

# EU Open Digital Ecosystems Consultation Analysis

Domain: security - Complete Analysis

Documented Insights Analysis System

February 2026

## Contents

<b>EU Open Digital Ecosystems Consultation</b>	<b>1</b>
Security and Privacy . . . . .	1
Executive Summary . . . . .	1
Market Sentiment Overview . . . . .	1
Term Usage Patterns . . . . .	3
Sentiment and Advocacy Patterns . . . . .	3
Related Themes and Context . . . . .	3
Sub-theme Distribution . . . . .	4
Policy Considerations . . . . .	4
Methodology . . . . .	4
<b>LLM Position Analysis - Security</b>	<b>5</b>
Stakeholder Positions . . . . .	5

## EU Open Digital Ecosystems Consultation

### Security and Privacy

**Analysis date** 07 February 2026

**Domain scope** Cybersecurity, data protection, vulnerability management, privacy concerns

**Commission context** NIS2 Directive, GDPR, Cyber Resilience Act, critical infrastructure protection

### Executive Summary

This domain received substantial engagement across the consultation, with 613 responses (37.0% of corpus) addressing related themes. Respondents from 42 countries and 11 stakeholder types contributed, indicating broad interest across the EU.

### Market Sentiment Overview

#### Coverage and Engagement

Metric	Value
Matching responses	613
Coverage of corpus	37.0%
Countries represented	42

Metric	Value
Stakeholder types	11
Organisations	219
Responses with attachments	117

## Stakeholder Positions

The consultation response was dominated by EU Citizens (59.2%), followed by Companies (19.7%). This distribution suggests strong grassroots interest rather than primarily industry-driven advocacy.

Stakeholder Type	Responses	Countries	Percentage
EU Citizen	363	25	59.2%
Company	121	20	19.7%
NGO	47	16	7.7%
Non EU Citizen	27	18	4.4%
Academic Research Institution	21	10	3.4%
Other	15	10	2.4%
Business Association	8	5	1.3%
Public Authority	7	6	1.1%
Consumer Organisation	2	2	0.3%
Environmental Organisation	1	1	0.2%
Trade Union	1	1	0.2%

## Geographic Distribution

Geographic engagement shows concentration in Germany (20.1%), with notable participation from Italy and Netherlands. The distribution across 42 countries indicates EU-wide relevance rather than localised concern.

Country	Responses	Percentage
Germany	123	20.1%
Italy	76	12.4%
Netherlands	72	11.7%
France	62	10.1%
Austria	34	5.5%
Belgium	33	5.4%
Poland	27	4.4%
Spain	21	3.4%
Sweden	19	3.1%
Portugal	17	2.8%
United Kingdom	15	2.4%
United States	14	2.3%
Finland	13	2.1%
Romania	12	2.0%
DNK	11	1.8%

## Term Usage Patterns

Analysis of term concentration reveals how strongly specific concepts feature in responses compared to the broader consultation corpus. A strength score above 1.5 indicates the term appears more frequently in this domain than in general discussion.

**attack (strength: 2.5)** Moderately concentrated in this domain

Positive framing – Used with: support, benefit, improve

Critical framing – Discussed alongside: limited, lack, problem

**privacy (strength: 2.0)** Moderately concentrated in this domain

Positive framing – Used with: support, supporting, improve

Critical framing – Discussed alongside: lack, barriers, barrier

**vulnerability (strength: 1.8)** Moderately concentrated in this domain

Positive framing – Used with: support, enables, enable

Critical framing – Discussed alongside: barriers, lack, limited

**breach (strength: 1.6)** Moderately concentrated in this domain

Positive framing – Used with: improve, improvement, improvements

Critical framing – Discussed alongside: limited, limits, problem

**security (strength: 1.4)** Standard usage frequency

Positive framing – Used with: support, supporting, strengthen

Critical framing – Discussed alongside: barriers, lack, limited

## Sentiment and Advocacy Patterns

Language analysis reveals the tone and advocacy intensity of responses addressing this domain.

Language Pattern	Percentage of Responses
Action-oriented language	44.5%
Problem-focused language	40.0%
Solution-focused language	45.2%

Strong advocacy for specific actions – Advocacy level: High

## Related Themes and Context

Terms that frequently co-occur with domain concepts reveal the broader context in which respondents frame this policy area.

Co-occurring Term	Occurrences	Documents	Document %
open	535	535	87.3%
source	481	481	78.5%
software	465	465	75.9%
security	402	402	65.6%
digital	383	383	62.5%

Co-occurring Term	Occurrences	Documents	Document %
public	379	379	61.8%
european	364	364	59.4%
support	341	341	55.6%
sovereignty	336	336	54.8%
infrastructure	313	313	51.1%
data	302	302	49.3%
open-source	278	278	45.4%
projects	274	274	44.7%
solutions	256	256	41.8%
europe	250	250	40.8%
code	250	250	40.8%
critical	249	249	40.6%
companies	247	247	40.3%
funding	247	247	40.3%
development	245	245	40.0%

## Sub-theme Distribution

Responses addressing this domain cluster around distinct sub-themes, revealing specific areas of concern or opportunity. Note that responses may address multiple sub-themes.

Sub-theme	Responses	Percentage
Protection	505	82.4%
Compliance	321	52.4%
Threats	115	18.8%
Supply Chain	22	3.6%
Assessment	11	1.8%

## Policy Considerations

### Market Structure Signals

- Strong grassroots engagement suggests public concern extends beyond industry advocacy

### Advocacy Intensity

- High action-oriented language indicates stakeholders expect policy intervention

### Geographic Considerations

- Broad geographic engagement suggests EU-level relevance

### Methodology

This analysis examines consultation responses through domain-specific keyword and keyphrase matching. Coverage statistics indicate the proportion of responses addressing the domain. Term usage strength compares domain-specific frequency to corpus-wide frequency. Sentiment analysis identifies language patterns without attributing positions to individual respondents.

**Search parameters** 46 terms (10 keywords, 36 keyphrases)

**Analysis date** 07 February 2026

---

# LLM Position Analysis - Security

Generated: Sat Feb 7 21:23:19 2026

## Stakeholder Positions

**LLM Processing Status:** 1129 responses analysed across all domains (68.1% complete, 481 remaining). **This domain:** 35 responses. Results are partial and will update as processing continues.

Analysis of positions extracted through LLM analysis of consultation responses. Extracted 102 positions across 23 categories.

## Position Overview

Position Category	Support	Oppose	Neutral/Mixed	Total
Public Funding	32	2	0	34
Procurement Preference	21	2	0	23
Digital Services Tax	10	4	1	15
Tax Incentive	1	5	0	6
State Aid	4	1	0	5
Cybersecurity Measures	2	0	0	2
Machine Readable Policy Manifests	1	0	0	1
Cyber Security Standards	1	0	0	1
Security Hashing	1	0	0	1
Security Trust	1	0	0	1
Security Viability	1	0	0	1
Non Bureaucratic Funding	1	0	0	1
Economic Incentives	0	1	0	1
Copy Left Licensing	1	0	0	1
Security Overall	1	0	0	1
Cyber Security Support	1	0	0	1
Residential Utility Improvements	1	0	0	1
Cybersecurity	1	0	0	1
Standardized Law Enforcement Api	1	0	0	1
Public Key Infrastructure	1	0	0	1
Vat Exemption	1	0	0	1
Cyber Security Improvement	1	0	0	1
Signed Warrants	1	0	0	1

## Detailed Position Analysis

### Public Funding

**Total responses** 34 positions extracted across 2 distinct responses

**Support position** 32 responses (94.1%), 53.1% express strong advocacy

**Primary stakeholders (support)** EU Citizens (23), Companies (6), Public Authorities (2)

**Core arguments (support)** The EU should finance the maintenance of critical open source components to ensure their continued availability and sovereignty.; Open Source must

be treated as critical digital infrastructure for more security, independence, and digital sovereignty.

**Opposition position** 2 responses (5.9%), 0.0% express strong opposition

**Core arguments (oppose)** The grant-system misses maintenance and infrastructure needs, which are not addressed by the current funding structure.; Current soft strategy and lack of impact assessment are insufficient to address security threats.

**Specific proposals mentioned** Create a European fund for small communities to adopt open source solutions. (1 mentions); creation of foundations indépendantes contrôlées par les citoyens européens (1 mentions); financer la maintenance de briques critiques (1 mentions)

**Evidence cited** proprietary solutions are used for influence, pression culturelle et géopolitique, espionnage économique et technologique (1); The Commission has noted that open-source is key (1); <https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094> (1); fonds dédié ou EDIC (1); <https://hep-alliance.org/Project/> (1)

## Procurement Preference

**Total responses** 23 positions extracted across 2 distinct responses

**Support position** 21 responses (91.3%), 23.8% express strong advocacy

**Primary stakeholders (support)** EU Citizens (14), Companies (5), CONSUMER\_ORGANISATION (1)

**Core arguments (support)** Open Source must be treated as critical digital infrastructure for more security, independence, and digital sovereignty.; Migrating to open source provides sovereignty, mastery, and confidentiality of data and connections.

**Opposition position** 2 responses (8.7%), 50.0% express strong opposition

**Core arguments (oppose)** The current affiliation programs with external technology solutions are detrimental to the EU, compromising data security and quality of services.; Current public procurement practices favor proprietary vendors, hindering the adoption of open source solutions.

**Specific proposals mentioned** Integrazione dello open source negli appalti pubblici (1 mentions); Open Source muss in Vergabe, Förderung und Betrieb endlich als kritische digitale Infrastruktur behandelt werden (1 mentions); Start building European counterparts to American big tech immediately, especially cloud and content delivery. (1 mentions)

**Evidence cited** Thales having migrated under Linux in 48h (1); The open-source software to replace GitHub has been developed in Europe (1); Gendarmerie Nationale in France (1)

## Digital Services Tax

**Total responses** 15 positions extracted across 3 distinct responses

**Support position** 10 responses (66.7%), 0.0% express strong advocacy

**Primary stakeholders (support)** EU Citizens (5), Companies (3), CONSUMER\_ORGANISATION (1)

**Core arguments (support)** A tax on proprietary vendors could incentivize the adoption of open source solutions.; A tax on proprietary vendors could promote the adoption of open source tools.

**Opposition position** 4 responses (26.7%), 0.0% express strong opposition

**Core arguments (oppose)** Taxing proprietary vendors could help level the playing field for European alternatives.; Chasing the latest fads is not a priority, and instead focus on achieving feature parity with non-EU products.

## Tax Incentive

**Total responses** 6 positions extracted across 2 distinct responses

**Support position** 1 responses (16.7%), 0.0% express strong advocacy

**Primary stakeholders (support)** EU Citizens (1)

**Core arguments (support)** Incentives (financial but not only) are needed to encourage good software development.

**Opposition position** 5 responses (83.3%), 0.0% express strong opposition

**Core arguments (oppose)** Permissive licenses, which do not enforce copy left, are not sustainable enough.; Europe has to secure its independence by producing its own hardware, and not relying on Taiwan and China.

## State Aid

**Total responses** 5 positions extracted across 2 distinct responses

**Support position** 4 responses (80.0%), 0.0% express strong advocacy

**Primary stakeholders (support)** EU Citizens (4)

**Core arguments (support)** Investing in open source relocalizes value within the European engineering, integration, cybersecurity, maintenance, and training sectors.; Public subsidies can help alleviate the burden on individual developers and improve security.

**Opposition position** 1 responses (20.0%), 0.0% express strong opposition

**Core arguments (oppose)** Public subsidies for open source projects might be necessary to compete with established proprietary vendors.