptly through authenticated channels; scheduled expiry is driven by the recorded expiry date. The instruments must reconcile routine filing periods with these duties. The Registrar applies its prescribed processes and the courts retain their jurisdiction; reconsideration under the third instrument does not itself stop a statutory clock or authorise prohibited use.

The boundary around private-law offices

A distributed model that relies on offices within the foundation's own governance raises a legitimate question of principle: whether functions that look supervisory should be

carried by privately appointed officers at all. The framework's answer is that they are not — because the data enforcer's functions, properly characterised, are not supervisory in the public law sense. The data enforcer holds no rule-making power, no power to impose penalties, no discretion exercised in the public interest, and no authority over any person other than through the ordinary routes private law provides: the duties owed to it under the Act and the framework, its statutory standing to bring matters before the registrar or the court and the court's judgment. It monitors the council's conduct against commitments the foundation itself has made — its instrument, its rules, its dedication instruments and its registered governance wrapper — in the same way the enforcer under existing foundations law monitors the council against the foundation's objects. Coercive outcomes are reserved throughout to statutory processes and to the court. The framework's instruments are drafted to hold that line, and the drafting notes in this Part identify the points at which it must be watched.

7.2 The data enforcer (sections 86 and 87)

The nature of the office

Every data asset foundation must appoint a data enforcer (section 86(1)). The office is modelled on the enforcer in existing Manx foundations law — a private law office within the foundation's governance, holding duties in respect of the foundation's compliance with its own constitutive commitments — but specialised to the data governance content of the regime. Section 86(7) disapplies section 14 of the 2011 Act for data asset foundations: the data enforcer replaces, rather than duplicates, the general enforcer for this class of foundation. Section 86(8), with the amendment to section 3, makes the data enforcer a person with sufficient interest, which is the source of its standing before the court under Part 5 of the 2011 Act and section 91.

The data enforcer must meet the criteria, and has the functions, set out in the data governance framework (section 86(2)), and must act in accordance with the framework's requirements when exercising them (section 86(3)). The council must cooperate with and assist it (section 86(4)), and it may disclose information received in the performance of its functions to the registrar (section 86(5)). Regulations may confer further functions (section 86(6)(a)) and may establish a reporting framework for assessing compliance (section 86(6)(b)).

The functions proposed

The framework proposes that the data enforcer's functions comprise:

1. reviewing, at the prescribed intervals and against the prescribed scope, the council's conduct of the foundation's affairs relating to its data assets against the foundation instrument, the foundation rules, the requirements of the framework and the terms of the registered governance wrapper, and acting on reasonable grounds where a departure comes to its attention, whether through that review or otherwise;
2. acting as the normal escalation point for detected non-conformities, including Verification Agent alerts and assurance provider qualifications, that the council does not resolve within the applicable period, including the remediation period

under section 85, without delaying independent notification duties or urgent action;

3. verifying that amendments giving effect to data subject rights, made under the amendment ground described in Part 5, have in fact been given effect in the asset;
4. notifying the registrar of mistakes in the register of which it becomes aware in performing its duties (section 83(5)); and
5. reporting under any reporting framework established by regulations (section 86(6)(b)). The intervals at which the review is carried out, and the events and documents within its scope, are prescribed in the Data Enforcer review standard (Category 2), and are calibrated to the classification of the assets the foundation holds rather than set at a single frequency for every foundation. The duty is bounded in the same terms as the protection at 2.4: a data enforcer is not liable for failing to detect a matter that a review conducted in accordance with the prescribed scope and intervals would not have revealed. The bound operates as a floor rather than a ceiling — a departure that comes to the enforcer's attention between scheduled reviews is to be acted on when it does.

What the office is not

The data enforcer is not a regulator, and the framework is drafted so that it cannot come to function as one. It is not an agent, delegate or informant of the registrar, the Department or the Information Commissioner: its duties run to the foundation's own legal framework. It is not a liaison with the Information Commissioner and it does not review data protection impact assessments. It does, however, have a notification route to the registrar, and that route is a duty rather than a discretion: where it becomes aware of a mistake in the register in the course of performing its functions it must notify the registrar without undue delay, and failure to do so is an offence (sections 83(5) and 83(10)). The framework should attach to that duty a protection from liability for notification made in good faith, and should state expressly that it imports no duty to investigate. Beyond that duty, its disclosure gateway to the registrar (section 86(5)) is a permission, exercised in the discharge of its own functions, and not a general reporting line. It has no power to penalise, to direct third parties, or to suspend or revoke anything; where it cannot secure remediation, its recourse is to put the matter before the registrar's prescribed processes or the court, where the decision is made by the body with authority to make it. And it exercises no supervision of the processing of personal data, which remains exclusively with the Information Commissioner.

Independence, qualification and liability

The value of the office depends on its independence from the council whose conduct it reviews. The framework proposes qualification criteria under section 86(2) directed at competence and independence — including restrictions on council members and connected persons holding the office — with appointment, retirement, removal and remuneration to be addressed under the regulation making power at section 92(3)(t) so that the council cannot remove an enforcer for doing its job. The Department's proposed approach is to leverage the EDM Association's training programme and provide a mandatory accreditation of data enforcers to ensure they have the

understanding of the data governance framework to provide the service. Section 87 supplies the liability floor: nothing in the foundation's documents, the framework or any contract can relieve the data enforcer of liability for fraud, wilful misconduct or gross negligence (section 87(2)), while section 87(3) protects it from liability for the foundation's own defaults absent consent, connivance or neglect.

Section 92(3)(s) contemplates regulations conferring on data enforcers powers equivalent to those in section 14 — to require the council to account for the administration of data assets, and to sanction or authorise council actions that the foundation rules would not otherwise permit. Whether those powers should be conferred, and with what conditions, is a genuine design question on which the Department has not settled a position. Conferring them strengthens the office's ability to secure remediation without litigation; it also moves the office closer to the supervisory character the design otherwise avoids.

For data protection purposes, the data enforcer is a controller in its own right of the personal data it processes in performing its functions, because it exercises independent judgement rather than acting on the foundation's instructions; it is not the foundation's processor. The controllership map in Part 5 carries a distinct row to this effect.

Protected disclosure to the data enforcer

The distributed model depends on departures being detected. The Verification Agent detects what can be mechanised, the assurance provider detects what an engagement examines, and the data enforcer detects what comes to its attention in the discharge of its functions. None of those routes reaches the thing most often known first by someone inside the arrangement: that a control is not operating as attested, that an entitlement has been granted outside the wrapper, or that the register no longer describes the asset.

The framework therefore proposes a protected disclosure route to the data enforcer. A person who is or has been a council member, an officer or employee of the foundation, an employee of its administrator or of a service provider, or a member of the data enforcer's or the assurance provider's engagement team, may disclose to the data enforcer a reasonable belief that the foundation has contravened the framework, that information given to the registrar or to an assurance provider is inaccurate, or that a matter has been concealed from either. The disclosure is protected: the foundation must not subject the person making it to any detriment for having made it, and a provision in a contract or in a foundation document purporting to preclude such a disclosure is to that extent of no effect.

The enforcer triages what it receives. A disclosure is not a finding, and the response follows the ordinary pathway: the enforcer raises the matter with the council as first responder and normally escalates to the registrar's prescribed processes or to the court if the council does not resolve it. Independent notification duties and urgent action proceed in parallel; direct recourse is available where the council or enforcer is unavailable, conflicted or implicated. The identity of the person making a disclosure is not to be communicated to the council except with that person's consent or where disclosure is required by law, and the enforcer records the fact of the disclosure and its disposal in any reporting required under section 86(6)(b).

The route displaces nothing. Disclosures about the processing of personal data belong with the Information Commissioner, disclosures about a regulated activity with the regulator of that activity, and nothing proposed here limits any protection a person has under employment law or otherwise.

7.3 The data asset registrar (section 77)

The data asset registrar is appointed by the Department (section 77(1)) and holds office in accordance with the terms of appointment (section 77(2)–(4)). Its statutory functions are to establish, keep and maintain the data asset register in the prescribed form (section 77(5)) and to charge prescribed fees (section 77(6)). Around that core, the Act assigns it the administrative functions of the registration lifecycle: accepting applications and recording provisional registration (section 79); completing registration where the requirements are met, and removing the provisional asset where they are not (section 80); recording accreditation status, marking an asset as subject to remediation, and following the prescribed removal process where remediation fails (section 85(3), (4) and (8)); updating the register, including the "under review" status and the correction of mistakes (section 83); and effecting removal in the further circumstances the Act and regulations provide (sections 68(5) and 81, and such circumstances of non-compliance as may be prescribed under section 86(6)(c)).

The remit is deliberately narrow, and the narrowness is the point. The registrar is the custodian of the register's integrity — the actor that keeps the constitutive record accurate, complete and trustworthy — and nothing more. It does not supervise the conduct of foundations or their councils. It does not adjudicate data protection compliance, or the validity of a data subject's request; its role at that interface is confined to recording the resulting amendment and verifying the integrity of the new asset state (Part 5). It does not manage, value or deal in data assets. And it does not accredit assurance providers: accreditation of providers is a function of the Department under section 84(1) and (2), with the registrar's involvement limited to the register-facing consequences of accreditation status. Where the registrar exercises the powers it does hold — notice and removal under section 68(5), removal under sections 80(3) and 85(8), updating under section 83 — it must comply with the requirements of regulations (sections 68(6), 83(7) and 85(8)), so that even the register integrity functions are exercised on prescribed grounds and process rather than at large.

Framed as oversight, the registrar's contribution is disclosure rather than direction. The status states the Act creates — provisionally registered, fully registered, under review, subject to remediation — are the regime's public signals of governance standing, maintained by the registrar and visible to everyone who deals with the foundation. Oversight by transparency is slower burning than oversight by directive, but it is also less discretionary, more predictable and self-enforcing in the place it matters most: the willingness of counterparties, lenders and dedicators to transact.

7.4 The Department

The Department for Enterprise is the steward of the framework rather than an operational supervisor. Its functions under the Part are legislative and administrative: it appoints (and may remove) the registrar (section 77(1) and (4)); it accredits assurance

providers against the criteria set out in this framework and the processes established in regulations, and maintains the public register of accredited providers (section 84(1) and (2)); it makes the regulations that carry the framework (section 92) and may issue guidance (section 93); and it must review the provisions of the Act relating to data asset foundations before the end of three years beginning with the day section 68 comes into operation, publish a report of its conclusions, and lay that report before Tynwald for its approval (section 94).

None of these functions involves directing a foundation, an enforcer or an assurance provider in an individual case. The Department's accreditation function under section 84 is the closest the regime comes to a public gatekeeping role, and it is confined to the assurance market: it determines who may provide accreditation services, on published criteria and process, and is treated in full in Part 6. The framework itself is subject to democratic control — regulations under the Part are subject to the affirmative procedure, with Tynwald approval required for the categories listed in section 92(10) — so that oversight of the oversight architecture rests where it should: with Tynwald, informed by the section 94 review.

7.5 The Verification Agent

The Verification Agent is infrastructure, not an office. It has no statutory personality, exercises no judgement, and carries no authority of its own: its specifications, attestation roots and failure mode handling sit in the standards tier, and its outputs take effect only by updating register state or by triggering escalation to the actors described above. It is the regime's mechanism for making verification efficient and continuous where verification can be mechanised — and only there.

The Agent is a Registrar-hosted staged capability and is not available at launch. AAP assurance and prescribed foundation evidence bridge that period. Initial automation addresses supported integrity, existence and parameter checks; semantic conformity and drift detection are later targets. Each check identifies actual inputs, observation time, scope and limitations and reports pass, fail, unavailable or inconclusive. Metadata-only access cannot support a claim that asset contents were inspected. Neither a successful check nor TEE attestation establishes complete inputs or universal compliance, and automated output takes effect only through the authorised workflow.

For data protection purposes the Verification Agent is not an actor at all: where it processes personal data within its trusted execution environment in performing integrity functions, that processing is attributed in accordance with the controllership map in Part 5.

7.6 The High Court (section 91)

Where a conventional regime would end in a regulator's enforcement discretion, this regime ends in the supervisory jurisdiction of the High Court — the terminal venue for matters that the council does not remediate and the registrar's prescribed processes do not resolve. Section 91 gives the court specific powers for data asset foundations, without prejudice to its existing powers under Part 5 of the 2011 Act: to order amendment of the foundation instrument or rules where that will assist the foundation to utilise its data assets or comply with the framework (section 91(1)); to order the

suspension or revocation of a data asset accreditation, or rectification of the register, where a person has failed to comply with the Act or the foundation's documents (section 91(2)); to give directions that will assist utilisation or compliance (section 91(3)); and to give directions or make orders concerning disputes over the utilisation of data assets or the practices of a foundation, on the application of a person with sufficient interest (section 91(4) and (5)).

Two features of section 91(4) matter to the oversight design. First, standing: the persons with sufficient interest include the data enforcer and the data asset registrar, so both the escalation actor and the register custodian can bring a matter to the terminal venue without depending on anyone else's discretion. Second, sequencing: the court's jurisdiction under section 91(4)(a) is engaged where the applicant has exhausted the alternative dispute resolution process to be prescribed under section 92(3)(n), or where the court is otherwise satisfied it is desirable to act — so that routine disputes are channelled to a proportionate forum first, and the court remains available where that process fails or urgency requires it.

7.7 The oversight pathway end to end

The table below states each actor's proposed oversight contribution and its limits in one place.

Actor	Oversight contribution	Source	Limits
Council	Normal first responder; operates controls and remediation; discharges its own notification duties without undue delay	ss.24, 88; s.83(4); s.85(5)–(7); framework instruments (Part 3)	Cannot self-certify conformity; evidence supplied by register state, verification and attestation
Data enforcer	Reviews council conduct at the prescribed intervals against the foundation's own commitments; acts on reasonable grounds on departures; normal escalation actor, without excluding direct statutory or urgent routes; standing before registrar processes and the court	ss.86–87; s.83(5); s.3 and s.86(8) (person with sufficient interest)	Private law office; no penalty, direction or rule making powers; no supervision of personal data processing

Actor	Oversight contribution	Source	Limits
Registrar	Custodian of register integrity; records status states (provisional, full, under review, remediation); removal on prescribed grounds	ss.77, 79–81, 83, 85; s.68(5)	Administrative; acts on prescribed grounds and process; no conduct supervision; does not accredit providers; no data protection adjudication
Department	Framework stewardship: regulations, guidance, provider accreditation, statutory review	ss.77(1), 84(1)–(2), 92–94	No case level direction of foundations, enforcers or providers; regulations subject to Tynwald control
Verification Agent	Machine verification of mechanically checkable conditions; outputs update register state or trigger escalation	Standards tier (specification); Part 6 (assurance bridge); Parts 2.5 and 7.5 (phasing)	Infrastructure, not an office; no judgement; capability bounded and honestly phased
Assurance provider	Independent professional assurance; issues and renews the data asset accreditation on which utilisation depends	ss.84–85; Part 6	Market supplied; accredited by the Department; independent judgement (controller in own right, Part 5); not an inspector or supervisor
Information Commissioner	Existing public supervision of personal data processing, unchanged	Data Protection Act 2018 and Applied GDPR; s.69(b); Part 5	Personal data remit only; demarcation and coordination per Part 5
High Court	Terminal venue: orders and directions, accreditation suspension or revocation, register rectification, dispute resolution	s.91; Part 5 of the 2011 Act	Engaged on application; no ADR process prescribed at launch, so s.91(4)(b) is the operative limb at commencement; internal reconsideration under the third instrument is available in the ordinary case without barring urgent court relief

A single worked pathway shows the chain in operation. A non-conformity is detected — by the Verification Agent within its capability, by an assurance provider in the course of an engagement, by the data enforcer in the discharge of its functions or by the council itself. The council is the first responder: it decides and executes remediation, using the amendment regime described in Part 4 where the register must change, and — where the failure is a lapse of accreditation — within the remediation period under section 85(5) to (7), during which the prohibition on utilising the asset applies. Independent notifications and urgent containment proceed in parallel; a council cure period does not postpone them. If the council does not resolve the matter, the data enforcer normally escalates: it may require the council to account (if the section 92(3)(s) powers are conferred), put the matter before the registrar where a register integrity or prescribed removal ground is engaged, or apply to the court under section 91. The terminal outcomes are those the Act itself prescribes: correction of the register, suspension or revocation of accreditation, removal of the asset from the register with the disposal and reversion consequences of section 81, or such other order or direction as the court considers appropriate. At every step, the actor deciding is the actor with authority to decide, and the record of what happened is register state.

Part 8: Roadmap

Q1 2027

Roadmap item	Description
Register a Data Asset Foundation	Establishing a Data Asset Foundation with the Central Registry, creating a separate legal entity with the structure needed to hold and govern data assets.
Use published guidance notes	Referring to published guidance and good practice on preparing, registering and maintaining data assets to a consistent standard.
Register data assets	Applying to register data assets on the Data Asset Register and completing the two-phase registration process.
Govern and utilise registered data assets	Managing and utilising registered data assets in accordance with the requirements set out in the Data Governance Framework and in the Data Asset Register and Registrar Regulations.

Q2 2027

Roadmap item	Description
Use the semantic layer for data assets	Describing registered data assets in a standardised, machine-readable form, creating a consistent basis on which assets can be interpreted and compared.

Q3 2027

Roadmap item	Description
Connect to the first integrated marketplace	Connecting registered data assets to the first integrated marketplace, opening new routes to market.
Use data asset passporting	Externalising the semantic layer through verifiable credentials and trusted issuance, giving other jurisdictions and commercial counterparties a machine-readable source of truth they can verify independently.

Q4 2027

Roadmap item	Description
Connect to additional marketplaces	Connecting registered data assets to further integrated marketplaces, widening access to new partners, customers and routes to market.

Future releases

Roadmap item	Description
Onboard and verify data assets more quickly	Using greater automation to reduce the manual steps involved in onboarding and verifying data assets.
Record security interests	Recording security interests over registered data assets to support clearer financing, ownership and risk arrangements.
Use a standardised Foundation model	Selecting a standardised Data Asset Foundation model built for a particular use case, with the operating structure, roles and governance arrangements already defined.
Rely on records held in equivalent registers	Using information and evidence from approved public or private registers that meet Data Asset Foundation requirements, reducing duplication and avoiding a second registration process.
Align with additional industry standards	Aligning registered data assets with further standards and frameworks to support broader recognition, interoperability and assurance.
Process sensitive data with additional protections	Handling sensitive data within a Foundation under enhanced security and confidentiality controls, for use cases that require them.

PLEASE NOTE: Roadmap items and timing are indicative and subject to change.

Annex A: Proposed Asset Boundary Profile Schema

Proposed content of the Asset Boundary and Material Change Standard [working title], published for consultation.

A.1 Purpose and status of this Annex

Every application to register a data asset must include an Asset Boundary Profile (the Profile). The Profile is the council's declaration of what the data asset is: what it consists of, the period and the sources it covers, where it sits in the classification matrix, what it is derived from, who governs it, and how far it may change while remaining the same asset. The personal property right conferred by section 80(4) of the Act attaches to the data asset as recorded in the Register, and the Profile is the part of that record which fixes the asset's boundary.

The Profile does three things. It defines the perimeter of the asset, stating what falls inside it and, as importantly, what falls outside. It gives the asset continuity of identity, by stating in advance which changes leave it the same asset and which would make it a different one. And it gives the accredited assurance provider, the Registrar and anyone relying on the Register a fixed description against which the asset can be checked. If the proposal in Part 4 for protection against interference with a registered asset is taken forward, the Profile would also mark the extent of what is protected.

This Annex sets out the proposed schema for the Profile. It is to be issued by the Department in the Asset Boundary and Material Change Standard [working title] (the Standard), a Category 3 instrument made under the Data Governance Framework Regulations (Annex B). The proposed content is published here so that it can be considered alongside this paper. Once the Standard is made, the schema will be maintained there alone and this Annex will be replaced by a reference to it, so that each requirement has a single home.

A.2 General rules for drawing the boundary

Defined by criteria. A data asset is defined by the criteria that decide whether any given record falls within it — its structure, its subject matter and its rules of inclusion and exclusion — rather than by a list of records or files. A closed, point-in-time snapshot may also be described by reference to its contents, but must still state the criteria.

One governance regime. A data asset is the largest body of data that operates under a single, uniform governance regime. Data that a foundation governs under more than one regime is registered as more than one asset.

One classification cell. Each data asset occupies exactly one cell of the classification matrix (Distribution Scope × Data Sensitivity). Data that would fall into more than one cell is registered as separate assets.

The asset as recorded. The property right attaches to the data asset as recorded in the Register, not to the underlying data as such. Two foundations may therefore register distinct data assets drawn from overlapping data, where the assets are sufficiently

distinct when their boundaries, classification, governance, foundations and provenance are taken together.

Proportionate description. Each attribute is described at the level of detail needed to identify the asset and to decide whether a change takes it outside its boundary, and no further. A justified statement that an attribute does not apply is always available.

A declaration by the council. The Profile is the council's declaration, made with the application and kept up to date.

A.3 The proposed seven attributes

For each attribute, this section states its purpose, the elements to be declared and the points to note. Every element is mandatory unless a justified statement is made that it does not apply.

A.3.1 Definitional scope

Purpose. Fixes what the asset consists of. It carries the most weight whenever it is disputed whether particular data forms part of the asset.

Element	What is declared
Structure	The logical schema or other structural definition of the data, identified by version. A published external schema may be referred to rather than reproduced.
Subject matter	What the data is about, stated precisely enough to distinguish the asset from other data held by the foundation.
Inclusion criteria	The rules that decide whether a record falls within the asset.
Exclusion criteria	What is expressly outside the asset, including similar or adjacent data held by the foundation.

The exclusion criteria matter as much as the inclusion criteria: a boundary stated only in positive terms invites dispute at its edges.

Where the data is or includes AI-generated data, the method of generation, the system used, the provenance of its inputs and any validation or curation after generation are described within this attribute, the provenance scope and the derivation rule. They are not an additional attribute.

A.3.2 Temporal scope

Purpose. Fixes the period the asset covers and whether it grows.

Element	What is declared
Temporal class	One of: (a) closed snapshot — fixed at a point in time, with no additions; (b) accreting series — open-ended growth within the asset's scope; or (c) rolling window — additions with programmed expiry or archiving.
Reference point	For a snapshot, the date and time at which it is fixed. For a series or a window, the point from which additions begin.
Window rule	For a rolling window, the period retained and the rule for expiry or archiving.

How fast the asset is expected to grow is stated in the growth parameter declarations, which form part of the change envelope (A.3.7).

A.3.3 Provenance scope

Purpose. Fixes where the asset's data may come from and how it enters the asset.

Element	What is declared
Permitted sources	The classes of source from which data may enter the asset, defined by criteria where the population of sources may change.
Entry channels	How data enters: direct capture, contribution by members, licensed ingestion, or derivation from other data.
Contributor eligibility	For a pooled asset, the criteria a contributor must meet.

For a pooled asset, who may contribute is part of what the asset is.

Data that enters outside the declared provenance scope does not enlarge the asset. It is removed or, where the change envelope provides for it, the Profile is amended.

A.3.4 Classification coordinates

Purpose. Places the asset in one cell of the classification matrix.

Element	What is declared
Distribution Scope tier	The asset's tier on the Distribution Scope axis.
Data Sensitivity tier	The asset's tier on the Data Sensitivity axis, which reflects the data protection status of the data.
Basis	A short statement of why the asset sits in that cell, sufficient for the accredited assurance provider to confirm it and for any later reclassification to be assessed against it.

The tiers and their definitions are set by the DAR Regulations and the Classification and Metadata Standard, not by this Annex.

A change of cell is always a material amendment and never requires a new registration: the asset keeps its Data Asset Identifier (DAI), its registration date and the licences and interests recorded against it.

The governance signals (Commercial Intent, AI Use Tier, Regulated Sector and Residency Tier) are recorded in Section 1 alongside the classification coordinates, but they are not part of the Profile (A.4).

A.3.5 Derivation rule

Purpose. Fixes how the asset is produced from other data, where it is derived rather than collected.

Element	What is declared
Sources	The data from which the asset is derived, whether or not that data is registered. A registered data asset is identified by its DAI; other data is described precisely enough to identify it.
Method	How the asset is produced from its sources, in enough detail for the accredited assurance provider to confirm it.
Refresh	Whether and how changes in the sources flow through: re-derivation on change, periodic refresh, or fixed at derivation.

An asset that is not derived from other data states that this attribute does not apply.

How a proprietary method can be described without disclosing it on the Register will be addressed in the Standard.

A.3.6 Governance status

Purpose. Fixes who governs the asset and under which rules.

Element	What is declared
Decision-rights holder	The organ of the foundation that holds decision rights over the asset, including the right to begin an amendment: the council, or a committee or delegate identified by role.
Governing rules	The rules, policy or rulebook that govern the asset, identified by version. Where permissions to use the asset are expressed in machine-readable policy, the reference identifies the policy regime and its version, not each permission.
Standing delegations	Any standing delegation of operational decisions, identified by role.

The Profile fixes the governing rules by reference and version, not the content of each permission. Changing a permission within the referenced version is not a change to the Profile; moving to different rules, or to a new version of them, is.

Roles are declared, not individuals, so a change in the membership of the council is not a change to the Profile.

A.3.7 Identity-preserving change envelope

Purpose. States in advance how far the asset may change and remain the same asset. It draws the line between a new state of the same asset and a different asset.

Element	What is declared
Growth parameter declarations	How the asset is expected to grow: (a) the maximum rate of growth in record volume in a stated period; (b) the number or range of contributing sources; (c) whether the temporal scope is rolling or fixed and, if fixed, its end date; and (d) the minimum and maximum intervals between updates.
Other declared changes	Any other changes declared to be within the envelope, for example planned schema evolution under which existing records remain valid, or changes in the contributors to a pooled asset.
Excluded changes	Changes declared to be outside the envelope, which would require a new registration.

Growth within the growth parameter declarations leaves the asset the same asset. The declarations must be reasonable and proportionate, having regard to the nature, size and purpose of the asset and to any historical pattern of growth; for a static asset they may state that they do not apply. Exceeding a declaration must be notified to the Registrar. The council then assesses whether the asset remains within its envelope: if it

does, it makes revised declarations by material amendment; if it does not, the change is beyond the envelope.

Some changes are within every asset's envelope: in particular, giving effect to a valid data subject rights request never by itself takes an asset outside its envelope, and a reclassification is always a material amendment.

The envelope should be drawn no wider than the council can evidence: each declared change is one that the council may be asked by the Registrar or the accredited assurance provider to justify. Any other change to an attribute is a change beyond the envelope.

A.4 What the Profile does not contain

Several matters recorded against a registered asset are deliberately kept outside the Profile, so that a change to them does not touch the asset's identity. The table below lists them.

Matter	Where it is recorded	Why it is outside the Profile
Governance signals: Commercial Intent, AI Use Tier, Regulated Sector, Residency Tier	Section 1 of the register record, alongside the classification coordinates.	They describe what is done with the asset and under what constraints, not what the asset is. A change is a material amendment, recorded against the entry without amending the Profile.
Declared purpose	The register record.	It states what the asset is for, not what it is. A change is a material amendment.
Accreditation status	A register state recorded under section 85(3) of the Act, in Section 5 of the register record.	It is a precondition of full registration and descriptive afterwards. It is not part of the asset's identity and is not a governance signal.
Fitness for purpose criteria	Assurance content recorded against the entry; the criteria are in the Data Quality Standard.	Conformity is assessed through assurance, not by amending the Profile.
The foundation in which the asset is vested, and the date and basis of vesting	Section 2 (Proprietorship).	A transfer changes who holds the asset, not what the asset is.
Licences, rights, interests, court orders and restrictions	Section 3 (Charges and Registered Interests), for information only.	Recording a dealing must never change the identity of the asset dealt with; otherwise granting security over an asset would alter the collateral.

Matter	Where it is recorded	Why it is outside the Profile
Integrity method	Recorded against the entry, separately from the Profile.	Kept outside the Profile so that a change of algorithm or method is not a change to the asset.
Descriptive metadata, contact and service details	Descriptive fields of the register record.	Updated without amending the Profile.

Annex B: Index of proposed DGF Framework Instruments

B.1 About this Annex

Section 3.1.1 sets out the headline instruments that make up the data governance framework. This Annex completes that list. It indexes every instrument in the framework family, including those that the paper names outside the tables in section 3.1.1, and the private instruments on which the framework relies.

How the instruments are grouped. The Data Governance Framework Regulations sit above the categories as the enabling instrument. Section 1.3 names two further statutory instruments in the family, model foundation rules and regulations under section 89, which are not placed in a category. Every other framework instrument sits in one of three categories, according to its principal subject: Category 1, Obligations of the DAF Council; Category 2, Other Actors in the Ecosystem; and Category 3, Data Asset Boundary and Material Change.

Categories are for navigation and are not exclusive. The "Read with" column in the table at B.2 gives the interlocking instruments, including those in other categories. Each new instrument made under the standards-making process will state its category in the instrument that makes it.

The tier test. Content that creates, alters or extinguishes a legal right, duty or power sits in Regulations. Operational or technical content within an enabling power sits in a Practice Direction or Standard. Purely explanatory content sits in a Guide Note.

Who makes the instruments. The Department makes the Data Governance Framework Regulations under section 92 of the Act, in discharge of its duty under section 69, and makes the Practice Directions and Standards under the standards-making process in those Regulations. It may issue Guide Notes at any time under section 93. Statutory powers remain with the Department; their exercise is delegated to the Registrar for administrative and operational matters and to Digital Isle of Man for policy and architecture. Technical standards are owned by Digital Isle of Man and published and maintained by the Registrar.

One rule, one home. Each requirement is set in one instrument and cross-referred to elsewhere, never restated. The DAR Regulations, for example, refer to the Asset Boundary and Material Change Standard for how the Asset Boundary Profile is declared and how a change is classified, rather than repeating it (Annex A).

Timing. The "Timing" column shows when each instrument is expected to be needed: at launch, when the Register opens in the first quarter of 2027; at a later stage, for staged capabilities; or still to be confirmed. It reflects the implementation plan in Part 8 and may change.

B.2 The proposed framework instruments

For each instrument the first column gives its tier, who makes it and its statutory basis.

Instrument	What it carries	Read with	Timing
Above the categories			
Data Governance Framework Regulations Regulations · Department, with Tynwald approval where s.92(10) applies · ss.69 and 92	Definitions; outcome duties; scope of application; transitional and review provisions; enabling powers for the Practice Directions and Standards; and the standards-making process itself. Includes the power under which the Asset Boundary and Material Change Standard is issued.	Every framework instrument. The DAR Regulations, which it cross-refers to but does not restate.	At launch
Further statutory instruments named in section 1.3 (not placed in a category)			
Model foundation rules Regulations · Department · s.74, with s.92(3)(v)	Default rules, deemed to be included where a foundation's rules are silent on a matter they cover and do not exclude them. An amendment does not affect a foundation established before it takes effect.	Foundation rules; Qualification Routes Standard	Later stage (to be confirmed)
Regulations on documents kept at the business address Regulations · Department · s.89 (supplementing s.41 of the 2011 Act)	Further documents and records that a data asset foundation must keep at its business address. The anchor for the Records Retention Standard.	Records Retention Standard	To be confirmed
Category 1: Obligations of the DAF Council			
Practice Direction 1 — Obligations of the Data Asset Foundation Practice Direction · Department · ss.69 and 88(2)(b)	The lead Category 1 instrument: the operational content of the foundation's residual duties and the foundation-side discharge of its constitutive obligations, including the duties on third-party rights within a dedicated asset (4.4.2). The council's obligations draw on DCAM and CDMC principles, expressed in the Department's own words.	Verification and Accreditation Framework (accreditation duties); Category 3 instruments (asset-side obligations)	At launch

Instrument	What it carries	Read with	Timing
Access Control and Information Handling Standard Standard · Department · s.69	Access controls aligned to the Distribution Scope axis; security duties that protect the integrity of the Register and reliance on it.	Classification and Metadata Standard (classification drives the controls)	At launch
Records Retention Standard Standard · Department · s.69; s.89 regulations	The retention schedule for the records of control kept by the foundation. The Registrar's own archive retention is set by the DAR Regulations.	Regulations on documents kept at the business address; DAR Regulations Part 5 (records of change)	To be confirmed (follows the s.89 regulations)
Publication Matrix Standard Standard · Department · s.69	Reporting and publication thresholds; the form and content of the foundation's annual report to the data enforcer. The Registrar's own publication duties are in the DAR Regulations (Part 9).	Data Enforcer review standard (receipt and use of reports)	Before the first annual reporting cycle
Qualification Routes Standard Standard · Department · s.88(1)	The routes by which the council qualification requirement may be met — professional qualification, recognised certification, demonstrated experience or a recognised course — so that more than one pathway works and qualified council members do not become a bottleneck (3.2, 4.1).	Data Governance Framework Regulations; foundation rules	At launch, as foundations are established
Category 2: Other Actors in the Ecosystem			
Verification and Accreditation Framework Standard (instrument home to be confirmed) · Department · ss.69(c), 84 and 85	The scheme for accredited assurance providers, including admission, conduct standards, rotation and withdrawal; the accreditation criteria and attestation profiles; the accreditation ladder, including the mandatory Level 3 provision; and the specification of the Verification Agent, which is staged. Incorporates the capability model applied by accredited assurance providers.	Practice Direction 1; Recognised Standards list; DAR Code controls; Data Quality Standard; DAR Regulations (recording under s.85(3), remediation, public register of providers)	At launch (needed for full registration)

Instrument	What it carries	Read with	Timing
Data Enforcer review standard Standard · Department · ss.86 and 87	The data enforcer's functions, conduct, standing and escalation pathways, and the intervals and scope of its reviews, calibrated to the classification of the assets held. The enforcer monitors at a prescribed cadence, within a prescribed scope and against prescribed events and documents, rather than continuously. The enforcer's duty to notify the Registrar, and its protection when it does so in good faith, are in the DAR Regulations.	Practice Direction 1 (cooperation duties); Publication Matrix Standard (annual report); DAR Regulations Part 5 (appointment, tenure and cessation)	At launch
Data Protection Interface Statement Guide Note · Department · s.93	Designed coexistence with data protection law: the controllership map, and the resolution pathways across the interface points in Part 5.	Practice Direction 1 (controller-side duties); DAR Regulations (data subject rights); Joint Guidance	At launch
Joint Guidance Guide Note (joint) · the Registrar with the regulators, jointly · s.93 and each regulator's own powers	Operational coordination between the Registrar and the regulators, as appropriate, so that there is no double penalisation and the boundaries with adjacent regimes are clear.	To be confirmed	To be confirmed
Recognised Standards list List kept by the Department (tier to be confirmed) · Department · s.69(c)	The external assessment schemes whose results may be recorded at Level 3, with DCAM and CDMC proposed as the first entries; revisable through the standards-making process (3.2.2, 6.8). Recognition does not make any statutory right depend on membership of a private body.	Verification and Accreditation Framework	At launch (cells where Level 3 is required)
DAR Code controls Control set (publishing instrument to be decided) · Department · s.69(c)	The Level 2 control set, proportionate to the asset's classification. The controls draw on DCAM and CDMC principles, expressed in the Department's own words (6.3, 6.8).	Verification and Accreditation Framework (attestation profiles); Data Quality Standard	At launch (Level 2 baseline)

Instrument	What it carries	Read with	Timing
Category 3: Data Asset Boundary and Material Change			
Classification and Metadata Standard Practice Direction · Department · s.92(5)(e); DAR Regulations Part 3 and Schedule 1	The two-axis classification taxonomy (Distribution Scope × Data Sensitivity) and the cells in which a current recognised Level 3 assessment is a condition of issue or renewal of accreditation. Released together with the Register Data Dictionary, the technical standard that represents each register field.	Access Control and Information Handling Standard; Asset Boundary and Material Change Standard; Register Data Dictionary	At launch
Asset Boundary and Material Change Standard [working title] Standard · Department, under the DGF Regulations · s.92(5)(e), applied by the DAR Regulations	How each of the seven attributes of the Asset Boundary Profile, including the growth parameter declarations, is declared, and the method by which a council assesses a change and places it in one of the categories in the DAR Regulations. Its proposed schema is in Annex A.	DAR Regulations (attribute list, change categories, register fields); Data Quality Standard; Register Data Dictionary	At launch (before the Register opens)
Data Quality Standard Standard · Department · s.69	Quality dimensions and metrics; fitness for purpose criteria; definitions of material drift.	Verification and Accreditation Framework (quality conformance); DAR Code controls; Asset Boundary and Material Change Standard (growth parameter declarations)	At launch (assessed at Level 2)
Sector and Residency Overlay Standard Standard · Department · s.69	Operational rules for sectoral overlays (financial services, gambling, life sciences and others) and residency overlays, including the overlays that bring an asset within the second limb of the mandatory Level 3 provision.	Practice Direction 1; DAR Regulations Schedule 1; Joint Guidance	At launch

B.3 Private instruments

Each data asset foundation also operates under private instruments, made by the parties under the general law, which the framework governs or relies on, including:

Instrument	Made by	Basis	How the framework interacts with it
Foundation instrument	Founder	s.68	Establishes the foundation. Checked by the Central Registry at establishment; the Register's remit begins with the application for registration (s.78).
Foundation rules, including the council provisions	Founder and council	ss.73, 75 and 88	Model foundation rules supply defaults where the rules are silent; the Qualification Routes Standard sets how the council qualification requirement is met.
Data asset dedication instrument	Dedicator, with the foundation as acceptor	s.76	Made in Form DAR-1 (Schedule 4 to the DAR Regulations), with any model clauses adopted; a transfer between foundations uses Form DAR-2.
Data licences	The foundation and the licensee	—	Licences granted by the foundation are recorded in Section 3 of the register record.
Terms of engagement of an accredited assurance provider	The foundation and the provider	s.84	Governed by the Verification and Accreditation Framework. The provider's liability is preserved at law.
Terms of appointment of the data enforcer	The council	s.86	Subject to the tenure protections in the DAR Regulations (Part 5) and to the Data Enforcer review standard.