EUROPEAN
COMMISSION

Brussels, 10.11.2025
COM(2025) 673 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Analysis of the necessity and feasibility of a domain name information and alert system for geographical indications pursuant to Article 35(3) of Regulation (EU) 2024/1143

GLOSSARY OF KEY TECHNICAL TERMS

ccTLD (Country-Code Top-Level Domain):

A top-level domain assigned to a specific country or territory, consisting of two letters (e.g. ".fr", ".de") and managed by a national registry.

Cybersquatting:

The bad-faith registration or use of a domain name identical or confusingly similar to a protected name – such as a trade mark or a geographical indication – with the intention of taking unfair advantage of its reputation, misleading consumers or reselling the domain for profit.

DNS (Domain Name System):

The hierarchical naming system that translates human-readable domain names (like "example.eu") into numerical Internet Protocol (IP) addresses used by computers to locate one another on the Internet.

DAS (Domain Availability Service):

A service used to check whether a specific domain name is available for registration or already taken, typically through automated queries to domain registries.

NS (Name Server):

A server within the DNS that stores and manages records linking domain names to IP addresses, enabling users to access websites using names instead of numeric addresses.

RDAP (Registration Data Access Protocol):

A standard Internet protocol that provides structured, machine-readable access to domain registration data, replacing progressively the older WHOIS system. RDAP offers improved security, standardisation and data protection features.

WHOIS (Who Is):

An Internet service that provides basic information about a registered domain name, such as its status, registrar and registration dates.

1. INTRODUCTION

Geographical indications (GIs) are a cornerstone of the European Union's quality policy. They protect the names of specific products whose qualities or reputation are linked to their geographical origin and the traditional know-how of the producers. As digital marketing and online presence have become central to the commercialisation of these products, safeguarding GIs in the domain name system (DNS) has become increasingly important.

To strengthen GI protection in this area, Article 35 of Regulation (EU) 2024/1143 ([1]) requires the Commission to analyse, by 14 November 2025, the need for and feasibility of an EU-level domain name information and alert system for geographical indications and submit a report with its main findings. Where appropriate, the report may be accompanied by a legislative proposal.

A domain name information and alert system would enable GI applicants to verify whether a GI is already registered as a domain name and, if they wish, to receive alerts when a domain name identical to a GI is registered.

This report summarises the results of this analysis and considers how a voluntary provision of information by EU-based ccTLD registries could work in practice. It fulfils the obligation set out in Article 35(3) of Regulation (EU) 2024/1143 and presents the Commission's findings.

2. LEGAL FRAMEWORK AND POLICY CONTEXT

Legal basis

Regulation (EU) 2024/1143 of the European Parliament and of the Council on geographical indications for wine, spirit drinks and agricultural products recognises the growing importance of protecting GIs in the DNS, as these rights are increasingly vulnerable to, and often targeted by, abusive domain name registrations, often referred to as 'cybersquatting'. To strengthen GI protection in this area, the Regulation (EU) 2024/1143 introduces the possibility of setting up a domain name information and alert system.

Under Article 35(2) of the Regulation, the Commission may entrust the EUIPO with setting up and managing such a system. The same provision provides for EU-based ccTLD registries to participate on a voluntary basis by providing relevant information and data to the EUIPO.

Article 35(3) of the Regulation requires the Commission to analyse whether it would be necessary and feasible to set up such a system, taking into account how the voluntary provision of information and data by registries could work in practice. The Commission must submit the analysis' results to the European Parliament and the Council by 14 November 2025.

([1]) Regulation (EU) 2024/1143 of the European Parliament and of the Council of 11 April 2024 on geographical indications for wine, spirit drinks and agricultural products, as well as traditional specialities guaranteed and optional quality terms for agricultural products (OJ L, 2024/1143, 23.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1143/oj).

Need for coordinated action across GI sectors

The analysis for agricultural GIs under Regulation (EU) 2024/1143 runs in parallel with the obligation set out in Article 72(2) of Regulation (EU) 2023/2411 ([2]) on craft and industrial (CI) GIs. That provision requires the Commission to analyse, by 2 June 2026, the feasibility of setting up an information and alert system to prevent the abusive use of CI GIs in the DNS.

These provisions form part of the broader EU policy to strengthen the protection of intellectual property rights online, as reflected in the EU intellectual property action plan ([3]) and in the development of the Commission Recommendation on measures to combat counterfeiting ([4]). The provisions also respond to concerns raised by stakeholders about the limitations of existing mechanisms to prevent or address the misuse of GIs online.

Agricultural and CI GIs have similar legal foundations, policy objectives and potential system architecture. It is essential to ensure policy coherence and avoid duplication of effort. This report, on which the future report of 2 June 2026 will build, is a first look at whether it would be possible to set up a single EU-level domain name information and alert system covering both agricultural and CI GIs, rather than two separate systems, each under its own legal framework. This would help ensuring consistency and contribute to a unified EU approach to GI protection in the DNS.

On 4 December 2024, the Commission and the EUIPO signed an administrative agreement to strengthen cooperation in areas such as GI protection and enforcement. The agreement specifically records the parties' readiness to cooperate on developing a domain name information and alert system and to explore whether the EUIPO's existing system (currently used for EU trade marks under the .eu top-level domain) could be extended to GIs, by means of delegated acts as provided for in Article 35(2) of Regulation (EU) 2024/1143.

The Commission has also cooperated closely with EURid – the registry for the .eu top-level domain. Here, the focus of cooperation was on analysing technical and legal boundaries and on helping identify a proportionate and efficient solution.

([2]) Regulation (EU) 2023/2411 of the European Parliament and of the Council of 18 October 2023 on the protection of geographical indications for craft and industrial products (OJ L, 2023/2411, 27.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2411/oj).

([3]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience, COM(2020) 760 final of 25 November 2020, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760.

([4]) Commission Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, C(2024) 1739, 19 March 2024, OJ L, 2024/915, https://single-market-economy.ec.europa.eu/publications/commission-recommendation-measures-combat-counterfeiting-and-enhance-enforcement-intellectual_en.

3. METHODOLOGY AND SOURCES

This analysis draws on a number of complementary sources of evidence.

- **Comprehensive study commissioned by the European Commission** ([5]) ('the study'). This study gathered evidence on abusive domain name registrations involving GIs and examined the technical, legal and organisational feasibility of a GI-focused domain name information and alert system. It also analysed the provisions common to the legal frameworks for agricultural and CI GIs and concluded that a coordinated EU approach to any future system would be technically feasible and desirable policy-wise.
- **CENTR position paper** ([6]). This formal position paper was drawn up by CENTR, the association representing Europe's national domain name registries. The paper presents members' views and concerns regarding any EU-level information and alert system.
- **Targeted consultation of EU ccTLD registries**. From August to September 2025, the Commission invited all EU-based ccTLD registries, EURid and CENTR to comment on the proposed technical model and on possible forms of voluntary cooperation. Their feedback is reflected in this report.
- **Bilateral interservice meetings and technical exchanges**. These involved Commission departments, EURid (as regards the operation of the existing EU trade mark alert system for .eu) and the intellectual property expert who contributed to the study.

4. ANALYSIS OF NEED

It is becoming increasingly important to protect geographical indications in the domain name system as online marketing and e-commerce play a growing role for GI producers. Although documented cases of GI misuse in domain names appear limited, this often reflects structural factors rather than an absence of risk.

Many GI producer groups are small or medium-sized enterprises or associations that do not have the resources to systematically monitor domain name registrations. They typically rely on occasional checks or act only once misuse becomes visible in the marketplace. Even when misuse is detected, producers frequently decide not to take action because existing procedures are costly and complex. While some private monitoring services exist, these are fee-based and designed primarily for trade marks, making them less accessible and not fully adapted to protecting GIs.

EU legislation, namely Article 35(1) of Regulation (EU) 2024/1143, now requires all EU ccTLD registries to recognise GIs as valid prior rights in their alternative dispute-resolution (ADR) mechanisms. This was not always the case. Before the Regulation's entry into force in May 2024, the only available remedy was often legal action before the national courts.

([5]) Study on intellectual property domain name information and alert system, commissioned by the European Commission, prepared by Wavestone in collaboration with Ivett Paulovics, Final Report – December 2023.

([6]) Council of European National Top-Level Domain Registries, *CENTR Comment on the geographical indications reform in the EU*, Brussels, 15 September 2022, available at: https://www.centr.org/news/news/comment-gi-reform.html.

Since taking legal action can be lengthy, expensive and of uncertain outcome, many GI producers decided not to pursue this option.

At international level, GIs are not recognised as rights eligible for protection under the Uniform Domain Name Dispute Resolution Policy (UDRP), the main dispute-resolution procedure for generic top-level domains (gTLDs) operated by the World Intellectual Property Organisation. This means that the procedure is unavailable to GI producers.

Consequently, the relatively low number of reported cases of GI misuse in domain names is not necessarily a reliable indicator of the actual level of risk: limited monitoring capacity and complex enforcement mechanisms mask the actual scale of the problem. Moreover, current domain name dispute-resolution mechanisms are inherently reactive and do not have a preventive function.

A proactive EU-level information and alert system would therefore:

- help GI applicants detect potentially abusive registrations early and act before reputational damage occurs;

- provide a single point of access to check whether a GI has been registered as a domain name across the otherwise fragmented ccTLD landscape – this would increase transparency in domain name registration without disclosing any additional personal data; and

- strengthen the overall enforcement framework for GIs online.

The Commission's analysis indicates that although instances of cybersquatting involving GIs are not yet widespread, they do occur and can cause significant economic and reputational harm. In light of the growing online visibility of GI products, a preventive EU-level system may therefore be considered necessary.

5. FEASIBILITY ANALYSIS

5.1. Alternative system models

A domain name information and alert system for GIs would provide two core services:

- **an information function**, which would enable GI applicants to check whether a domain name identical to a GI is already registered;

- **an alert function**, which would send optional notifications when such a domain name is newly registered.

These functions mirror the alert system already in place for EU trade marks (EUTMs) under the .eu domain, which is operated jointly by the EUIPO and EURid. That system relies on exact-match searches of domain names and automatically notifies EUTM holders if an identical .eu domain name is registered, without any exchange of registrants' personal data.

The Commission first examined whether the existing .eu system for EUTMs could be extended to GIs and to EU-based ccTLDs. A number of architectural alternatives were

analysed, differing in terms of who would perform the matching and how the data would be exchanged:

- **Decentralised matching.** Each ccTLD registry would run availability checks and send the results to the EUIPO.

- **Centralised matching.** The EUIPO would collect registration data from registries and perform the checks itself, in the same way as for the existing .eu system for EUTMs.

- **Third-party model.** An intermediary would collect or match the data before passing results to the EUIPO.

All these approaches are technically feasible in principle. However, each would require registries to make significant changes. These include developing application programming interfaces (APIs), which are standard technical interfaces enabling automated communication between computer systems, building matching tools or exporting domain name registration data on a regular basis. These changes would entail costs and infrastructure changes for registries. From a legal perspective, these models would also require contractual arrangements with every registry to govern data sharing and to avoid risks relating to confidentiality or data protection. The complexity and burden of such arrangements were identified as a major obstacle.

Registries consulted in the context of the study largely opposed these alternatives and, more broadly, questioned the need for a GI-specific alert system. They indicated that the required changes would impose significant costs and operational burdens and raised concerns about data protection and confidentiality. They did not consider such a system to be necessary and expressed unwillingness to invest in infrastructure changes. In its position paper, CENTR likewise stressed that any EU system should remain voluntary and should avoid unnecessary obligations. CENTR underlined the low number of GI-related disputes in the domain name space, the existence of ADR mechanisms, and the need to prevent additional burdens on registries.

In view of these limitations, an additional alternative was examined that would not involve expanding the existing .eu system for EUTMs to GIs and to EU-based ccTLDs. Instead, it would involve creating **a dedicated GI system operated by the EUIPO and relying mainly on publicly available DNS tools**. It would offer the same information and alert functions as the current .eu system – based on exact matches with registered GIs – but it would not be necessary for registries to export or share registration databases. Technically, the system would rely by default on **name server (NS) lookups**, a standard DNS query that simply checks whether a domain name exists. Where an NS lookup returns no result (for example when a name is registered but not yet delegated ([7])), this could be complemented by automated queries through:

- the **WHOIS protocol** or its secure successor, the **Registration Data Access Protocol (RDAP)**; and/or

([7]) A domain name is 'registered but not yet delegated' when it is recorded in the registry's database and therefore unavailable for others to register, but the registrant has not yet linked it to name servers, so it does not lead to any website or email service.

- a **domain availability service (DAS)**, where such a service is offered by the registry.

This model has clear advantages. It would entail no development or operational costs for ccTLD registries and no changes to their infrastructure. It would also build on the experience gained by the EUIPO with the alert system already in place for EUTMs, creating synergies. The necessary coding would be developed centrally by the EUIPO to enable NS and WHOIS/RDAP lookups. These methods use only publicly available DNS data and do not require registries to share the complete lists of registered names (known as 'zone files') or personal data. A system based solely on NS lookups could function even without cooperation from registries.

However, to improve accuracy and coverage, **voluntary cooperation from registries could take the form of:**

- **whitelisting** the EUIPO's IP address to allow automated WHOIS or RDAP queries; and/or

- **granting access** to a DAS, where such a service exists.

This would ensure that the system also captures domain names that are registered but not yet delegated. Such cooperation would remain strictly voluntary and would not create any legal obligation for registries.

5.2. Conclusion on the alternative system models

The analysis identifies an EU-level domain name information and alert system managed by the EUIPO and based on standard, publicly available DNS tools as **the most proportionate and technically viable model**.

Ambitious architectural models are technically possible. However, they should be excluded because they would entail disproportionate costs, create legal complexity and face strong opposition from registries. By contrast, a lightweight EUIPO-managed model based on standard, publicly available DNS tools is technically and legally feasible, could be designed to comply with EU data-protection and cybersecurity requirements, and would minimise costs and operational burdens. It addresses many of the concerns expressed by registries, provided that participation remains voluntary and appropriate safeguards and contractual arrangements are put in place.

This model offers a technically feasible and low-impact solution, as described above, that:

- requires no technical adaptations or development costs for registries;
- does not involve the sharing of zone files, personal data or other registration details; and
- would be supported by clear legal safeguards, ensuring that any data or queries are used solely for the operation of the system.

Any cooperation by ccTLD registries would remain strictly voluntary and would not create any legal obligation for them.

This proposed model would give GI producer groups an EU-level preventive tool against cybersquatting and the misuse of GIs in domain name registrations, while addressing registry operators' principal concerns over operational burden, data protection and technical feasibility.

6. CONSULTATION OF COUNTRY-CODE TOP-LEVEL DOMAIN NAME REGISTRIES

6.1. Description of the consultation

To analyse the practicability of this model and the willingness of registries to cooperate on a voluntary basis, the Commission carried out a targeted consultation from August to September 2025. This was addressed to all 27 EU ccTLD registries, EURid and CENTR.

In the consultation, the Commission outlined the proposed technical model and asked whether registries would, in principle, be willing to:

- whitelist the EUIPO's IP address to enable automated WHOIS queries; and/or
- grant access to a DAS, where such a service is available.

The registries' input is reflected in this report. It provided an indication of the level of voluntary participation that could be expected for a future EU-level domain name information and alert system for GIs.

6.2. Results of the consultation

In addition to CENTR and EURid, 22 EU ccTLD registries replied.

Support for the proposed model, subject to safeguards

Most respondents indicated that they would, in principle, be willing to participate in the proposed model through at least one of the two voluntary forms of cooperation, namely:

- granting automated access to domain name registration information (via the WHOIS protocol or the RDAP); or

- providing access to a DAS.

Registries that were positive about cooperating consistently underlined a number of safeguards that would need to be put in place and practical conditions that would need to be met for cooperation to be acceptable.

- **Purpose limitation**. Any data must be used strictly for the operation of the EU-level domain name information and alert system and only for checking the availability of GI names.

- **Data protection**. Cooperation must comply with EU data-protection requirements and no personal data should be shared.

- **Cybersecurity and NIS 2 compliance**. Cooperation must comply with the EU's NIS 2 Directive ([8]), which sets common EU rules to keep networks and information systems secure and classifies domain name registries as 'essential entities' subject to strict security and risk-management measures.

- **Clear operational parameters**. The expected number and frequency of automated queries (DNS lookups) must be set and kept within reasonable limits.

- **Exclusion of zone files**. Sharing of zone files must remain excluded.

- **Technology preference**. Where possible, queries should use RDAP, the modern and more secure successor to WHOIS.

- **Fair competition**. Any privileged access for the EUIPO to DNS data must not distort competition in the brand protection services market or give the EUIPO a preferential advantage. Any data obtained for GI protection must therefore be used strictly for that purpose.

Registries further underlined that any cooperation with the EUIPO could only be envisaged as part of a **formal agreement**. Such an agreement would need to clearly define the scope of cooperation, include appropriate security clauses, and address the broader concerns raised during the consultation.

Several registries also suggested practical improvements, such as pilot projects. Examples included: (i) a 'push' model, which would involve the registry itself notifying the EUIPO of matching registrations rather than the EUIPO repeatedly issuing queries (DNS lookups); and (ii) the use of open datasets (daily lists or monthly open data) to reduce the need for special access.

Reservations

Some registries that were otherwise open to cooperation nevertheless questioned the scale of GI abuse in the EU domain space. They considered granting preferential access – e.g. through WHOIS whitelisting or DAS – to be disproportionate in this context. Instead, they suggested starting with what is already publicly accessible, namely NS lookups, which simply check whether a domain name exists, while leaving the question of preferential access for the EUIPO to be considered at a later stage.

A minority of respondents indicated that they could not support the development of such a system, citing the low incidence of GI abuse and the existence of security risks and legal or technical constraints.

Implications for the proposed model

The results of the consultation confirm that the proposed model – based mainly on public NS lookups and, where necessary, supplemented by WHOIS/RDAP queries or a DAS – is technically feasible. They also show that voluntary cooperation is realistic, provided that the Commission and the EUIPO put in place clear legal safeguards, keep the operational

([8]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

burden minimal, and ensure standardised and secure access (preferably via RDAP) with reasonable limits on the number and frequency of queries.

A phased approach would best reflect the diversity of registry set-ups and the concerns expressed. Such an approach would start with what can already be achieved through public DNS lookups, before progressively including registries that wish to provide additional voluntary access. Pilot projects, such as the 'push' model or the publication of open datasets, could further improve efficiency.

7. FINDINGS AND CONCLUSIONS

The analysis confirms that misuse of geographical indications in domain names – though underreported and thus difficult to quantify – poses a real and growing risk to the economic value and reputation of GI products. The low number of reported cases more likely reflects the limited monitoring capacity of many producer groups and the reactive nature of existing dispute-resolution mechanisms rather than an absence of risk.

Current enforcement tools for EU-based country-code top-level domains are largely reactive. Alternative dispute resolution at national level provides only remedies in response to a dispute, once a domain name has already been registered. Court litigation is often lengthy, costly and unpredictable, and private monitoring services are expensive and primarily designed for trade marks rather than GIs.

A preventive EU-level domain name information and alert system would help fill this gap. By enabling GI applicants to check whether a name they intend to protect as a GI has already been registered as a domain name and to receive alerts when identical names are registered, such a system would enable producer groups to act before economic and reputational damage occurs.

The analysis confirms that setting up an EU-level domain name information and alert system for GIs is both necessary and technically feasible. Such a system would provide GI producers with a preventive tool against cybersquatting and help protect the reputation and economic value of GI products in the online environment.

The most appropriate model is an EUIPO-managed system based on standard, publicly available DNS tools and on the voluntary cooperation of ccTLD registries. This approach avoids the need for registries to adapt their infrastructure or share personal data.

The analysis shows that a system based mainly on public DNS tools could be implemented without requiring registries to share personal data or make technical changes. Such a system would be based especially on name server lookups. Where needed, these would be supplemented by WHOIS or RDAP queries, or by a domain availability service.

The targeted consultation of EU-based ccTLD registries, CENTR and EURid indicates that voluntary cooperation is realistically achievable. Most respondents expressed willingness in principle to grant automated WHOIS/RDAP or DAS access, provided that:

- the system's purpose is strictly limited to GI protection;

- cooperation complies with the EU's cybersecurity rules, in particular the NIS 2 Directive (Directive (EU) 2022/2555), which sets common EU rules to keep networks and information systems secure; and
- formal agreements clearly define the scope of cooperation and the necessary security safeguards.

Concerns raised by registries – such as the need for proportionality, strong data-protection safeguards and minimal operational burden – could be addressed by a lightweight design and strictly voluntary participation.

This report provides the factual and policy basis required by Article 35(3) of Regulation (EU) 2024/1143 and fulfils the obligation to analyse the need for and feasibility of such a system. On the basis of this analysis, the Commission does not intend, at this stage, to present a legislative proposal.

8. WAY FORWARD

The Commission will continue internal coordination and dialogue with stakeholders to determine the most appropriate framework for a possible EU-level domain name information and alert system for geographical indications.

Any step towards a legislative proposal will be considered together with:

- the conclusions of the Commission's separate analysis on craft and industrial GIs under Article 72(2) of Regulation (EU) 2023/2411, which (as mentioned above) is due by 2 June 2026; and
- further technical consultations and pilot projects with the EUIPO, EURid and the EU-based ccTLD registries to test practical arrangements and ensure that any future system is proportionate and workable.