CRITERIA CATALOGUE

Trusted E-Technology GmbH

„EuroTechSeal"

Certification framework for European digital sovereignty

0. PREAMBLE AND SCOPE

This criteria catalogue constitutes the normative basis for awarding the „European Tech Seal - EuroTechSeal" in its four variants. The seal confirms that a company fulfils one or more of the modules defined below. The modules are cumulative; a company may hold all four seal modules simultaneously. Certification is modular, so that each module can be applied for, assessed and awarded independently. In case of doubt, TET reserves the right to carry out more detailed assessments of compliance with the criteria.

The seal is aimed at European (not only EU) digital as well as analogue technology companies, products, services or hybrid offerings such as cloud providers, software providers, AI service providers and digital platform operators that wish to give their customers — in particular companies within the scope of the GDPR and the Data Governance Act — demonstrable guarantees regarding European control, European infrastructure and European value creation.

The seal must not create the impression that it automatically confirms data protection compliance, IT security, GDPR compliance, protection of trade secrets, KRITIS compliance, NIS2 compliance, AI Act compliance or any other regulatory compliance. Such statements may only be made if they have been separately assessed and certified.

1. MODULE 1: EUROPEAN OWNERSHIP

1.1 Objective and subject matter

The objective of this module is to demonstrate that the applicant company is controlled by a majority of natural or legal persons domiciled or resident in the EU, the EEA or the UK, and that structural safeguards against a change of control in favour of non-European owners exist or are contractually secured.

1.2 Scope

The module applies to all legal forms. In the case of groups or corporate groups, the module is to be assessed at the level of the ultimate parent company that exercises control over the applicant company.

1.3 Criteria

1.3.1 Majority European ownership

At least 50.1% of the shares and voting rights in the applicant company are held, directly or indirectly, by natural persons resident in an EU or EEA member state or the UK, or by legal persons with their registered office and actual place of management in an EU or EEA member state or the UK. In the case of indirect participation, the participation chain must be fully documented and disclosed. Trust structures in which the beneficial owner is resident outside the EU/EEA or the UK do not fulfil this criterion.

1.3.2 Transparency of the ownership structure

The company provides the certification body with a current, complete ownership structure consisting of a shareholder overview, participation relationships and a current transparency register/UBO register extract in accordance with the requirements of the Anti-Money Laundering Directive (AMLD). The ownership structure must be updated at least annually and any material changes must be reported without undue delay. This includes in particular, but not exclusively, a change of control. Any transaction that alters the majority relationships or the control structure is deemed material.

1.3.3 No controlling non-European influence

Irrespective of the formal participation relationships, no de facto controlling situation may exist in favour of a non-European actor. This includes in particular voting-rights agreements, veto rights, management agreements or debt relationships that grant a non-European creditor or contractual partner a decisive influence on the company's strategy.

2. MODULE 2: EUROPEAN SOVEREIGNTY

2.1 Objective and subject matter

The objective of this module is to demonstrate that the company, with the certified product or the certified service, operates its essential technological services — computing power, data storage, AI services — predominantly on European infrastructure and is not in an operational dependency on non-European technology providers that would prevent an autonomous continuation of operations.

2.2 Scope

The module applies to all technical services provided in connection with the certified product or the certified service, including development, test and production environments. Internal tools without any customer relationship may be exempted upon request, provided they do not enable access to customer-related data. European Sovereignty does not necessarily mean full self-sufficiency. However, it is required that at least 80 percent of the technical value creation and operating performance essential to the assessed service is provided from within Europe. In addition, there must be no non-European technology dependencies that would render the service inoperable at short notice in the event of discontinuation or blocking, without a realistic exit or substitution plan being in place.

2.3 Criteria

2.3.1 European infrastructure quota for computing power

At least 80% of the computing capacities used (CPU, GPU, HPC) are provided in data centres that are physically located in an EU or EEA member state and are operated by a provider that is subject to European law without reservation. Cloud services whose operators are subject to the US Cloud Act, the Chinese Data Security Law or comparable non-European disclosure obligations are not counted as European for the calculation of the 80% quota, even if the server location is physically within the EU.

2.3.2 European infrastructure quota for data storage

At least 80% of data storage — primary data holding, backups and archiving — takes place in systems that are physically operated in the EU/EEA and are managed by providers that are not subject to the scope of non-European data access laws. Encrypted storage with non-European providers, where the key remains exclusively with the applicant company and there is no operational access by the storage provider, may be recognised subject to a separate technical assessment. The company must document where production data is stored and which providers, subcontractors, administrators or support units may obtain access to this data. In addition, the cryptographic control layer under criterion 2.3.9 (external key management) must be taken into account.

2.3.3 European AI services

Insofar as the company uses AI services — inference, training, embedding models or generative models — in its products or its infrastructure, at least 80% of these services must be provided via providers or instances that are fully subject to European law and whose processing infrastructure is located in the EU/EEA.

2.3.4 Dependency analysis and risk assessment

The company has prepared a documented dependency analysis (dependency map) for all critical technology components. The analysis identifies non-European providers, assesses the operational risks in the event of a data access or an outage, and must be updated at least annually.

2.3.5 No mandatory operational dependencies

The company is not bound to non-European providers through contractual arrangements, licensing structures or technical architecture in a manner that de facto precludes an independent continuation of operations without the involvement of those providers. Proprietary formats without open interfaces or export functions are regarded as an indicator of such a mandatory dependency and must be separately justified.

2.3.6 Exit Capability

The company has prepared a documented migration plan for all critical non-European technology dependencies that enables a switch to a European alternative provider within twelve months. The plan must be technically plausible and backed by sufficient resources. The migration plan contains a defined trigger mechanism that initiates the migration in the event of material political, security-related or licensing-related changes.

2.3.7 Self-declaration and internal control

Since a full external verification of the infrastructure quotas is only possible to a limited extent without far-reaching technical audit rights, the company undertakes to submit an annual self-declaration to the certification body.

2.3.8. Documented provider landscape

The company must disclose all essential technology providers, in particular cloud, hosting, CDN, AI, database, monitoring, security, identity, payment, support and DevOps providers.

2.3.9 External key management

Insofar as the certified service uses cryptographic procedures, the technical and organisational possibility exists to manage the encryption keys outside the provider's infrastructure (external key management / Bring Your Own Key / Hold Your Own Key). The applicant company documents the cryptographic control layer and demonstrates that operational access by non-European providers to plaintext data is excluded. This criterion supplements the physical storage-location question governed in 2.3.2 with cryptographic control.

2.3.10 Open interfaces and export-capable standard formats:

The company offers, for the certified service, open, documented interfaces (APIs) as well as export-capable, standardised file formats, so that customers can migrate data and configurations without proprietary lock-in. Standardised interfaces and file formats are regarded as an independent sovereignty indicator and give concrete effect to the prohibition of mandatory operational dependencies governed in 2.3.5.

2.3.11 Supply chain transparency at software and hardware level / SBOM:

The company maintains, for the certified service, a Software Bill of Materials (SBOM) as well as a documented inventory list of the essential hardware and software suppliers, stating the respective countries of origin. The SBOM and the inventory list must be made available to the certification body upon request and must be updated at least annually.

2.3.12 Disconnect capability:

The company maintains a documented process by which all non-European network connections can be disconnected without impairing the availability, integrity and confidentiality of the certified service. The disconnect process must be tested at least annually and the test result documented.

3. MODULE 3: BUILT IN EUROPE — DEVELOPED AND DESIGNED IN EUROPE

3.1 Objective and subject matter

The objective of this module is to demonstrate that the essential value creation in the development, design, conception and implementation (the R&D work) of the products and services takes place in Europe. The module addresses the question of where intellectual property arises, where design decisions are taken and where core technical competencies are located.

3.2 Scope

The module applies to all phases of the product development cycle, from conception through implementation to quality assurance. It does not apply to operational activities after market launch, which are covered by Module 4.

3.3 Criteria

3.3.1 European value-creation quota in development:

At least 80% of the value-creating activities in product development — measured by the personnel effort deployed in full-time equivalents or in person-hours — are performed by employees or

contractors whose place of work is in an EU or EEA member state or the UK, or in Europe as a whole. The outsourcing of development work to non-European contractors is calculated on a pro-rata basis and factored into the value-creation quota.

3.3.2 European ownership of core technology and intellectual property:

The essential intellectual property rights in the product — in particular copyrights in the source code, patents and database rights under § 87b UrhG or Art. 7 of the Database Directive — are owned by the applicant company or a European group company. Licensing structures in which the intellectual property in the core technologies lies outside the EU/EEA and the applicant company acts merely as a licensee do not fulfil this criterion.

3.3.3 Product design and architecture decisions in Europe:

The key decisions on product architecture, system design, data-protection-by-design implementation pursuant to Art. 25 GDPR and security architecture are taken by teams that are predominantly active in Europe. As evidence, a declaration by the management on the organisational structure of the responsible teams must be submitted.

3.3.4 Data protection by design as a development principle

Product development follows a demonstrable privacy-by-design process pursuant to Art. 25 GDPR. The company has internal or external procedures for ensuring data protection compliance.

3.3.5 Research and development in Europe:

Insofar as the company conducts its own research and development activities, these take place predominantly in Europe. Cooperation with European universities or research institutes as well as participation in European funding programmes such as Horizon Europe or IPCEI are assessed positively.

3.3.6 Supply chain transparency:

The company documents its essential development and procurement partners at the first supply-chain tier as well as their geographical location. The documentation enables the certification body to carry out a plausibility check of the declared value-creation quota.

3.3.7 Self-declaration and internal control:

Every two years the company submits a self-declaration describing the value-creation quota, the structure of the development teams and the IP relationships. The declaration must be signed by the management. Sample audits by the certification body are permissible.

3.3.8 European alternatives assessment

The company demonstrates in documented form that, when selecting essential technology components, European alternatives were actively evaluated before a non-European solution was chosen. The documentation covers the alternatives assessed, the evaluation criteria and the decisive reasons for the selection decision.

3.3.9 Open-source principle

The company builds its core components predominantly on open-source software or publishes its own developments under a recognised open-source licence. Fulfilment of this criterion must be evidenced by suitable proof (licence information, repositories, dependency lists).

4. MODULE 4: OPERATED IN EUROPE — OPERATED AND CONTROLLED IN EUROPE

4.1 Objective and subject matter

The objective of this module is to demonstrate that the operational core of the company — infrastructure operation, technical customer service and strategic management — is anchored in Europe. The module differs from Module 3 in that it focuses not on development but on the ongoing operation and strategic management of the company.

4.2 Scope

The module applies to all operational activities that arise after the market launch of a product or service, including infrastructure operation, customer support, security management and corporate management. It can be combined with Module 2 and Module 3 but sets independent requirements.

4.3 Criteria

4.3.1 Operation of the core infrastructure in Europe

The infrastructure components essential to production operation — production systems, monitoring, incident response and emergency operation — are managed by teams whose place of service is predominantly in an EU or EEA member state. On-call services outside Europe are permissible, provided they cover no more than 20% of the total operating time and the decision-making authority for critical measures always remains with personnel resident in Europe.

4.3.2 Technical advisory and support services in Europe

Technical advisory and implementation services provided for customers in the EU are predominantly performed by employees whose place of work is in the EU/EEA. Escalation paths and support decisions at higher levels (Tier 2 and Tier 3) lie exclusively with personnel resident in Europe.

4.3.3 Strategic management and governance in Europe

The operational company management — managing directors, Chief Operating Officer, Chief Technology Officer or equivalent functions — has its habitual residence and place of service in an EU or EEA member state. Strategic decisions on product operation, security architecture and data protection compliance are taken by persons who are subject to European law and who can address European supervisory authorities without procedural restrictions.

4.3.4 Data protection responsibility in Europe

The controller within the meaning of Art. 4 No. 7 GDPR has its seat in the EU/EEA. Insofar as an establishment of the company exists outside the EU/EEA, the main establishment for the certified services must be located in the EU/EEA. An appointed data protection officer pursuant to Art. 37 GDPR with a place of work in the EU must be evidenced, provided the statutory requirements are met.

4.3.5 Accessibility for European authorities

The company is directly reachable for European supervisory authorities — data protection supervisory authorities, the Federal Network Agency (Bundesnetzagentur), BSI, ANSSI, national cybersecurity authorities — without forwarding mechanisms to non-European bodies. Insofar as the company does not maintain an EU establishment, a European representative pursuant to Art. 27 GDPR must be appointed.

4.3.6 Emergency and crisis management in Europe

The company has a documented business continuity plan and incident response plan in which the responsibilities for critical decisions lie exclusively with personnel resident in Europe. In the event of a security incident, the notification obligation pursuant to Art. 33 GDPR can be fulfilled without dependence on non-European decision-makers and within the statutory deadlines.

4.3.7 Ingress Data Control

All incoming software updates and operating data of the certified service are routed through a secured, controlled network zone and checked before being transferred into the production environment. The company documents the control mechanisms and responsibilities employed.

4.3.8 Self-declaration and internal control

The company submits an annual self-declaration documenting the organisational structure of operations, the location of the management personnel and the accessibility for authorities. The declaration must be signed by the management. Sample audits by the certification body are permissible.

5. MODULE 5: FULL SOVEREIGNTY — COMBINED SOVEREIGNTY SEAL

5.1 Objective and subject matter

The objective of this module is the award of an independent, aggregated seal „EUTechSeal — Full Sovereignty“ that makes visible a company's particular sovereignty maturity. Unlike Modules 1 to 4, Module 5 does not establish any new substantive individual criteria but requires the combined fulfilment of several base modules. The „Full Sovereignty“ seal bundles the properties demonstrated in the base modules into an overall statement on the European control, value creation and operational authority over the certified product or service.

5.2 Scope

Module 5 can only be applied for in respect of the same product or the same service for which the underlying base modules are certified or are certified at the same time.

5.3 Criteria

5.3.1 Combination requirement (mandatory criterion):

The „EUTechSeal — Full Sovereignty“ seal is awarded if Module 1 (European Ownership) is fulfilled and, in addition, at least two of the three further modules — Module 2 (European Sovereignty), Module 3 (Built in Europe) and Module 4 (Operated in Europe) — are fulfilled. Module 1 is a mandatory prerequisite; without effective certification of Module 1, the „Full Sovereignty“ seal cannot be awarded, even if all three remaining modules are fulfilled.

5.3.2 Relevant degree of fulfilment:

A base module is deemed „fulfilled“ within the meaning of 5.3.1 only if it has been assessed with the result „fulfilled“ pursuant to Chapter 6. A module assessed as „conditionally fulfilled“ counts as fulfilled only once the remediation pursuant to Chapter 6 has been confirmed. A module assessed as „not fulfilled“ is disregarded.

5.3.3 Concurrence of validity (accessoriness):

The „Full Sovereignty“ seal is accessory to the underlying base modules. It exists only for as long as the module combination required under 5.3.1 is effectively certified. If the certification of one of the modules relied upon lapses — for example through expiry, suspension or withdrawal — and the company thereby falls below the combination requirement (Module 1 plus two further modules), the entitlement to use the „Full Sovereignty“ seal also lapses. In this case the company is obliged to cease using the seal without undue delay.

5.3.4 Self-declaration and internal control:

The company confirms to the certification body that the module combination required under 5.3.1 is continuously fulfilled and reports the lapse of any module relied upon without undue delay. For Module 5, the certification body relies on the assessment results of the base modules; a separate substantive assessment takes place only with regard to the combination requirement.

6 CROSS-CUTTING PROCEDURAL REQUIREMENTS

6.1 Application procedure

The application for certification must be submitted online via the website to the certification body. The evidence and self-declarations required for the specific module must be attached to the application. The certification body confirms receipt within two weeks and informs the applicant within four weeks whether the application is complete.

6.2 Assessment procedure

The certification body checks the submitted documents for completeness and plausibility. For Module 1, an active verification of the ownership structure is carried out on the basis of public registers and the documents submitted. For Modules 2 to 4, the assessment is carried out primarily on the basis of the self-declaration and the attached evidence; the certification body is entitled to request supplementary documents.

6.3 Validity period and recertification

The seal is awarded for a term of two years. Three months before the expiry of the validity period, the certification body commences recertification, unless the customer has terminated the certification application at least 3 months before the expiry of the certification period. Material changes in the circumstances relevant to certification must be reported to the certification body without undue delay and may lead to a suspension or withdrawal of the seal.

6.4 Sample audits

The certification body is entitled to carry out both event-based and event-independent sample audits. The certified company is obliged to provide complete information within four weeks and to grant access to the relevant documents.

6.5 Withdrawal of the seal

The seal may be withdrawn if a mandatory criterion is permanently no longer fulfilled, if a self-declaration contains incorrect information, if a material structural change was not reported without undue delay, or if the company does not cooperate with a sample audit. Before withdrawal, the company must be given an opportunity to comment.

6.6 Use of the seal and terms of use

The seal may be used exclusively for the modules for which an effective certification exists. Any extension to non-certified products or services is inadmissible. Misleading use of the seal may trigger competition-law consequences under §§ 5, 5a UWG as well as trademark claims of the certification body.

6.7. For the purposes of this criteria catalogue, „Europe“ is generally to be understood as follows:

a. Member states of the European Union,

b. Contracting states of the European Economic Area,

c. Switzerland.

d. United Kingdom

e. Serbia

6.8. The applicant must provide a complete and accurate self-disclosure via the online form provided. The applicant must confirm that material changes during the term of the certificate will be reported without undue delay.

6.9. Evidence for depicting the corporate-law structure may include (non-exhaustively):

- Commercial register extract.
- Current shareholder list.
- Cap table.
- Participation structure diagram
- Articles of association or shareholders' agreement.
- Voting agreements.
- Investor agreements.
- Convertible loan, option, SAFE or similar financing documents.
- Declaration by the management on the completeness of the information.
- Evidence regarding beneficial owners.
- For listed companies: voting-rights notifications, annual reports, investor-relations documents and known major-shareholder structure.

6.10. Evidence for the other criteria may include, among others:

- Architecture diagrams.
- Data flow diagrams.
- Cloud and hosting contracts.
- Subcontractor lists.
- Provider lists.
- Data residency confirmations.
- AI provider and model overview.
- Documentation of deployments and operating environments.
- Access concepts.
- Key management documentation.
- Exit plans.
- Internal risk analysis of technology dependencies.
- Management confirmation.

- Samples from billing or usage statistics.

CHAPTER 7 — ASSESSMENT PROCEDURE AND ASSESSMENT STANDARDS

7.1 Principles of the assessment procedure

The certification body assesses fulfilment of the criteria of all four modules according to a uniform assessment procedure. This procedure is divided into a document review, a plausibility check and — insofar as provided for on a module-specific basis or required in an individual case — an in-depth expert assessment. The assessment is carried out module by module; each module is concluded separately and leads to an independent assessment result.

7.2 Assessment stages

The assessment is carried out in two regular stages.

In the first stage, the certification body checks the submitted documents for formal completeness. Incomplete applications are returned to the applicant with an indication of the missing documents. The period for completion is six weeks from receipt of the objection. If the period is not observed, the application is deemed withdrawn.

In the second stage, the certification body assesses the substantive fulfilment of the criteria on the basis of the submitted documents and the self-declaration. The certification body is entitled to request supplementary information and documents; the applicant must respond to this within four weeks.

7.3 Assessment result

For each module, the assessment result is either „fulfilled“, „conditionally fulfilled“ or „not fulfilled“.

„Fulfilled“ is awarded if all mandatory criteria of the module are demonstrated completely and without material objection.

„Conditionally fulfilled“ is awarded if individual mandatory criteria are not fully fulfilled at the time of application but the certification body, after weighing the overall circumstances, concludes that fulfilment is realistically achievable within a remediation period of three months. In this case the seal is awarded only after confirmation of the remediation. The remediation period may be extended once by a further three months if the applicant submits a documented progress report.

„Not fulfilled“ is awarded if one or more mandatory criteria are structurally not fulfilled and remediation within the deadlines is not plausible, or if the applicant fails to submit the required documents in full despite being requested to do so.

7.4 Assessment report

Upon completion of the assessment procedure, the certification body prepares an assessment report which is transmitted to the applicant. The assessment report contains the assessment result per module, a listing of the criteria assessed with the respective individual result, a justification for objections and — where relevant — the conditions of the remediation requirement. The assessment report is confidential and is made accessible to third parties only with the express written consent of the certified company, unless statutory disclosure obligations preclude this.

7.5 Objection and complaint

The applicant may lodge a written objection with the certification body within four weeks of receipt of the assessment report. The objection has suspensive effect vis-à-vis a withdrawal, but not vis-à-vis the refusal of the initial certification. The objection is decided by an independent complaints body appointed by the certification body within eight weeks. The right to bring proceedings before the ordinary courts remains unaffected.

Hamburg/Wien, August 2026