European Commission

eGovernment Benchmark 2026

Insight Report

Written by

Capgemini sogeti Part of Capgemini IDC

June - 2026

Manuscript completed in May 2026

Authors and study team

Capgemini: Niels van der Linden, Sem Enzerink, Arman Behrooz, Stan Vugs & Jasper Oortgiesen

Sogeti: Sandrine Cipponeri, Erlend Firth & Mauro Baldacchini

IDC: Massimiliano Claps, Fung-Yee Tang, Giorgio Micheletti & Marion Germaine-Terrasse

Contact: Niels van der Linden (Project Manager eGovernment Benchmark)

E-mail: niels.vander.linden@capgemini.com

1st edition

Luxembourg: Publications Office of the European Union, 2026

PDF ISBN 978-92-68-39462-5
ISSN 2811-8383 doi:10.2759/0999131
KK-01-26-045-EN-N

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology

Directorate B — Digital Decade and Connectivity

Unit B.2 — Digital Decade Coordination

Contact: *Silvia Beghelli*

E-mail: CNECT-DIGITAL-DECADE@ec.europa.eu

European Commission
B-1049 Brussels

Contents

Executive Summary 5

Glossary of Key Terminology 7

1. Introducing the eGovernment Benchmark 8

1.1 The Digital Decade Policy Programme 9
1.2 Methodological Updates and Strategic Alignment 10
1.3 Policy Initiatives Promoting End-To-End eGovernment 11

2. eGovernment as a Cornerstone of the Digital Decade Policy Programme 14

2.1 Digital Public Services for Citizens 16
2.2 Digital Public Services for Businesses 20

3. Complementary Indicators for Effective Digital Public Services 24

3.1 Pre-Filled Forms 25
3.2 Transparency of Service Delivery, Design, and Personal Data 26
3.3 User Support 27
3.4 Mobile Friendliness 28

4. Key Priority Areas 30

4.1 Artificial Intelligence (AI): a Promise for Uplifting the User Experience 31
4.2 Cybersecurity: a Need for Safer eGovernment Services 33
4.3 Sovereignty: Ensuring Digital Continuity of Public Sector 35

5. Digital Governments across Cities, Regions and Countries 42

5.1 National versus Cross-Border Services, in Light of the Single Digital Gateway Regulation (SDGR) 43
5.2 Government Tiers Are Still Apart 45

6. Key Conclusions and EU Policy Recommendations 48

6.1 Progressing towards the Digital Decade by Overcoming Cross-Border Challenges 49
6.2 Accelerating the Implementation of Pre-Filled Forms, Transparency Building Blocks, User Support and Mobile Friendliness 49
6.3 Realising AI-driven, Cybersecure and Sovereign Digital Governments 50
6.4 EU Policy Recommendations 52

EUROPEAN COMMISSION

eGovernment Benchmark 2026 Executive Summary

Insight Report

Directorate-General for Communications Networks, Content and Technology
eGovernment Benchmark 2026

2026 EN

Executive Summary

Government services play an important role in daily life. They affect how citizens live, work, study and travel, as well as how entrepreneurs do business. Therefore, the EU prioritises the digitalisation of key public services. Every year, the **eGovernment Benchmark** assesses the digitalisation of a selected set of public services in the 27 European Union Member States (EU). The study tracks a wide range of digital government trends and developments, as well as the EU's advancement towards achieving the European Commission's Digital Decade target of providing key public sector services online by 2030.

To **measure the availability and quality of most commonly used digital public services as selected in the eGovernment Benchmark**, an EU-wide network of Mystery Shoppers visited over 14,000 government websites in November 2025. They evaluated 96 key public services relevant to nine common life events – key moments in individuals' lives – that require contact with the government. Seven life events were examined for citizens, families, unemployed, students, consumers, and patients: Career, Family, Health, Justice (Starting a Small Claims Procedure), Moving, Studying and Transport. For entrepreneurs that start, run and grow a business, two life events were investigated: Business Start-Up and Regular Business Operations. The study is based on a long-standing method, with 19 indicators and 11 pilot indicators.

The eGovernment Benchmark annually monitors two **Digital Decade Key Performance Indicators (KPIs)** as part of the digitalisation of public services target of the Digital Decade:

1. **Digital public services for citizens:** This KPI tracks online provision of key public services for citizens, measured as the share of administrative steps that can be done fully online for major life events. In 2025, this indicator reached 84.6 out of 100 for the EU. It rose from 79.4 in 2023 and 82.3 in 2024 (yearly increases of 3.7% and 2.8%). Among the citizen life events, Transport, Moving and Studying perform the best. Health services remained the least digitalised. As often observed, cross-border services tend to perform worse than services for national users.

2. **Digital public services for businesses:** This KPI monitors online provision of key public services for businesses, measured as the share of administrative steps needed to start a business and conduct regular business operations, which can be done fully online. In 2025, this indicator stood at 88.6 for the EU. It steadily improved, from 85.4 in 2023 and 86.2 in 2024 (yearly increases of 0.9% and 2.7%). Both the Business-Start Up and Regular Business Operations scores remain relatively high overall. As for the citizen life events, the cross-border services for businesses require particular attention.

In addition to the two Digital Decade KPIs, four complementary indicators provide insight into how easily and effectively users can access and operate online government services. With an increase of more than 7% on the **Pre-Filled Forms** indicator, scoring 75.9, public sector bodies are accelerating their efforts in pre-filling personal data already known in online service forms. Government performance on the **Transparency of Service Delivery, Design, and Personal Data** indicator is stagnant, standing at 69.6 and having almost no improvement compared to 2024. Foremost, consumers who start a legal small claims procedure, the only service investigated in the Justice life event, miss clear service timelines. They also lack information on personal data reuse and have more limited participation options to improve digital government services compared to other life events. The score of 90.0 for **User Support** shows that citizens and entrepreneurs benefit from widely available and comprehensive user assistance when interacting with public sector bodies online. Improved online support, help features, and feedback mechanisms for both national and cross-border users in the Health and Family domains were a main driver for the indicator's continued success. The score of 97.4 attained for **Mobile Friendliness** tells us that most government websites are responsive to mobile devices. The websites that eGovernment users need for Regular Business Operations and Transport life events lead the way in making websites easy to read on smaller screens.

Artificial Intelligence (AI), Cybersecurity and Sovereignty are three crucial priority areas for the EU's digital government transformation. As it currently stands, **AI capabilities for user interactions** have not taken full flight. Less than half of the government portal websites analysed offer AI-powered live support. Their impact on users is also limited, as most chatbots are technically immature. Via most of the currently available chatbots, users can only perform basic interactions and receive limited support when needing guidance through multi-step procedures. Fewer than one out of five chatbots can transfer requests to a human agent, while the linguistic features of chatbots in the EU are also limited. Relatively few chatbots can translate information into clear and accessible language (e.g. summarising chatbot responses into short answers, using plain language, without abbreviations). Most chatbots do not support multilingualism and cannot properly answer questions specific to cross-border users.

Ensuring compliance with **cybersecurity** standards and protocols across government portals remains relevant. However, most common security and modern internet standards are only met by half of the government websites assessed. Raising cyber awareness among the wider public is also essential to safeguarding sensitive information and maintaining trust in digital public services. However, less than one out of four government websites use official government domain suffixes that visitors can easily recognise, such as ".gov". Slightly more promising is the fact that about half of the government portals raise

phishing awareness, actively guiding users in recognising phishing attempts, for instance, explaining how to verify that a domain is legitimate.

As digital sovereignty remains a priority for the European Union, the infrastructure underlying public-facing websites and email domains is increasingly becoming a point of strategic reflection for governments. Pilot indicator findings show that more than one third of eGovernment websites and portals are hosted on servers controlled by operators whose ultimate beneficial ownership lies outside the EU. For incoming and outgoing mail servers this is even more than half of the government email domains.

Glossary of key terminology

- **eGovernment:** electronic government, also digital government.
- **Life event:** a package of government services, usually provided by multiple agencies, that support citizens or entrepreneurs through key points of their lives, such as the birth of a child or starting a business. The eGovernment Benchmark covers nine life events:
  - For citizens: Career, Family, Health, Justice (Starting a Small Claims Procedure), Moving, Studying, and Transport.
  - For businesses: Business Start-Up and Regular Business Operations.
- **Life event services:** services within a user journey for national and cross-border users.
  - Informational services: services and procedures that provide users with adequate and personalised insight into their situation.
  - Transactional services: services and procedures needed to fulfil the essential requirements of a life event, such as registration.
  - Portal websites: eGovernment websites that gather and provide information and services from multiple public administrations, also known as one-stop-shops.
- **National users:** citizens and entrepreneurs that seek information and services in their own country.
- **Cross-border users:** citizens or entrepreneurs that seek information and services in a European country other than their own.
- **Method:** the way in which we collected the data.
  - Mystery Shopping: the primary type of data collection in the eGovernment Benchmark – a proven evaluation method that makes the user journey and experience the primary focus of attention.
  - Automated tools: online tests through which websites are entered and assessed on a number of criteria.

01.

Introducing the **eGovernment** *Benchmark*

1. Introducing the eGovernment Benchmark

The 2026 edition of the eGovernment Benchmark Insight Report provides an updated assessment of Europe's progress in digital public service delivery. Using data collected in 2025, this report examines the progress of the European Union (EU) on its digital transformation journey and what remains necessary to reach the goals of the Digital Decade policy programme, focusing on the two Key Performance Indicators (KPIs) used to monitor digital public services (digital public services for citizens and digital public services for businesses). In addition, four additional indicators that fall under the Digitalisation of Public Services dimension *(Pre-Filled Forms, Mobile Friendliness, Transparency of Service Delivery, Design, and Personal Data, and User Support)* are presented.

The report also highlights key priorities within the EU digital government landscape. These include pilot indicators measured through the eGovernment Benchmark, such as the use of artificial intelligence in live support functionalities, the sovereignty of networks that carry government web and email traffic, as well as aspects of cybersecurity. Lastly, the report explores how digital public services perform across different levels of government and territorial scales, highlighting differences between national and cross-border services as well as variations across cities and regions. All 27 Member States of the European Union participated in the 2025 data collection, and they are referred to collectively as the 'EU' throughout this report.

1.1 The Digital Decade policy programme

The EU's Digital Decade policy programme (DDPP) is designed to accelerate the digital transformation of Europe through to 2030.[1] This comprehensive framework includes measurable goals oriented towards four focus areas (connectivity, digital skills, digital business, digital public services), each with its own targets. The Digital Decade policy programme allows the EU and its Member States to work together to reach 2030 targets and objectives.[2]

The eGovernment Benchmark not only allows policy makers, experts and practitioners across the EU to monitor the maturity of EU digital public services, but it also specifically tracks two KPIs that are part of the monitoring system of the Digital Decade policy programme for the Digital Public Services dimension.[3] The two KPIs are:

- **Digital public services for citizens:** Online provision of key public services for citizens, measured as the share of administrative steps that can be done fully online for major life events. The following life events are considered: moving; transport; starting a small claims procedure; family; career; studying; health.
- **Digital public services for businesses:** Online provision of key public services for businesses, measured as the share of administrative steps needed to start a business and conduct regular business operations, which can be done fully online.

[1]See online Decision (EU) 2022/2481 on establishing the Digital Decade Policy Programme 2030: https://eur-lex.europa.eu/eli/dec/2022/2481/oj.

[2]The Digital Decade DESI visualisation tool allows to interactively monitor progress along Digital Decade KPIs and supporting indicators.

[3]For further details, see Commission Implementing decision - 2023/1353 - EN - EUR-Lex.

1.2 Methodological updates and strategic alignment

The eGovernment Benchmark has become an internationally recognised study that looks at how platforms for citizens, businesses and all user segments (start-ups, students, unemployed, families, etc.) continue to improve. The rapid changes in the digital landscape underline the necessity to frequently assess and, where necessary, update the data collection and reporting method of the eGovernment Benchmark.

As such, the 2025 data collection cycle introduced piloted enhancements across services, indicators, and sampling, listed below. Importantly, given the 'pilot status' of such pilot services, pilot indicators and the piloted expanded regional and local samples, these new elements are not included in the eGovernment Benchmark scoring. Hence, these results are not affecting any of the study's indicators or KPIs.

First, eight services were piloted, covering topic areas such as sustainability, innovative business support, advanced digital skills, digital identity, and civic participation:

- *Career service 4.4: Apply for government reskilling funds and subsidies*
- *Career service 6.1: Apply as a highly skilled (ICT) worker coming from outside the EU*
- *Family service 3.3: Obtain an eID*
- *Justice service 4.1: Check information and requirements on submitting a vote*
- *Moving service 1.7: Apply for housing decarbonisation subsidies*
- *Business Start-up service 1.4: Check requirements for obtaining a European patent*
- *Business Start-up service 3.2: Apply for scale-up funding*
- *Business Start-up service 7.3: Apply for decarbonisation subsidies for your office or store*

Second, 11 pilot sub-indicators were tested to deepen the assessment of AI, Cybersecurity, Sovereignty, and Multilingualism. Among these indicators, seven are assessed through Mystery Shopping, while four employ automated tools. These include:

- *AI-powered chatbot maturity, escalation, understandability, multilingualism support, and cross-border support*
- *Phishing-awareness content*
- *Domain suffix verification*
- *Certification Authority Authorisation (CAA)*
- *Server & email sovereignty*
- *Multilingualism of cross-border portals*

Third, the study piloted an expanded regional and local sampling approach, increasing the number of assessed administrations – particularly smaller municipalities and regional bodies – to obtain a more representative picture of public-sector digital service provision.

The eGovernment Benchmark methodology in a nutshell

To present an in-depth view on eGovernment performance, the analysis covers 96 key public services, as well as two Single Digital Gateway Regulation (SDGR) related services, across nine life events – sequences of digital services that the average citizen and business are likely to require.

The services are related to life events concerning persons' Career, Family, Health, Justice (Starting a Small Claims Procedure), Moving, Studying, Transport, Business Start-up and Regular Business Operations.

Well-trained Mystery Shoppers – citizens from the participating countries – evaluated the life events by visiting and assessing government websites using a standardised survey.

Across the EU, Mystery Shoppers assessed 14,154 websites: 7,341 websites and 655 portals from their own governments, 3,816 cross-border websites and 655 portals from other European countries, as well as 1,687 websites / apps for mobile users. Across the countries, this equates to 524 websites per country on average. Additional automated open tools shed light on Mobile Friendliness, Accessibility Foundations, Speed and Performance, Security and Findability.

The study covers 2,573 public administrations: 1,411 central, 494 regional, and 668 local government bodies. When considering the piloted enlarged sampling method, the study would cover 3,358 public administrations: 1,411 central, 957 regional, and 990 local government bodies.

1.3 Policy initiatives promoting end-to-end eGovernment

In addition to the Digital Decade policy programme, the eGovernment Benchmark methodology is linked to multiple European policy plans and actions aiming to further the EU's vision for a better digital future.

Strengthening interoperability is a core priority across these frameworks. The Interoperable Europe Act promotes seamless cooperation between public administrations across borders, sectors, and organisational layers, enabling secure data exchange and shared digital solutions. By aiming to reduce administrative burdens and support interconnected public services, it reinforces the relevance of indicators such as *eID, Cross-Border eID, and Pre-Filled Forms*, which together offer a practical view of interoperability in the EU.

A modern and interoperable digital public sector also depends on trusted and user-centric digital identity. The evolution from the original eIDAS Regulation to the new Regulation establishing the European Digital Identity Framework addresses longstanding interoperability limitations and introduces the EU Digital Identity Wallet. This new approach obliges Member States to provide secure digital wallets that can combine national eID with verifiable attributes (e.g., licences, diplomas or bank credentials) while ensuring strong privacy protections and security requirements. Mutual recognition of these wallets, supported by a common technical architecture and strengthened cybersecurity rules, will enable cross-border authentication for both public and private services. The Benchmark indicators on *eID and Cross-Border eID* reflect this policy push toward seamless, secure identification across the EU.

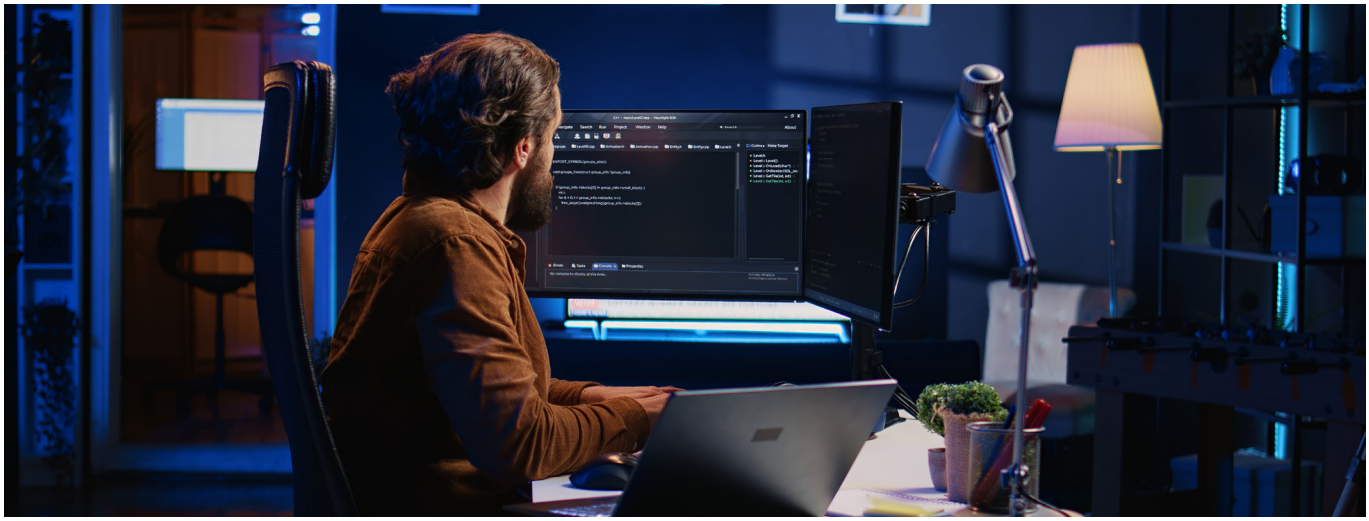
Complementing this is the Single Digital Gateway Regulation (SDGR), which ensures that citizens and businesses can access information, procedures and assistance services online when interacting with another EU country. Its technical backbone – the Once Only Technical System (OOTS) – enables cross-border data reuse between administrations and reduces the need for users to repeatedly submit the same information. The eGovernment Benchmark assesses progress toward these goals through dedicated SDGR indicators, including *Delivery of Output, Cross-Border Delivery of Output, OOTS implementation and Cross-Border ePayments.*

As digital technologies evolve, policy in the EU reflects the commitment to a digital environment that is secure and strategically autonomous. The AI Act, the first comprehensive regulatory framework on AI worldwide, sets risk-based rules for developers and deployers to ensure safety, fundamental rights, and human-centric design. The eGovernment Benchmark's new pilot indicators on AI-powered chatbots align with the Act's objective of fostering transparent, reliable digital interactions within public services.

In line with the EU's resilience agenda, the Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products with digital elements, ensuring that devices are securely designed, updated, and maintained throughout their lifecycle. The Benchmark's Cybersecurity pilot indicator tests 13 security aspects of government websites; in the 2026 edition, an additional element was piloted, with the inclusion of Certification Authority Authorisation (CAA) checks.

In parallel, the emerging EU Cloud Sovereignty Framework promotes secure, trusted and resilient cloud infrastructures grounded in European values. These priorities are reflected in the Benchmark's new Server Sovereignty and Email Server Sovereignty pilot indicators.

Finally, digital accessibility remains a cornerstone of the EU's commitment to inclusion. The Web Accessibility Directive requires public sector websites and mobile apps to comply with a harmonised technical standard that ensures content is perceivable, operable, understandable and robust for all users. This legislative foundation is reflected in the Accessibility Foundations indicator, which assesses whether government websites meet essential accessibility requirements and provide interfaces that support equitable access for all user groups.



Measuring eGovernment progress via life events

What is measured for citizens:

- **Career:** For citizens seeking services in the employment domain, this life event assesses whether they can register as unemployed online; whether information on unemployment benefits and entitlements is available; and whether these can be applied for online. Similarly, assistance services for finding a job are assessed, along with information on retirement as well as online pension claims.
- **Family:** For parents, the services in this life event relate to the social protection domain, covering services around: birth, marriage, personal documents and registering death.
- **Health:** For citizens that require healthcare services, this life event includes services related to obtaining basic healthcare, searching for relevant healthcare providers, applying for the European Health Insurance Card (EHIC), receiving e-consultations, and accessing digital medical records.
- **Justice (Starting a Small Claims Procedure):** A citizen life event related to the justice domain, covering services around: preparing a claim, issuing a claim and monitoring status and appeal.
- **Moving:** For those moving into a new residence, this life event relates to the housing domain, covering services around: find, adapt and move to a new house, and moving and living abroad.
- **Studying:** For students, this life event includes services such as information on the enrolment process in university programmes in the country of origin and abroad; whether application procedures for student loans and other financing schemes are available; and if, for students already enrolled, they can track grades online.
- **Transport:** For car owners, this life event includes services related to the transport domain, covering services around: buying a car, and taxes, certificates, permits and public transport.

What is measured for businesses:

- **Business Start-Up:** For citizens looking to start a business or those already in the process, this life event falls under the economic affairs domain. It encompasses services related to orientation, administrative requirements, basic registration, tax matters, insurance matters, hiring the first employee, and requesting an environmental permit.
- **Regular Business Operations:** For entrepreneurs, this life event includes services from the economic affairs domain. This includes services around: tax and corporate finance, VAT and business changes. In addition, it includes information on working conditions for employees, and whether businesses can change employee status online.

02.

eGovernment as a cornerstone of the **Digital Decade policy programme**

2. eGovernment as a cornerstone of the Digital Decade policy programme

The **digitalisation of public services target** under the Digital Decade policy programme 2030, aims for: a) 100% online accessible provision of key public services and, where relevant, to achieve the possibility for citizens and businesses in the Union to interact online with public administrations; b) 100% accessibility to EU citizens' electronic health records, and c) 100% accessibility to secure electronic identification (eID) means that are recognised throughout the Union, enabling EU citizens to have full control over identity transactions and shared personal data. Point a) translates into two KPIs on online government services for citizens and for businesses, as shown below.[4]

These two Digital Decade KPIs measure whether governments make it possible to deal with them online – one from the citizen's point of view, and one from the business's point of view. The KPI scores are based on the eGovernment Benchmark indicators **Online Availability and Cross-Border Online Availability**, grouped by the seven citizen life events as well as the two business life events. The *Online Availability* indicator is defined as the extent to which informational and transactional services and information concerning these services is provided online and can be reached via main portal websites. The *Cross-Border Online Availability* indicator measures the extent to which informational and transactional services and information concerning these services is provided online for users from other European countries.

eGovernment Benchmark related Digital Decade KPIs

1. Digital public services for citizens: Online provision of key public services for citizens, measured as the share of administrative steps that can be done fully online for major life events. The following life events are considered: moving; transport; starting a small claims procedure; family; career; studying; and health.

2. Digital public services for businesses: Online provision of key public services for businesses, measured as the share of administrative steps needed to start a business and conduct regular business operations, which can be done fully online.

[4]The KPI definitions can be found online: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-policy-programme-path-digital-decade

Figure 1 shows the **steady improvement** of government services that are digitally available for citizens and businesses in the past three years. These scores and their progression indicate that while the scores for citizens still lag behind those for businesses, the gap is gradually narrowing. *Digital Public Services for Citizens* across the EU now stands at 84.6 out of 100, while *Digital Public Services for Businesses* reaches 88.6. To reach the 100%-mark, in practice the EU Member States still need to improve 270 services for national citizens and businesses as well as 610 services requested by cross-border users.

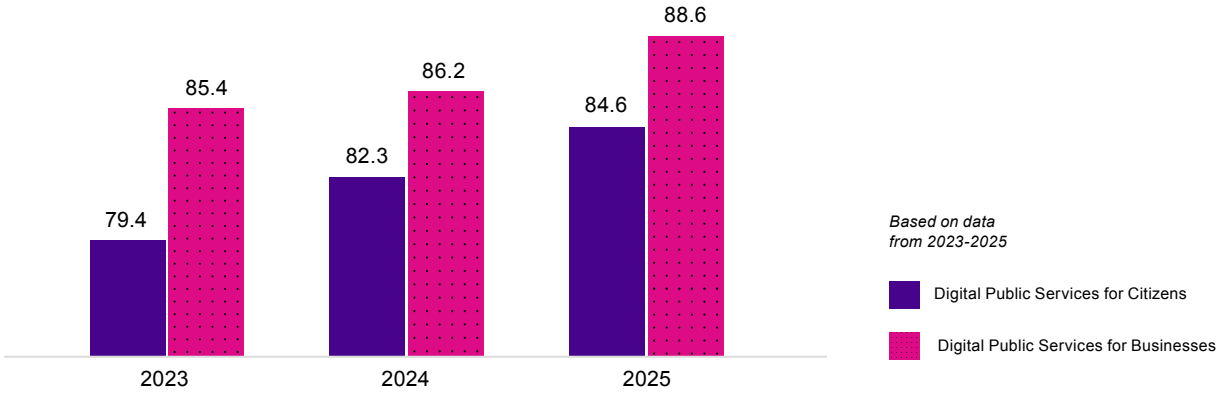


Figure 1: Progress of Digital Decade indicators Digital Public Services for Citizens & Digital Public Services for Businesses

2.1. Digital public services for citizens

As shown in Figure 2, the 2025 score for **Digital Public Services for Citizens** across the EU is 84.6 out of 100. It rose from 79.4 in 2023 and 82.3 in 2024. This represents year-on-year increases of 3.7% and 2.8%. It shows how far governments have gone in making online the services that matter in daily life, for citizens, families, unemployed, students, consumers, and patients. Can people easily handle government tasks, without paperwork or office visits? The indicator evaluates public services linked to the seven citizen life events measured in the eGovernment Benchmark. It checks whether services are available online end-to-end, meaning whether online information is available, whether the service can be fully completed online, and whether the services are offered via a central government portal. It aggregates these elements and assesses whether services work for national users *(the Online Availability indicator) and cross border users (the Cross-Border Online Availability indicator)*.

The 2025 score is underpinned by a 94.0 score on the Online Availability indicator and 75.3 score on the Cross-Border Online Availability indicator. This shows that the vast majority of required administrative steps for national citizens can be completed fully online, and digital services can be reached via government portals. At the same time, the need persists for governments to serve cross-border users digitally too, such as international students, relocating families, tourists in need of medical assistance, etc. **The gap between national and cross-border online availability** suggests that while national services for citizens are widely accessible online, there is still room for improvement in ensuring the same

level of availability for cross-border users. In particular public health institutions and employment agencies face difficulties in providing fully online cross-border services, as indicated by the comparatively lower cross-border availability of health and employment related services. On a positive note, the EU average for cross-border services went up from 68.4 in 2023 and 71.3 in 2024, denoting yearly increases of 4.2% and 5.6%.

Five key public services for citizens are **fully online in all EU Member States for national users**. These services relate to moving places, employment and starting a small claims procedure and have reached the 100% target: "Register new address with additional organisations", "Register you signing out from old municipality", "Check relevant legislation and rights for defending your case", "Check obligations for keeping unemployment benefits" and "Declare personal income taxes". The remaining 63 services need to close the last offline steps for national and/or cross-border users in at least one of the EU Member States. In total, the EU Member States still need to improve 246 services for national citizens and 406 services for cross-border citizens to reach the 100%-mark (averaging 9 and 15 services per Member State).

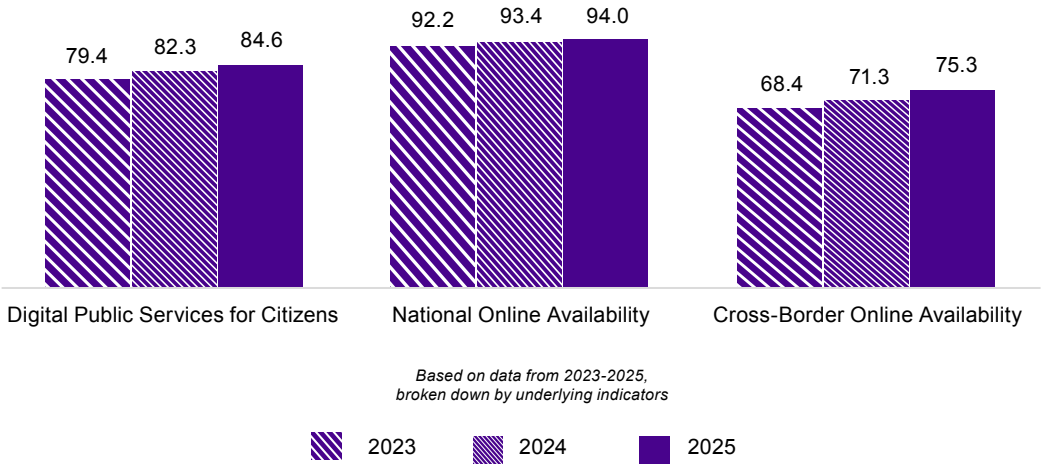


Figure 2 – Digital Decade Digital Public Services for Citizens KPI

As displayed in Figure 3, the **Transport** life event is the highest scoring citizen-related life event with 90.4. This strong performance is explained by a solid 93.0 score on the Online Availability indicator, combined with the highest Cross-Border Online Availability indicator of all life events at 87.8. This is good news for Europeans seeking travel-related services in their own country or needing to obtain a public service in another Member State. Top-performing online services in the EU for car owners and public transport passengers are "Declare vehicle/road tax", "Obtain permit for toll roads or vignettes" and "Obtain public transport tickets (standard tariff)", scoring all above 94.0 for both Online Availability and Cross-Border Online Availability (where this applies).

In second place is the **Moving** life event with 89.2. This digitalisation level is primarily driven by a near-perfect Online Availability score of 96.8, and a considerable increase in Cross-Border Online Availability, which went up from 78.2 to 81.6. People moving places within one Member State can administer most services online. However, municipalities and other competent authorities rely on fewer digital solutions for citizens who move across two EU countries, with "Register new address in municipality register" and "Obtain proof of residence", achieving the lowest scores in this life event, respectively 67.7 and 67.8 for Cross-Border Online Availability.

The **Studying** life event also ranks among the top performers, achieving 89.1 in 2025. The online higher education services part of this life event increased from 86.4 in the 2024 assessment. This performance is supported by a 95.9 score for the Online Availability indicator. A relatively high score of 82.4 for Cross-Border Online Availability also shows that many ministries, agencies and universities are well-attuned to welcoming international students. For example, students can use online channels across Member States to "Register in higher education" and "Obtain recognition of diploma declaration, certificates or other proof of studies or courses", at 89.6 and 86.7 for Cross-Border Online Availability.

The **Career** life event scores 82.8, an increase from 78.5 in 2024. Employment agencies and other service providers in the work and pension domain continue to improve on the Online Availability pillar, now at 95.8. The lower overall score is due to the performance of 69.9 on the Cross-Border Online Availability, albeit again higher than the 63.8 the year before. To improve the online user journey, most efforts are needed for the lowest-performing services, to "Register circumstances that impede you from looking for work" and "Appeal against decision when unemployment benefits are not granted", scoring 47.6 and 52.1 on this indicator.

Although the **Family** life event obtains a comparable score of 82.4 in 2025 with respect to 2024, the story is different. It is one of the life events in which the service levels between Online Availability and Cross-Border Online Availability are less far apart, still 87.7 and 77.2, respectively. The lagging civil registries by municipal bodies are a priority, such as for persons that need to "Register parental authority (e.g. with court in case not married)" or "Register with civil/local registry in order to get married or to close a civil partnership", currently at 71.2 and 72.6 for Online Availability.

The **Justice** (Starting Small Claims Procedure) life event ranks as the second lowest scoring life event with 82.1 in 2025. Increasing from 81.0 in 2024, the year-on-year improvement is small for consumers with a dispute, such as when they receive a damaged product ordered online. Online Availability reaches 94.9, which is contrasted by the 69.2 for Cross-Border Online Availability. Although the first application steps of the European small claims procedure have been improved in many Member States, it

is much harder for consumers to “Monitor the status of a case” and “Appeal against a court decision” once they have filed a claim up to €5,000 against a person, organisation or business based in another EU country. These lowest-performing services score 53.6 and 55.6 on Cross-Border Online Availability respectively.

As in previous years, the **Health** life event records the lowest score among all life events in 2025, with 76.4. On a positive note, a year-on-year increase of 3.8% was registered. However, digitalisation is not accelerating as much as the previous year, with the indicator having improved by 6.1% from 69.4 in 2023 to 73.6 in 2024. The Online Availability indicator continued to grow, now standing at 94.0. The Cross-border Online Availability indicator also rose, but despite the annual increase from 55.1 to 58.9, cross-border service delivery for health services stands at the lowest level among all life events. Among all cross-border services evaluated under the Health life event, the service to “Apply for e-consults with a hospital doctor (tele-consultation)” stands out as the most underperforming, at 27.0 for Cross-Border Online Availability. This service entails providing citizens with the necessary information and digital channels needed to consult hospital-based medical professionals remotely (e.g., discussing test results, scans, medical concerns). Despite their major cost saving potential, it is nearly impossible for EU citizens residing or traveling in another Member State to access tele-consultation services.

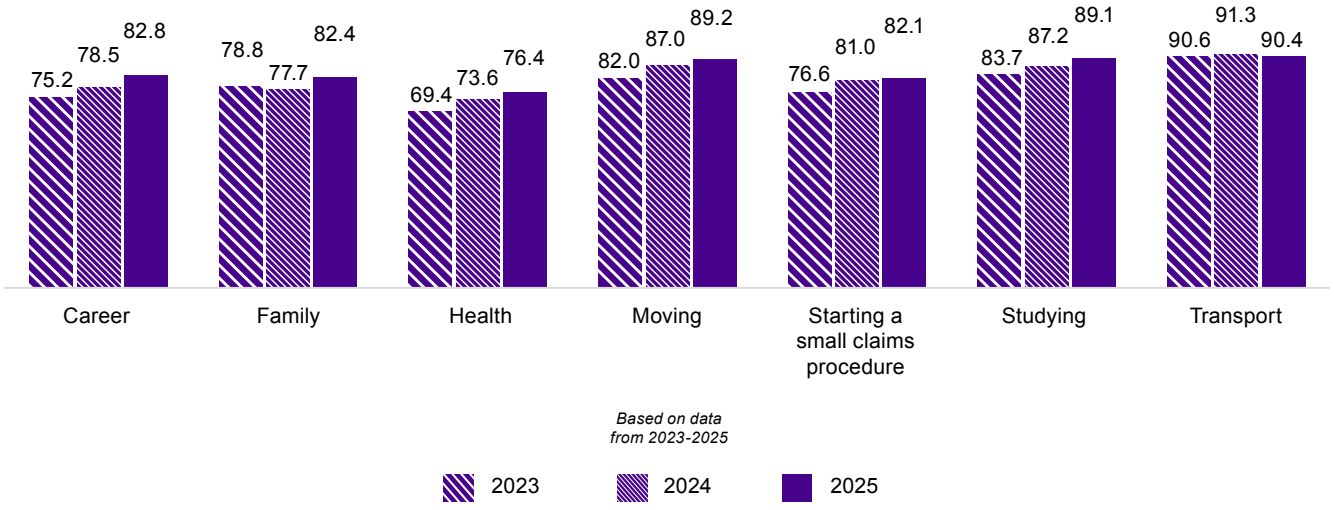


Figure 3 – Life event scores in the Digital Decade Digital Public Services for Citizens KPI

2.2. Digital public services for businesses

The latest eGovernment Benchmark data reveals that the score for Digital Public Services for Businesses across the EU has steadily increased: from 85.4 in 2023, to 86.2 in 2024 and 88.6 in 2025. This equals year-on-year increases of 0.9% and 2.7%. As in previous years, government services for businesses have clearly advanced towards the 2030 target, while room for further improvements remains. This indicator shows how widely it is possible for businesses to deal with governments digitally, including when operating in other EU countries. Can companies interact with governments online, within and across borders? This KPI focuses on public services needed for entrepreneurs that start, run, and grow businesses. It checks whether service information is available online, procedures are fully digital, not partly paper-based, and companies can operate across borders in the EU without unnecessary red tape.

As displayed in Figure 4, the overall KPI score is underpinned by a 98.8 score on the Online Availability indicator and 78.4 score on the Cross-Border Online Availability indicator. This means that almost all public services needed to start and run a business are fully available online for national entrepreneurs. In contrast, entrepreneurs operating across borders face the most digital barriers. Similar to citizen-related services, the gap between national and cross-border online availability suggests that while national public services are widely accessible online there is still room for improvement in ensuring the same level of availability for cross-border business affairs. Necessary advancements will ensure that entrepreneurs residing outside their home country within the EU can efficiently navigate administrative procedures. Enhancing this access will not only support business mobility and regulatory compliance but also contribute to a more integrated European economy.

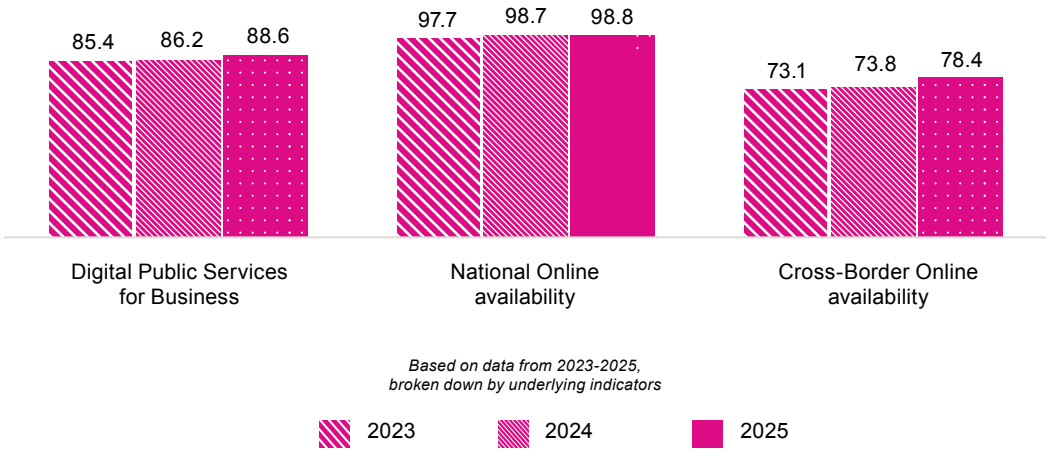


Figure 4 – Digital Decade Digital Public Services for Businesses KPI

Two key public services for businesses are **fully online in all EU Member States for national users**. These are the informational services “Check requirements for starting a business” and “Get guidance with how to explore financial possibilities”. While they have reached the 100% target, they apply to national businesses only and do not require transacting online. The remaining 26 public services need to digitalise final transactional steps for national businesses and/or have to implement such online services for businesses from other EU countries – in at least one of the EU Member States. In total, the EU Member States still need to improve 24 services for national businesses and 204 services for cross-border businesses to reach the 100%-mark (averaging 1 and 8 services per Member State).

An examination of the two underlying life events shows that the strong KPI performance is particularly driven by services in the Regular Business Operations life event, which achieves 89.9 in 2025, improved from 87.7 in 2024. The Online Availability indicator for this life event reaches an impressive 99.1. In fact, 7 out of 11 Regular Business Operations services are fully accessible to national entrepreneurs online across the EU, including tax-related services such as “Declare corporate tax”, “Declare social contributions” and “Declare VAT”. Among the least digital service is “Appeal against VAT decision”, with 96.3 on average for national businesses and 79.6 for cross-border Value Added Tax transactions. Although possible for all nationally located companies, “Report the termination of business activity, excluding

involvement of insolvency or liquidation procedures" is least available online for cross-border entrepreneurs, at 66.4.

Business Start-Up life event services achieve a score of 87.3, up from 84.8 in 2024. This performance is driven by high scores in the underlying Online Availability indicator, with a score of 98.5. Notably, 7 of the 17 national start-up services are fully online, such as initial registrations with the tax and social security agencies, reflected in "Obtain tax identification card/number", "Obtain VAT collector number" and "Register with Social Security Office". Once again in contrast, the Cross-Border Online Availability indicator achieves a score of 74.2, although higher than the 71.2 in the previous assessment. Governments particularly struggle to provide social security-related services to start-ups, for instance aiming to digitally "Apply for a PD A1 (certificate of coverage)", an official document proving which country's social security legislation applies to employed persons posted to another EU. Another insufficiently digitalised service is "Obtain a pollution/environmental permit", which particularly underperforms in terms of Cross-border Online Availability, acquiring only 46.6 across the EU in 2025.

The benefits of meeting the 2030 Digital Decade targets

For citizens:

- Meeting the Digital Decade targets would significantly improve how citizens interact with public administrations by making services available fully online, faster, and more accessible. Digital public services reduce the need for travel, waiting times, and paper-based procedures, allowing people to complete administrative tasks outside office hours and receive outputs electronically. Over their lifetime, most people interact with nearly all key public services, meaning time and cost savings affect a large share of the 330 million Europeans.
- For example, in Austria, collective time savings for citizens using digital services are estimated between 86 and 114 million hours, assuming 1.5 to 2 hours spent travelling to and from government office appointments and 57 million visits annually.

For businesses:

- For businesses, achieving the Digital Decade targets primarily reduces administrative burden and red tape. Fully online procedures eliminate, where possible, the need for physical identification and in person visits, lowering compliance costs and lost productivity, especially for Micro Enterprises as well as Small and Medium-Sized Enterprises (SMEs), which make up 99%of EU enterprises.
- For example, a European Commission study (2024) pinpointed the cost and time savings from using the Once-Only Technical System (OOTS) by SMEs and self-employed workers. SMEs currently spend about an average of €10,000 on their administrative procedures. They could reduce their expenditures by 53% and reduce 6.4 weeks from an average of 14.4 weeks on the entire procedure, representing a 44% reduction. Self-employed workers who currently spend roughly €2,500 could lower their costs by 59% as well as save 5.4 weeks of the average 10.2 weeks to complete the administrative procedures, a 53% reduction.

For governments:

- Governments benefit through lower unit costs, automation, and more efficient use of staff time, freeing resources for higher value tasks. Digital services reduce paper consumption, printing, and physical processing, contributing to sustainability goals and cost savings.
- For example, the Joint Research Centre of the European Commission estimated that improved interoperability would save EU businesses about 30 billion hours and €568 billion annually when completing core interactions with the administration in 2019 – such as paying taxes, registering property, and more. For public sector bodies in the EU, the same improved interoperability can reduce general government production costs (with 0.3 percentage points of GDP), increase general government revenues (with 0.07 percentage points of GDP), and reduce general government expenditures (with 0.6 percentage points of GDP).

03.

Complementary indicators for **effective digital public services**

To complement the Digital Decade KPIs on fully online public service delivery for citizens and businesses by 2030, the eGovernment Benchmark also examines a set of additional indicators that capture how efficient, transparent, supportive and accessible online services are in practice. They are Pre-Filled Forms, Transparency of Service Delivery, Design and Personal Data, User Support, and Mobile Friendliness. These indicators highlight conditions that must be in place for citizens and businesses to complete procedures smoothly and confidently, complementing the two Digital Decade KPIs on digital public services.

3.1 Pre-filled forms

The Pre-Filled Forms indicator measures the share of administrative steps that present pre-filled data, already known to public administrations, in online forms to the user. In other words, it shows how often citizens or businesses do not have to re-enter information that the government already has (e.g., names, addresses, company details) because the system fills it in for them using trusted government databases. This indicator, which is derived from the eGovernment Benchmark's Pre-Filled Forms indicator, provides a single score that reflects how many services requesting data through an online form present users with information that public administrations already hold.

As shown in Figure 6, the indicator rises to 75.9 in 2025, up from 70.9 in 2024, representing a yearly increase of 7.1%. All life events record improvements, demonstrating that citizens can increasingly use online forms in which key information is already filled in for them. The biggest improvements were seen in Family (70.7; yearly increase of 14.4%) and Career (85.8; yearly increase of 9.9%), whereas Regular Business Operations (91.4; yearly increase of 4.9%) is the highest-scoring life event overall. By contrast, Transport and Justice continue to be the domains with the lowest levels of pre-filled information. While transportation services improved faster than the average (54.4; yearly increase of 7.3%), the pre-filling of forms for consumers who start a small claims procedure lags behind the EU average, with a lower year-on-year growth rate as well (56.7; yearly increase of 2.9%). Taken together, these developments indicate steady progress across all government sectors, while also pointing to areas where pre-filling capabilities in public services remain limited.

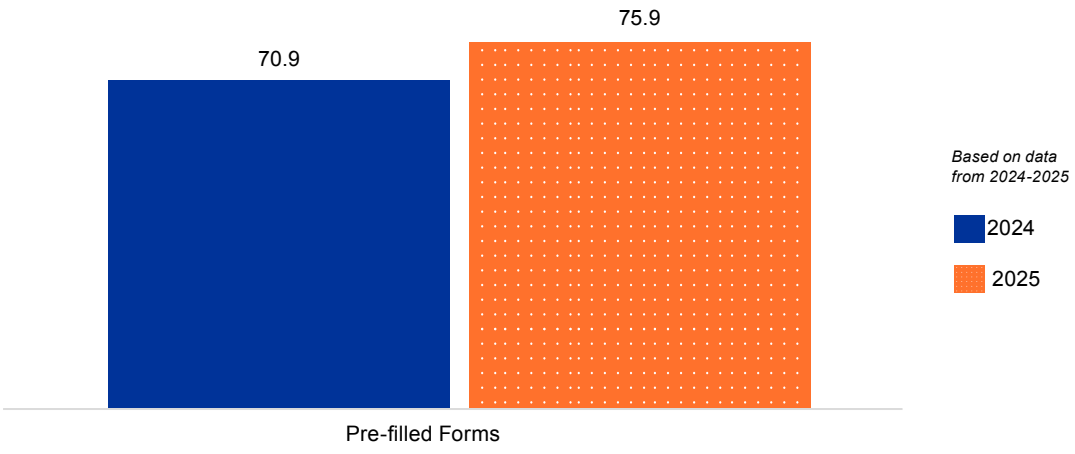


Figure 6 – Pre-Filled Forms

3.2 Transparency of service delivery, design, and personal data

The Transparency of Service Delivery, Design, and Personal Data indicator looks into the extent to which service processes are transparent, services are designed with user involvement and users can manage their personal data. It is composed of three sub-indicators whose combined score reflects the overall transparency of public services. The Transparency of Service Delivery sub-indicator captures whether users are informed about what to expect when completing a service, including the process steps and indicative or legal timelines. The Transparency of Personal Data sub-indicator evaluates the degree to which portals allow users to access, correct and monitor the personal data held about them. Finally, the Transparency of Service Design sub-indicator examines the information provided about how digital services and related policies are developed, and the opportunities offered for users to contribute to these processes.

Figure 7 shows that the combined transparency indicator remains stable in 2025, standing at 69.6 points, compared with 69.5 in 2024. Most life events show only marginal differences compared to 2024, indicating broadly stagnant transparency practices across the EU. The Regular Business Operations life event records the most notable increase (74.0; an increase of 3.2% since 2024) while the Justice and Business Start-Up services have become slightly less transparent over the same period (61.5; decreased by -1.5%, and 72.5; decreased by -1.7% in one year). These decreases are mainly attributable to newly assessed government portals in the Transparency of Personal Data and Transparency of Service Design sub-indicators. In 2025, this means Justice services still rank lowest, a position these have held since 2021. This suggests that services relating to small claims procedures have consistently demonstrated the most need for improved transparency in clarifying service processes, the handling of user's personal data, and user involvement opportunities.

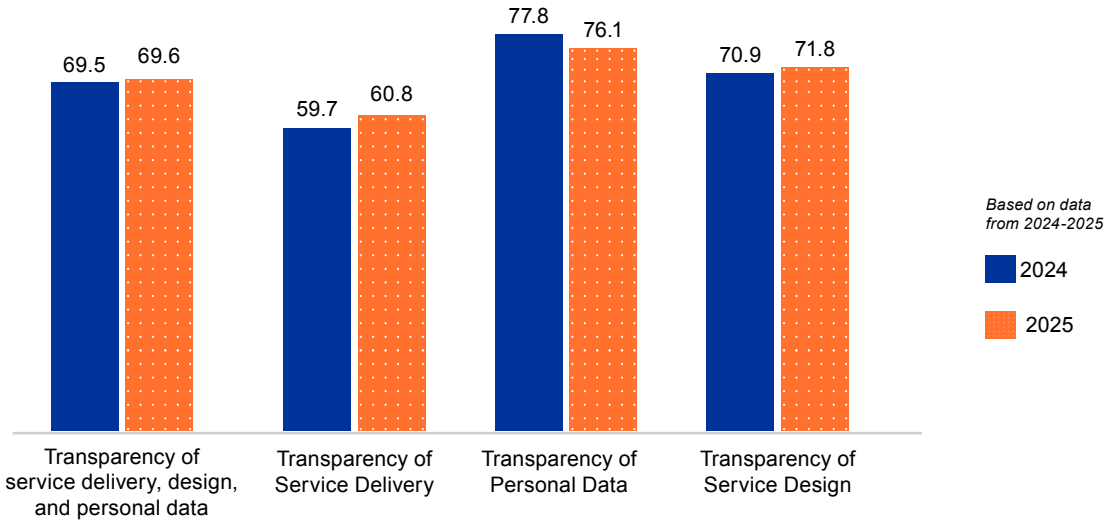


Figure 7 – Transparency of Service Delivery, Design, and Personal Data, and underlying eGovernment Benchmark sub-indicators.

When looking at the individual sub-indicators, it becomes clearer which types of transparency features require the most attention. Transparency of Service Delivery, while still the lowest scoring sub-indicator overall, improved to 60.8 (an increase of 1.9% in one year), driven mainly by improvements in the Regular

Business Operations, Health, and Career life events. Transparency of Personal Data decreased to 76.1 (a decrease of -2.2% in one year), with the steepest declines in Career and Business Start-Up services. Transparency of Service Design reached 71.8 points (an increase of 1.3% yearly), with the most notable increases found in the Regular Business Operations and Studying life events, indicating growing efforts to communicate how digital services are developed and where users can contribute to those processes.

3.3 User support

The eGovernment Benchmark's User Support indicator consists of the sub-indicators User Support and Cross-Border User Support. It measures the availability of online support, help features, and feedback mechanisms for both national and cross-border users. It aggregates multiple elements, namely the extent to which government portals contain Frequently-Asked-Questions (FAQs) sections, demos, contact information towards a responsible department and other channels of communication, feedback mechanisms, discussion fora for national and cross-border users, complaint procedures, as well as help functionalities.

As displayed in Figure 8, in 2025 the overall User Support indicator achieved 90.0 points, marking an increase of 1.4% compared to 2024. Most life events show only minor changes, indicating broadly stable support features across online portals in the EU. Notable increases can be found in the Health domain (90.1 points; an increase of 5.1%) and Family life event (92.1 points; an increase of 4.7%).

two well-performing life events show slight decreases: Transport services (88.6 points; a decrease of -1.7%) and Business Start-Up (91.4 points; a decrease of -1.0%). These smaller declines may be explained by some of the newly assessed portals that ended up scoring less than average. Justice remains the lowest-scoring life event, with below-average growth, suggesting that EU citizens continue to face more difficulty obtaining help or support when interacting with justice-related digital services (79.6 points; an increase of 0.8%).

The National User Support sub-indicator remains high at 96.1 points, despite a slight decrease compared with 2024 (a decrease of -0.7% in one year). The strong score reflects the fact that most national portals continue to offer a broad range of support features, such as clear FAQs sections, live support functionalities, and accessible feedback mechanisms. Cross-Border User Support has advanced to 84.0 points (an increase of 3.9%), indicating that most overall growth comes from improved support for international users. Here, services in the areas of Family (an increase of 12.5%) and Health (an increase of 13.3%) contribute most to this increase, showing enhancements in the availability of support channels for families and patients accessing services from another EU country.

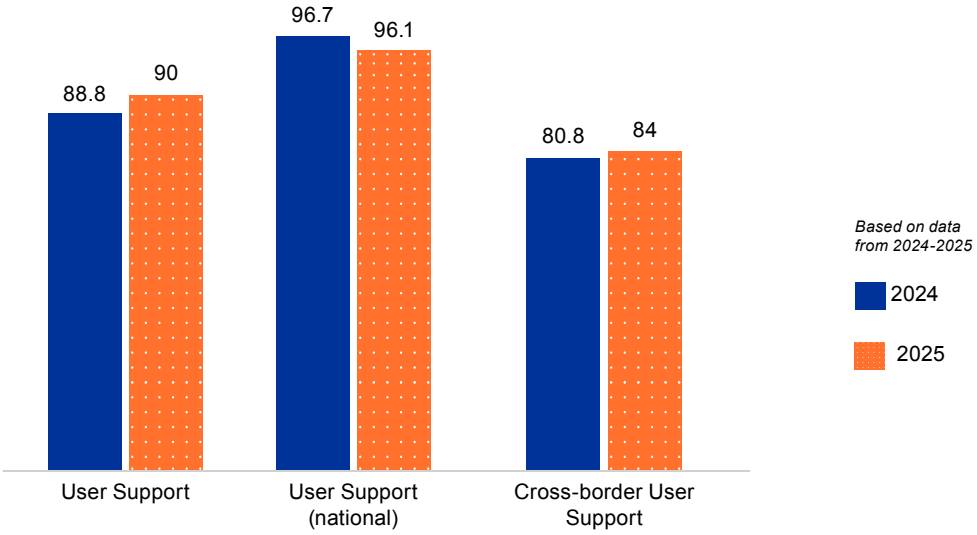


Figure 8 – User Support and underlying eGovernment Benchmark sub-indicators.

3.4 Mobile friendliness

Mobile Friendliness assesses national service websites on their responsiveness to mobile screens through automated tooling. As depicted in Figure 9, this indicator stands at 97.4, representing a year-on-year increase of 1.4%, from 96.1 in 2024. Mobile Friendliness remains highly mature, suggesting that most assessed EU services are provided through interfaces that are compatible with mobile devices. When looking at the nine life events, the mobile friendliness of government websites has steadily improved. Regular Business Operations (99.6), Business Start-Up (98.3) and Family (97.6) are the highest-scoring life events, illustrating that these domains generally offer strong mobile-responsive interfaces. In a time where mobile phones are the main device for users to manage their digital life, full coverage of the Mobile Friendliness indicator remains a worthy pursuit.

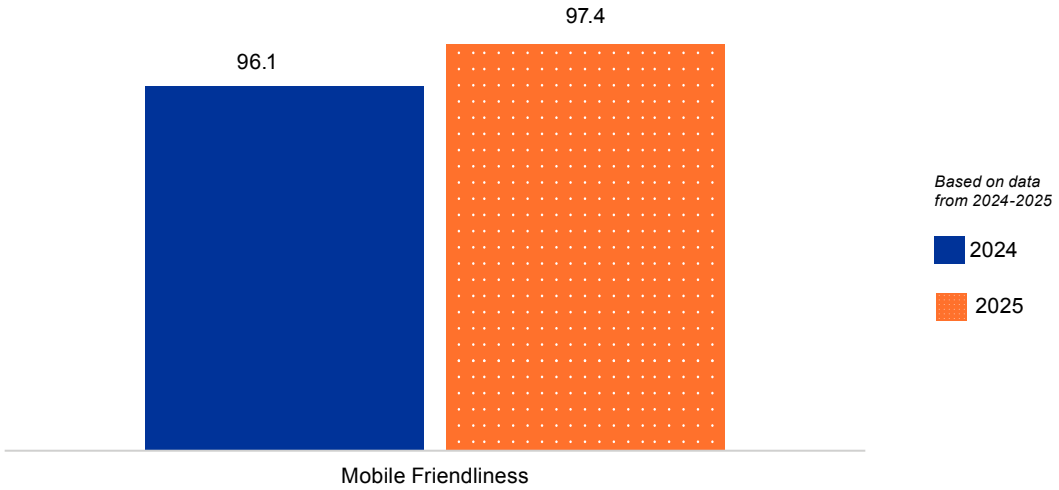


Figure 9 - Mobile Friendliness

04.

Key **priority areas**

4. Key priority areas

Eurostat data shows that 76% of Europeans who used the internet in the last 12 months also used online government services, underlining how widely digital public services are used among internet users. As reliance on these services grows, three priority areas stand out as particularly important for achieving the Digital Decade targets and ensuring high quality, secure and resilient digital public services across the EU. First, the growing use of Artificial Intelligence (AI) presents new opportunities to improve user experience and provide more intuitive support to citizens and businesses. Second, the increasing exposure to cyber threats highlights the need for stronger security measures to safeguard government portals and protect the personal data of citizens and businesses. Third, maintaining digital sovereignty has become essential as governments depend on complex infrastructures that are often operated by non EU providers. In addition to existing indicators, the 2026 edition of the eGovernment Benchmark explored these areas through new pilot indicators, presented in the following sections.

4.1 Artificial Intelligence (AI): a promise for uplifting the user experience

AI is emerging as one of the most influential technologies shaping how people access and experience online public services. Its rapid uptake across sectors has made the potential of AI highly visible, prompting national government bodies across the EU to explore how AI-enabled tools can support users most intuitively when navigating public services. Notably, public administrations are also beginning to adopt AI powered chatbots to provide live support for public services. To capture this development, the availability of live support functionality, and whether this support is delivered through an AI chatbot, was assessed across all national portals landscaped.

The average for **live support functionality** — which captures both human based live support and AI powered live support — decreased from 60.5 to 56.4 (out of 100). A similar downward trend is visible in the availability of **AI powered live support,** which dropped from 43.0 to 40.3 (out of 100). As a result, the share of government portals that meet both conditions — offering live support and delivering that support through an AI chatbot — stands at 23% in 2025, compared to 26% in 2024.

The decreases in both indicators on live support stem from changes in how life events were classified compared with the previous edition (eGovernment Benchmark 2025). For the question on the availability of live 'click-to-chat' support with a human or chatbot response, some cases previously marked as offering this functionality were reassessed as not meeting the criteria, contributing to the decline. For the question on whether available live support is provided by a chatbot rather than a human, the decrease similarly results from reclassification, as well as cases moving between 'not applicable' and other answer categories. Such shifts make previously excluded assessments scorable, and they enter the calculation as 'No', which lowers the indicator.

The observed decrease in AI powered live support availability is primarily the result of changes in how individual life events were classified compared to the previous edition. Several cases that were previously marked as offering chatbot based live support were reassessed as not fulfilling the criteria this year. In addition, some cases that were previously marked as not applicable are evaluated as not offering such functionality in this year's edition, and a small number shifted from being assessed as offering the functionality to not being applicable. These classification changes collectively contribute to the downward trend reported in the indicator.

Adoption levels also vary substantially across Member States. Some countries offer AI chatbots on nearly all assessed life events for their national portals, while others do not provide any AI enabled support functionality. These uneven patterns illustrate that while several Member States are rapidly scaling AI enabled assistance, others have yet to introduce such capabilities into their online public service delivery.

The maturity level of AI powered chatbots is 39.5 (out of 100), indicating that most chatbots are still equipped to handle only basic interactions and offer limited support when users need guidance through multi step procedures. **Escalation options of AI-powered chatbots** also remain underdeveloped. With only 17.3% of chatbots providing a handover to a human agent, users frequently lack an alternative when the AI tool cannot address their request. In addition, the score for **understandable AI-powered chatbots** is 20.2 (out of 100), showing that relatively few chatbots are able to translate information into clear and accessible language. Together, these findings suggest that while AI enabled support features are present on many portals, their capacity to provide reliable, comprehensible and complete assistance remains limited.

Inclusiveness is also constrained. **Multilingualism support of AI powered chatbots** shows that chatbots offer 3 to 4 languages on average. While most chatbots function only in the national language and sometimes in English, some portals provide wider coverage, such as the Greek chatbot, which offers support in all official EU languages. This means many users who do not speak the national language may experience difficulties when they require assistance to complete public services. Moreover, **cross border user support of AI-powered chatbots** stands at 18.5 (out of 100), showing that only a small proportion of chatbots are equipped to assist users from another country. As a result, many AI enabled support tools remain closely tied to national contexts and offer limited guidance for mobile citizens, students, international workers or businesses seeking to access services outside their home country.

The assessment highlights two notable good practices, with Greece and Portugal achieving the strongest overall performance across the chatbot-related indicators. **Greece's digital assistant chatbot** (mAigov), available on the main government portal gov.gr, stands out for its extensive language coverage, offering support in 24 official EU languages as well as additional regional languages. Trained on open data from more than 5,000 administrative procedures, it combines Natural Language Processing technologies with a user-centred design to provide clear explanations, concise summaries, and cross-border information. **Portugal's virtual assistant** on *gov.pt* similarly demonstrates advanced implementation. It supports six official EU languages and six additional non-EU languages and offers both written and voice interaction. Together, these assistants illustrate how broader language availability, high maturity levels and cross border support can significantly enhance the potential of AI powered user support.

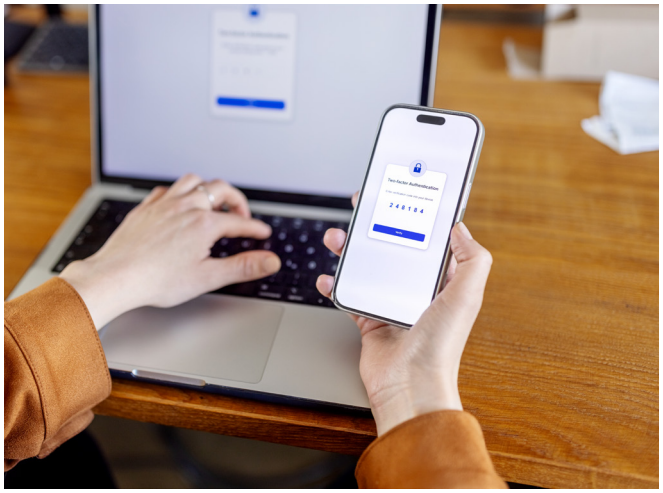
Broader research further underscores the relevance of AI-powered user support in public service delivery. According to the Digital Decade Eurobarometer, 84% of Europeans expect digital technologies to significantly influence how they access public services online. This highlights the growing demand for clear, reliable, and easy to use digital guidance when completing (online) public services. Moreover, a recent OECD report (2025) shows that AI is increasingly used in public service delivery to help governments provide information, support user interaction and automate routine processes, particularly

through AI-powered chatbots. It further notes that chatbots can enable faster access to relevant information and more responsive user interaction, yet their effectiveness depends on strong safeguards, including transparency, clear governance frameworks and measures to mitigate risks such as misinformation. An EU study (2024) similarly identifies AI-powered chatbots to be one of the most promising and most used AI applications in the public sector, emphasising that they are most effective when supported by high-quality and interoperable datasets and sufficient human oversight to manage risks.

The upcoming AI Act will also shape how AI systems are used in public service delivery. Under this new framework, AI-powered tools that support interactions between citizens and public administrations are classified as high-risk. Accordingly, chatbots will need obligations that are designed to meet requirements related to transparency. These obligations are designed to ensure that citizens know whether they are talking to an AI system or are seeing content generated by AI. In addition, AI systems used to evaluate eligibility for essential public services or benefits and to triage emergency calls and dispatch first response fall under high risk application areas and must meet high risk requirements. For online public service delivery this means that AI systems must be developed and deployed with strong safeguards to ensure that automated tools support rather than undermine the reliability and quality of digital public services.

4.2 Cybersecurity: a need for safer eGovernment services

Cybersecurity has become a crucial factor in the reliability of online public service delivery. That is because governments increasingly operate critical systems online and process personal data from citizens and businesses alike. At the same time, public administrations face a rapidly evolving threat landscape, with cyberattacks targeting government institutions and citizen data. EU initiatives like the NIS2 Directive and the Cyber Resilience Act have raised standards for more robust online protection across public administrations, while the Cyber Solidarity Act put in place a framework for improving resilience and response to cyber threats. This underlines that achieving fully online public services depends not only on availability, but also on ensuring these services are secure and trustworthy for users.



The overall *Security* indicator score in the EU improved from 41.9 to 46.6 (out of 100) between 2024 and 2025. However, still only 49.9% of all tests (described in more detail in the rest of the section) receive a pass result and no government website across the EU meets all 13 criteria. **Content Security Policy** is the lowest performing test with only 3.6% of the assessed websites enforcing it, meaning that most government websites remain vulnerable to cross-site scripting or clickjacking attacks. **Subresource Integrity** performs similarly poorly at 5.9%, indicating that only a small share of websites is protected against attackers modifying the contents of JavaScript libraries. Internet standards also require attention, as the tests for **IPv6, DNSSEC**, and **HTTPS** all score below 25% and are therefore not yet widely adopted across government websites. By contrast, strong performance is visible in **Cross-origin resource policy** and **Cross-origin resource sharing**, scoring 98.6% and 100% respectively. Together, they show that almost all government websites prevent their resources from being embedded on unauthorised external sites and all government websites prevent foreign sites from reading their content or accessing private user information.

This year's assessment also introduced three pilot indicators that provide additional insights into (cyber)security of government websites. First, **Certification Authority Authorisation** shows that only 14.7% of websites restrict which certification authorities may issue certificates for their domain. For the majority of websites, configurations are either absent or incomplete, meaning that restrictions are not clearly or fully defined. This increases the risk of certificate mis-issuance, which could enable attackers to impersonate official portals, intercept traffic, or conduct phishing attacks that appear legitimate to citizens and businesses.

Second, **Phishing awareness** information is available on 48% of national portals, meaning that only about half actively guide users in recognising phishing attempts. This includes resources such as tips for spotting phishing attempts, explanations on how to verify that a domain is legitimate (e.g., checking HTTPS or common warning signs), or public awareness materials like articles, guides and campaign messages.

Third, results for the **Domain Verification Suffix** test show that not all portals use a trusted government domain ending. Of the 6,982 national services URLs for which this test could be applied, 76% did not use an official government domain suffix, meaning that users cannot always immediately verify whether a website is an official government portal.

Security performance varies widely across Member States. The Netherlands stands out as a clear frontrunner with an overall score of 79.7 (out of 100), reflecting long-standing national efforts to adopt security standards. However, performance varies considerably

across the EU. While some countries score well above the EU average of 46.6 (out of 100), others fall significantly below it, highlighting substantial disparities. This indicates that some countries have already embedded cybersecurity standards, but significant improvements are needed across all countries.

Other research substantiates the importance of strengthening cybersecurity on government websites. A Eurobarometer report on the Digital Decade 2025 shows that 81% of Europeans consider improved cybersecurity and better protection of online data essential for their daily use of digital technologies. Similarly, findings from the ENISA Threat Landscape 2025 highlight the vulnerability of the public sector: public administrations were the most targeted sector, accounting for 38% of observed cyber incidents. In sum, government bodies have ample room to improve the cybersecurity of government websites across the EU. Applying cybersecurity standards, protocols and policies across Member States will minimise risks. Moreover, eGovernment users can benefit from clear awareness materials on national portals to recognise online threats, for example guidance on how to identify phishing attempts, suspicious domains or unsafe links. Closer coordination between Member States and the European level may help in this regard. Within the current voluntary cooperation framework, shared testing tools, common approaches, and the exchange of lessons learned can help administrations identify vulnerabilities more quickly and strengthen their resilience.

4.3 Sovereignty: ensuring public sector digital continuity

Digital sovereignty has become an increasingly prominent objective of the EU as public administrations grow ever-more dependent on complex digital infrastructures. The ambition of full online availability of public services requires resilient digital infrastructures that operate under reliable European oversight. Government portals and their underlying data systems rely on hosting providers, cloud services and network operators that may fall under non-EU jurisdictions. When these critical infrastructures are operated by non-EU providers, they can create dependencies that affect strategic autonomy and weaken the long-term resilience of Europe's digital public infrastructure. Strengthening digital sovereignty is therefore essential to ensure that citizens and businesses can rely on public services that remain resilient over time and operate within a trusted European environment.

In this light, the European Commission recently introduced a new EU Cloud Sovereignty Framework designed to strengthen Europe's digital autonomy and reduce reliance on non-EU cloud and hosting providers. In parallel, the European Commission is preparing a Cloud and AI Development Act (CAIDA), aimed at significantly expanding Europe's datacentre capacity in the coming years. These initiatives underscore that cloud sovereignty has become a strategic necessity for ensuring long-term control over critical digital infrastructure.

The eGovernment Benchmark 2026 assessment introduces the Server *Sovereignty* pilot indicator, which targets a specific component of digital public infrastructure: the routing and communication layer that determines how government web and email traffic is transported across the internet. This pilot indicator attributes operational and routing control to the organisations that govern this part of the infrastructure and identifies the jurisdiction of their ultimate owners.

This assessment begins by identifying the Autonomous System Number (ASN) associated with the IP server address of a government website. The ASN identifies the organisation that owns and operates the network level infrastructure – the IP address ranges and

routing systems that ultimately determine how traffic reaches the website. This unique identifier is assigned to a network that follows a single routing policy and is used in global internet routing to show which organisation controls a given IP address range. Because ASNs are allocated by Regional Internet Registries and announced through the Border Gateway Protocol (BGP), they provide an objective and verifiable means of attributing operational control to a specific network operator. Using IPinfo.io, it is possible to retrieve the ASN linked to the website's hosting environment. In addition to identifying the ASN associated with the website's hosting environment, the assessment applies the same ASN based logic to the domain's email infrastructure. For outbound email, Hosting Checker is used to parse the domain's SPF (Sender Policy Framework) records, identify the providers authorised to send email on behalf of the domain, and map the authorised IP ranges to their corresponding ASNs. This reveals the network operators that control outbound mail delivery and therefore govern the routing environment in which outgoing messages are handled. For inbound email, the script analyses the domain's MX (Mail Exchanger) records, retrieves the underlying mail server IP addresses, and maps these to their ASNs to identify the operators responsible for receiving and processing incoming mail traffic.

Routing works much like an international postal system, except instead of letters, it is a user's request to access a government website. When someone enters the web address of, for example, their national tax portal, their request does not travel straight to the government's server. It is passed through several large 'postal hubs' on the internet, known as Autonomous Systems, each operated by an organisation responsible for delivering traffic within its own range of IP addresses.

While many Autonomous Systems handle the request in transit, the Autonomous System Number we identify is the one associated with the website's destination IP address – the final 'postal hub' responsible for receiving and delivering the traffic. The destination Autonomous System determines which organisation's network infrastructure the government website actually sits on: whose IP space it uses, whose routing rules it follows, and which jurisdiction governs its operation. It is this final operator that our sovereignty pilot assessment focuses on.

Once the Autonomous Systems organisation is identified, the assessment determines the headquarter country of its ultimate beneficial owner (UBO). We focus on the country because this is where the operator's legal obligations originate and where jurisdictional control is exercised, making the UBO's country of incorporation the most reliable basis for assessing whether the organisation is bound to EU law or exposed to non EU legal frameworks.

By 'ultimate corporate ownership', we refer to the highest controlling entity in a company's ownership chain, which is typically the publicly listed parent corporation or private holding company that exercises substantial control over subsidiaries. This includes companies where the largest or majority shareholders (i.e., shareholders or investor groups that collectively hold more than 50% of a company's voting rights or effective control) are non EU institutional investors or corporate entities. Due to the absence of a single consolidated, open-source register that reliably captures global corporate ownership structures, this information was gathered through a combination of publicly available sources. These included international corporate databases (e.g., OpenCorporates, Beneficial ownership registers interconnection system (BORIS), Yahoo Finance, etc.), provider maintained ownership disclosures, and country

specific materials such as company registries, press releases, and reputable news reporting. Taken together, these sources allowed the identification of the ultimate beneficial owner (UBO) of each ASN operating organisation, focusing on the highest institutional owner in the corporate chain unless control could be clearly attributed to a single individual. While each ASN entity is formally governed by the laws of the country in which it is incorporated or operates, its ultimate ownership structure may still create exposure to foreign legal or governmental influence. In cases where the parent company, or even a controlling or majority block of shareholders, is based outside the EU, the entity may be indirectly subject to foreign regulatory pressures, access regimes, or strategic interests, even if it is not directly bound by that jurisdiction's laws. This is especially applicable to corporations based in jurisdictions such as the United States, where national security, intelligence sharing, and disclosure laws (e.g., FISA, Executive Orders, subpoenas) can require companies, and by extension their foreign subsidiaries, to provide data or assistance to government authorities.

Furthermore, the ASN proves a reliable indicator of server sovereignty because, unlike other indicators such as physical server location, it consistently attributes control to the organisation that operates the underlying network. Modern hosting and cloud architectures routinely obscure the physical origin of a service through virtualisation, load balancing, and globally distributed Content Delivery Networks, making location an unstable and increasingly misleading proxy. In contrast, an ASN does not identify a single edge node but the network operator whose routing policies, peering decisions, and legal and regulatory obligations ultimately determine how traffic flows and under which jurisdiction the infrastructure is governed. As a result, ASN attribution offers a far more stable and governance relevant measure of sovereignty than physical hosting location.

For example, if the ASN belongs to Microsoft (a non-EU based entity), even if a website's IP address server block appears registered in Belgium, Microsoft still controls routing decisions (how traffic flows across the internet), peering relationships (connections with other networks), and operational policies for that network segment. Therefore, that network path is placed under Microsoft's operational management and is subject to the legal obligations that apply to the company in its home jurisdiction (i.e., the United States), as well as Belgium and the EU.

Webserver: eGovernment Benchmark results

Based on the ASN of the web server, 62.7% of the 7,332 government websites analysed resolve to an autonomous system operated by an EU headquartered organisation, while the remaining 37.2% are controlled by operators whose ultimate beneficial ownership lies outside the EU. Nine non EU countries were identified in the analysis. One of these was an EFTA member (Switzerland), while the remaining eight consisted of third country jurisdictions: United States, United Kingdom, Israel, Mexico, Canada, China, Australia, and Japan.

In terms of the organisational typology of identified Autonomous System, 37.5% of all sampled websites are ultimately owned by government or public sector bodies, 25.6% by cloud provider companies, 11.3% by ICT provider companies, 9.2% by private equity or investment firms, 6.9% by telecom operators, 6.6% by internet infrastructure providers, 2.2% by nonprofit organisations, 0.7% by financial services companies, 0.1% by media companies, and 0.01% by private business owners.

Germany is the most frequently appearing EU jurisdiction, representing 10.3% of all Autonomous System operators identified and providing the network infrastructure through

which 8.6% of all sampled websites are routed. When excluding instances where German Autonomous Systems appear within Germany's own national sample, they account for 3% of all sampled websites. Among EU owned Autonomous System operators, Serviciul de Telecomunicatii Speciale, the Romanian government authority responsible for telecommunications for public institutions, appears most frequently, accounting for 2.2% of all websites sampled. The Latvian State Radio and Television Centre (Latvijas Valsts radio un televīzijas centrs) follows with 2%, and the Slovak National Agency for Network and Electronic Services ranks third with 1.7%. All three operators appear exclusively within their respective national samples and are not identified as providers for any other Member State.

The United States is the most frequently appearing non EU jurisdiction, representing 6.7% of all Autonomous System operators identified and providing the network infrastructure through which 32% of all sampled websites are routed.

The non-EU organisations that appear the most are also the top three when considering the EU sample, making them the most prominent across Europe. They are all Autonomous Systems with ultimate ownership in the United States. In first place is Cloudflare Inc accounting for 11.7% of all websites, appearing across 26 Member States. In second place is Microsoft Corporation, accounting for 6.5% of all websites, appearing across 22 of 27 EU countries. In third is Amazon Inc accounting for 5.2% of all websites, appearing across 24 of 27 EU countries.

Mail-server: eGovernment Benchmark results

The mail-server sovereignty indicators are based on a smaller subset of the overall 7,332 webserver sample because email routing can only be evaluated for domains that actively operate mail services. For incoming email, this resulted in a sample of 6,230 domains with valid MX records; for outbound email, a total of 6,083 domains contained usable SPF records.

Incoming mail-server indicator

At 60.4%, the incoming mail-server ASN score indicates that a large portion of inbound government email services are handled by network operators whose ultimate ownership is based outside the EU. Providers are identified to be from all EU Member States, as well as 11 non EU countries. Two of these were EFTA members (Switzerland and Norway), while the remaining nine consisted of third country jurisdictions: United States, United Kingdom, Mexico, Australia, Canada, China, Japan, Tunisia, and India.

In terms of the organisational typology of identified Autonomous Systems, 41.0% of all sampled websites are ultimately owned by government or public sector bodies, 29.7% by cloud provider companies, 8.3% by telecom operators, 7.6% by private equity or investment firms, 5.8% by ICT provider companies, 5.4% by internet infrastructure providers, 2.1% by nonprofit organisations, 0.06% by media companies, and 0.02% by financial services companies.

Germany is the most frequently appearing EU jurisdiction in the routing environment for inbound government email. German operated ASNs account for 12.9% of all identified inbound mail server operators and handle the delivery of 10.3% of all sampled domains. When excluding cases where German Autonomous Systems appear within Germany's own national sample, they still account for 3.7% of all inbound mail server pathways.

Among EU owned Autonomous System operators for inbound email, the Department of

Information Technology Services (DITS) of Cyprus appears most frequently, accounting for 3% of all sampled domains. It is followed by the Lithuanian State Centre for Telecommunications (Kertinis valstybės telekomunikacijų centras) with 2.8%, and by Romania's Serviciul de Telecomunicatii Speciale with 2.6%. All three operators appear exclusively within their respective national samples and are not identified as inbound mail providers for any other Member State. Among non EU operators involved in inbound mail routing, Microsoft Corporation stands out as the most dominant, accounting for 26.3% of all sampled websites and appearing across all 27 EU Member States. In second place is Google LLC, accounting for 2.9% of websites and appearing across 22 countries. In third place is Proofpoint Inc., accounting for 1.9% of websites and appearing across 21 Member States.

Outgoing mail-server indicator

With an outgoing mail-server ASN sovereignty score of 50.3%, half of all outbound government email services are operated by providers whose ultimate beneficiaries are outside the EU. The assessment identified operators from 26 EU Member States and from nine non EU jurisdictions. Two of the non EU jurisdictions were EFTA members (Switzerland and Norway), while the remaining seven were third country jurisdictions: United States, United Kingdom, Mexico, Australia, Canada, China, and Japan.

In terms of the organisational typology of identified Autonomous System operators for outbound email, 35.5% of all sampled websites rely on cloud provider companies, followed by government or public sector bodies at 29.7%. ICT provider companies account for 13.2%, private equity or investment firms for 9.8%, and internet infrastructure providers for 5.6%. Telecom operators represent 3.9% of the sample, nonprofit organisations 1.3%, financial services companies 0.8%, and media companies 0.15%.

Germany is the most frequently appearing EU jurisdiction in the routing environment for outbound government email. German operated ASNs account for 11.9% of all identified outbound mail providers and handle the delivery of 7.6% of all sampled domains. When excluding cases where German Autonomous Systems appear within Germany's own national sample, they still account for 2.4% of all outbound mail pathways. Among EU owned Autonomous System operators for outbound email, the French ICT provider Mailjet SAS, whose ultimate beneficial owner is the Swedish ICT company Sinch AB, appears most frequently. Mailjet SAS accounts for 2.26% of the total sample and appears across 21 Member States. The Latvian State Radio and Television Centre follows, accounting for 2.18% of sampled domains and appearing exclusively within the Latvian sample. In third place, the Slovak National Agency for Network and Electronic Services represents 2.03% of the sample and appears only within the Slovakian sample.

The United States is the most frequently appearing non EU jurisdiction in the routing environment for outbound government email, representing 7.6% of all identified providers and supplying the network infrastructure through which 45.5% of all sampled domains route their outbound mail traffic.

The non EU organisations that appear the most in the outgoing mail routing environment are also among the top ranking providers when considering the wider EU sample, making them some of the most prominent operators across Europe. They are all Autonomous System operators with ultimate ownership in the United States. In first place is Microsoft Corporation, accounting for 32.1% of all sampled websites and appearing across all 27 EU Member States.

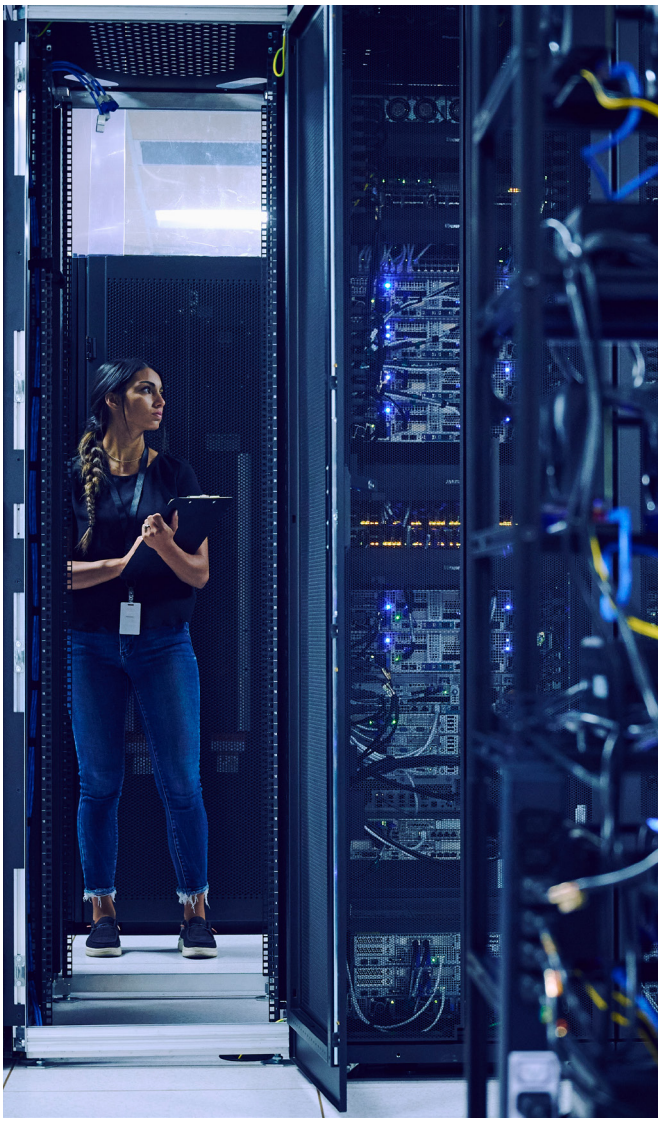
In second place is Google LLC, accounting for 5.12% of websites and appearing across 20 Member States. In third place is Amazon.com, Inc., accounting for 2.4% of websites and appearing across 18 EU countries.

Implications of the eGovernment Benchmark assessment

The implications of these findings point to a notable dependence by government websites and their associated email services on foreign owned network operators at the routing and communication layer. In this setting, sovereignty considerations are not driven by isolated cases where a single ministry uses non-EU providers. Instead, they emerge from the cumulative pattern of multiple EU government websites and email systems making use of non EU network operators.

Because ASNs identify the organisations that operate the underlying network through which traffic is routed, reliance on foreign owned providers means that government communications may fall under the legal and regulatory obligations applicable to those operators. For providers headquartered in jurisdictions with extra territorial access laws, such as the United States, this includes statutory frameworks like the U.S. CLOUD Act, which enables authorities to compel U.S.-based companies to provide certain forms of data when specific legal thresholds are met. This does not imply that such access is happening, but it establishes a potential pathway for lawful requests that would not exist if the service were operated entirely under EU jurisdiction (Jansen et al., 2023).[5]

For example, for business related life events such as Regular Business Operations and Business Start Up, 25% of all incoming mail-server ASNs and 36% of all outgoing mail-server ASNs across the EU are ultimately owned by U.S.-headquartered companies. These services involve communications related to business registration, tax compliance, permits, regulatory submissions, and interactions with public administrations – communications that often carry confirmations, authentication links, notices, or case specific information. Similarly, on the



[5]Jansen, B, Kadenko, N., Broeders, D, Eeten, M. van, Borgolte, K. & Fiebig, T., *Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions, Government Information* Quarterly, Volume 40, Issue 4, 2023, 101862, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2023.101862.

web infrastructure side, 33.6% of all landscaped EU websites supporting the Health life event, covering digital interactions around healthcare access, are hosted on ASNs ultimately owned by U.S. entities.

While the content exchanged through these services may be encrypted, service operators still retain data generated during access – both metadata (e.g., timing, frequency, and destination information) and diagnostic traces (e.g., log files or packet samples governed by the provider's own retention policies and legal obligations). In addition, service availability remains dependent on these operators, which may be affected by outages, misconfigurations, or global routing incidents. Overall, sovereignty concerns arise from the fact that non EU operators can govern data retention and jurisdiction, while also influencing service availability, which is subject to the commercial, regulatory, and political decisions of such actors and may diverge from European interests.

At the same time, the landscape of how Member States host and route their government websites and email services varies considerably across the EU. Certain governments primarily use state owned infrastructures, whereas others depend extensively on third party providers for their public communication systems. This divergence can result in cross border spillover risks. Since government services increasingly depend on interoperable systems and cross border data exchange, inconsistencies in how Member States host or route their communication layers can allow vulnerabilities in one country to affect services and data flows across the EU.

These dependencies can be understood as part of a recent global shift from on premises hosting to large scale third party providers because of operational incentives. Namely, access to globally distributed data centre resources, flexible scaling, high availability, lower capital and operational costs, and superior performance for websites and digital services are especially meaningful for governments with limited domestic hosting capacity or constrained public sector IT budgets (Kumar et al., 2024).[6] However, the trade off is that performance, resilience, and cost efficiency increasingly come at the price of diminished jurisdictional control.

This trade-off between the operational benefits of global providers and the sovereignty implications of relying on them underscores the need for more deliberate and risk aware decision making about the networks through which governments route and deliver digital services to citizens, businesses, and one another. For example, governments may choose to increase the share of web portals and associated communication systems that run on EU based network operators, helping ensure that the public communication infrastructure underpinning essential services remains under European operational control. In addition, Member States should work together to lower their reliance on non EU infrastructure by developing shared European solutions, for example through future European Digital Infrastructure Consortia (EDIC) that allow countries to build and manage essential systems together.

[6]Kumar, R., Carisimo, E., De Angelis Riva, L., Buzzone, M., Bustamante, F., Ayyub Qazi, I, Beiró, M., *Of Choices and Control - A Comparative Analysis of Government Hosting*, 2024, in: Proceedings of the 2024 ACM on Internet Measurement Conference (IMC '24). Association for Computing Machinery, New York, NY, USA, 462–479. https://doi.org/10.1145/3646547.3688447

05.

Digital governments across cities, **regions and countries**

5. Digital governments across cities, regions and countries.

Digital government services are provided at various levels of administration, encompassing central, regional, and local authorities. In addition to national provision, these services also operate across borders, enabling both citizens and businesses to access key public services when moving or conducting activities between different countries. This multi-tiered and cross-border perspective reflects the EU's commitment to facilitating seamless digital interactions within the Single Market, ensuring that individuals and enterprises benefit from efficient and accessible public services regardless of their location within the EU.

5.1 National versus cross-border services, in light of the Single Digital Gateway Regulation (SDGR)

As noted in the previous chapters, governments provide more services online for national citizens and businesses than for cross-border users from other EU Member States. The EU's **Single Digital Gateway Regulation (SDGR)** aims to simplify access to key administrative procedures across the EU by requiring that essential services be made available online, including for cross-border users. Since 2024, the services in the eGovernment Benchmark have been mapped to the procedures listed in Annex II of the Single Digital Gateway Regulation. Moreover, indicators that evaluate Cross-border ePayments, the (Cross-Border) Delivery of Output of the service, and the Once-Only-Technical-System (OOTS) were added to the eGovernment Benchmark. With this integration, the eGovernment Benchmark covers high-impact services that target both domestic and foreign users. In line with the goals of the SDGR, the integration of these procedures and technological solutions removes obstacles for (especially cross-border) EU citizens and businesses to gain information on and complete simple procedures.

Some 17 eGovernment Benchmark services link to citizen-related procedures from Annex II of the Single Digital Gateway Regulation. These services perform above average. For all 68 national citizen services measured in the eGovernment Benchmark, the Online Availability indicator scores 93.3. Further, the sub-set of SDGR services scores higher at 95.0 out of 100 instead. For cross-border SDGR procedures the advantage is slightly smaller, with the full set of key public services together averaging 74.8 and the SDGR procedures averaging 75.4.

The 11 eGovernment Benchmark services linked to **business-related procedures** from Annex II of the SDGR show a mixed picture. For national businesses, the SDGR services are at 96.1 out of 100, ahead of the 88.0 for all 18 national business services measured in the eGovernment Benchmark. However, the SGDR cross-border services fall below the average, with 71.2 against 77.4. This is primarily due to the underperforming SDGR procedures related to the Data Governance Act: "Register as a data intermediation service provider" and "Register as a (would-be) data altruism organisation recognised in the European Union". These results imply that whereas business can complete most cross-border services online, they often cannot register as a data intermediation service provider or data altruism organisation in another Member State. These two services average 59.6 and 62.5 for the Cross-Border Online Availability indicator.

As displayed in Figure 10, other indicators linked to the SDGR show that governments do not yet offer seamless cross-border services. **Cross-Border ePayment** is the highest performing indicator at 77.5, indicating that

most EU users can pay service fees online without restrictions based on their payment provider or account location (although slightly less than in 2024).

A similar number of services as for cross-border ePayment ensure that the **output of the services is delivered digitally**, currently scoring 76.4. This is less common for citizens and businesses dealing with another EU Member State, only at 48.9. Meaning, cross-border service requests may be filed online, but the resulting certificates or other formal documents are still sent by post or need to be collected in person.

To ease exchange of official public documents and data across borders, part of the Single Digital Gateway Regulation is the **Once Only Technical System (OOTS)**. This system enables the exchange of data between public administrations across borders between EU countries. OOTS is cross-sectoral and in principle can be implemented for a wider set of procedures than currently set out in the Single Digital Gateway Regulation. While the EU Member States have been connecting their national infrastructure, the OOTS has not been implemented in any of the EU countries, yielding a score of 0. It illustrates that, until this point, no citizen or business in the EU can yet give consent for the automatic retrieval of documents from their home country's issuing authority through the OOTS. The good news is that since 2024, the number of EU Member States that are production ready has grown from 2 to 21, of which 13 countries deploy first end-users transactions.[7] Based on this, further implementation and uptake are expected in the foreseeable future.

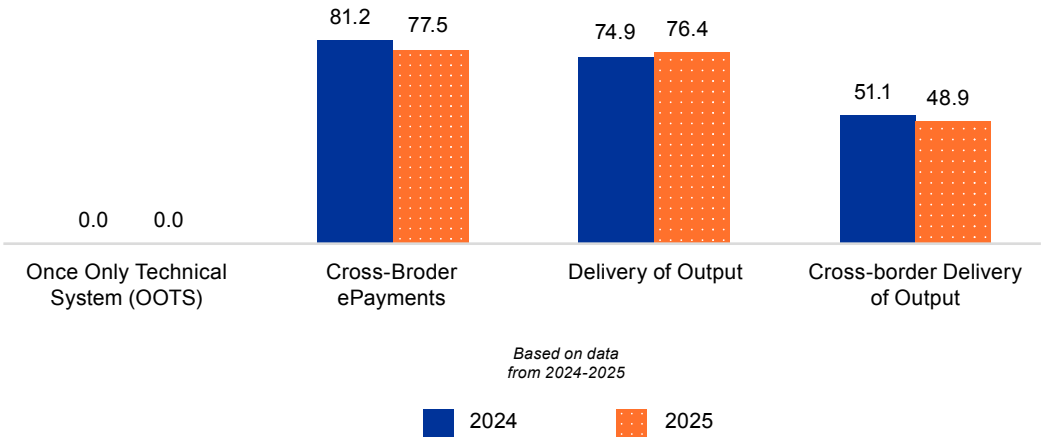


Figure 10 – Indicators related to the Single Digital Gateway Regulation

[7]European Commission, *Once-Only Technical System Acceleratormeter*, European Commission website, November 2024, accessed May 2026, https://ec.europa.eu/digital-building-blocks/sites/spaces/OOTS/pages/592642684/Implementing+the+OOTS

5.2. Government tiers are still apart

Public services across the European Union are offered by different layers of government. The eGovernment Benchmark specifies three governmental levels. From the largest to the smallest, these are central (national), regional (e.g. provinces, universities, hospitals), and local (municipalities) governments. The distribution of the eGovernment Benchmark services varies across countries and depends on the type of service or on the delegation of legal responsibilities within the respective country.[8] The results show that digital performance continues to differ across these assessed government levels.

As shown in Figure 11, central government services have been performing better (85.4 out of 100) than regional (84.4 out of 100) and local ones (82.8 out of 100) for the Digital Public Services for Citizens KPI. Services provided by ministries, agencies and other central government bodies are closer to reaching the digital decade target than provinces, regions, cities, and other regional and local authorities. For the Digital Public Services for Businesses KPI, most of the key public services measured are provided by central government bodies, such as ministries of economic affairs, enterprise agencies, etc. Hence, the disparities between central, regional and local government are less representative for the business-related target than for the citizen-related target. Still, central government services have been performing better (91.4 out of 100) than regional (85.2 out of 100) and local ones (86.6 out of 100). Among other factors, the persisting gap may be due to the smaller scale of regions and municipalities, having more limited access to digital infrastructure, lower concentration of IT-skilled civil servants and suppliers, as well as fewer financial resources.[9]

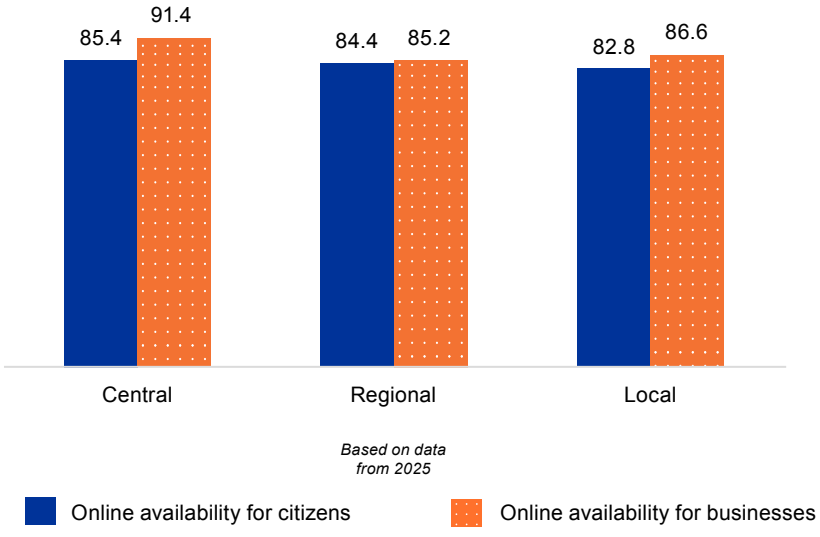


Figure 11 – Online Availability across government levels

[8]In practice this means that several eGovernment Benchmark services are provided by central government bodies in all countries, while other services are provided centrally in one country and regionally or locally in another. The study assesses the relevant competent authorities, thus tailoring per country where the service is delivered, as opposed to a generic assessment of central, regional and local administrations. Moreover, whenever a specific service is not applicable or not applicable for all regions or cities, the service status and scoring are adjusted (e.g. if parking permit applicability varies across cities in the same country, only those cities with parking permits are taken into account).

[9]The Council of European Municipalities and Regions (CEMR), Digital local and regional governments – *The interests of European local and regional governments in the EU's digital policies and their implementation – CEMR position paper*, 2025, https://ccre-cemr.org/wp-content/uploads/2025/11/CEMR-Position-paper-digitalisation-EN.pdf

eGovernment performance does not only differ across the three main tiers of government (central, regional and local). Digitalisation of public sector services may also differ between different regions or different cities in the same country. As a general hypothesis, smaller government bodies are expected to perform worse than larger ones. To test this, the 2026 eGovernment Benchmark performed a **new, comparative analysis of two samples of regional and local administrations**. The main sample includes the largest regional bodies and municipalities, including capital cities (in line with the sample used since 2012). The extended sample includes smaller regions and cities, such as small towns and municipalities typically located in rural parts of the Member States.

As displayed in Figure 12, the main sample of regions and cities scores 95.1 and 75.8 for the Online Availability and Cross-Border Online Availability indicators.

The newly piloted enlarged sample consists of additional mid-sized and small administrative units (on top of those included in the main sample). They average 76.8 and 37.3 on Online Availability and Cross-Border Online Availability respectively. This means that Online Availability is 18.3 points lower for the additional mid-sized and small administrations, while Cross Border Online Availability is 38.5 points lower compared with the largest administrations in the main sample. These results reveal a substantial performance gap, meaning that citizens and entrepreneurs requiring services from smaller administrations have **more limited access to fully online and cross border services**. Such performance gaps may be explained by the fact that wider economic growth and investments are unevenly distributed: capital regions and large metropolitan centres perform better in terms of innovation and competitiveness, quality of public governance and administration, connectivity and education attainment, than regions with lower population density.[11]

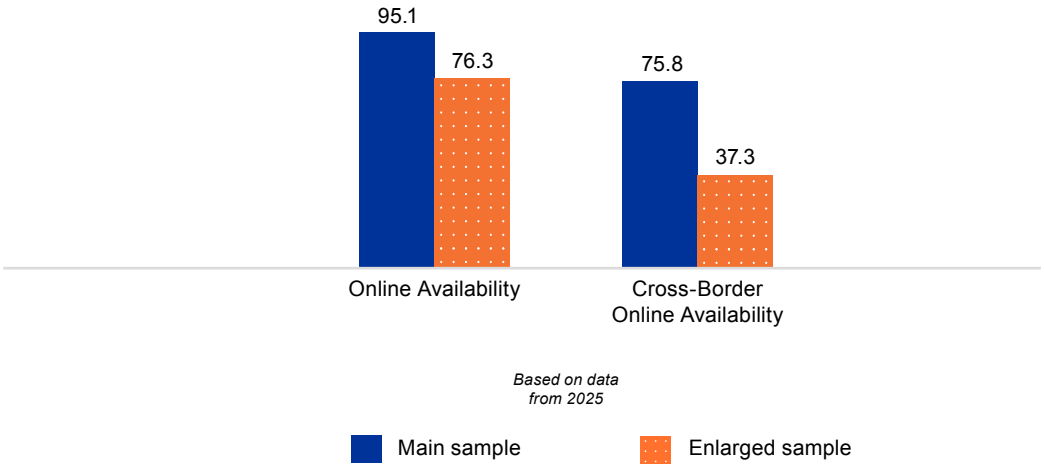


Figure 12 – (Cross-Border) Online Availability for the main and enlarged sample

[10]For instance, the main sample for Germany consists of the largest 20 German regions and cities. The extended sample includes 14 additional mid-sized and small regions and cities. More information on the composition of the samples can be found in the eGovernment Benchmark Method Paper.

[11]Durán Laguna, J., D'Apice, P., Grzegorzewska, M., De Franceschi, F., Brons, M., Maes, J., De Dominicis, L., Pesaresi, E., Gianelle, C., Heidelk, T., Monfort, P. & Walsh, J., *Ninth report on economic, social and territorial cohesion*, Publications Office of the European Union, Luxembourg, 2024, https://ec.europa.eu/regional_policy/information-sources/cohesion-report_en

06.

Key conclusions and **EU policy recommendations**

6. Key conclusions and EU policy recommendations

6.1. Progressing towards the Digital Decade overcoming cross-border challenges

The eGovernment Benchmark 2026 shows that the EU continues to advance towards the 2030 Digital Decade targets for digital public service delivery. While Digital Public Services for Businesses continues to score higher than Digital Public Services for Citizens, both Digital Decade KPIs show year-on-year improvement.

Among the citizen life events, Transport, Moving and Studying perform the best. In these high-scoring areas, government bodies score particularly well on the Online Availability indicator, combined with solid Cross-Border Online Availability. In other words, the majority of services associated with them are accessible online, also for tourists, international travellers and students. Health services remained the least digitalised, with challenges primarily due to low scores on the Cross-Border Online Availability indicator, affecting patients seeking medical assistance in another EU Member State.

Both the Business-Start Up and Regular Business Operations scores remain relatively high overall, although annual improvements have been limited. As for the citizen life event services, the cross-border services for businesses require particular attention.

Overall, the data continues to highlight a significant disparity between national and cross-border online availability. While digital public services are widely accessible within individual Member States, cross-border availability lags behind. Bridging this gap will be essential for delivering on the Digital Decade objective of ensuring 100% online accessibility of key public services by 2030.

6.2. Accelerating the implementation of pre-filled forms, transparency building blocks, user support and mobile friendliness

In addition to the two Digital Decade KPIs, the eGovernment Benchmark provides data on four additional indicators that underpin the Digitalisation of Public Services dimension of the Digital Decade policy programme. In 2025, Mobile Friendliness and User Support remained the strongest performing indicators, suggesting that EU citizens and entrepreneurs benefit from strong mobile responsive websites and the availability of comprehensive user assistance when interacting with digital public services. The Regular Business Operations and Transport life events lead the way for the Mobile Friendliness indicator, while improvements in Health and Family were a main driver for the gains in the User Support indicator. With an increase of more than 6%, it seems public sector bodies are accelerating on the Pre-Filled Forms indicator. eGovernment users can increasingly submit online forms in which key information is already listed for them, now the case in three out of four services. Online forms needed to obtain Family and Career services improved most, setting an example for the Transport and Justice life events, which perform worse and show slower improvement too. Government performance on the Transparency of Service Delivery, Design, and Personal Data indicator is stagnant. Notably, the sub-indicator for Transparency of Service Delivery scored the lowest within this category, meaning citizens and entrepreneurs lack clarity on how and when services are delivered. Judicial organisations struggle most. They have ample room to better inform consumers who start a small claims procedure with clear service timelines, as well as information on personal data reuse and involving users to improve digital products and services.

6.3. Realising AI-driven, cybersecure and sovereign digital governments

AI, Cybersecurity and Sovereignty are three crucial priority areas for the EU's digital government transformation. Further enhancing of eGovernment AI capabilities might lead to improved user interactions. As it currently stands, the implementation of AI chatbot functionalities has not taken full flight. Although some Member States seem to rapidly scale AI-enabled assistance, others have yet to introduce such capabilities into their online public service delivery. In fact, fewer than half of the government portal websites offer AI-powered live support. Their impact on users is also currently expected to be limited, as most chatbots are technically immature. Users can only perform basic interactions and receive limited support when needing guidance through multi step procedures. Less than one out of five chatbots can transfer requests to a human agent, while the linguistic features of chatbots in the EU are also limited. Relatively few chatbots are able to translate information into clear and accessible language, support multilingualism and properly answer questions specific to cross border users.

In addition, promoting and ensuring compliance with cybersecurity standards and protocols across government portals remains important. However, most common security and modern internet standards are only met by half of government websites. Government websites remain particularly vulnerable to cross-site scripting or clickjacking attacks (Content Security Policy). Furthermore, only a small share of websites is protected against attackers manipulating the contents fetched by browsers (Subresource Integrity). New pilot findings also pinpoint the risk of certificate mis-issuance, which could enable attackers to impersonate official portals, intercept traffic, or conduct phishing attacks that appear legitimate to citizens and businesses (Certification Authority Authorisation). Raising cyber awareness among the wider public is essential to safeguarding sensitive information and maintaining trust in digital public services. However, less than one out of four government websites use official government domain suffixes that visitors can easily recognised, such as ".gov". Positively, about half of the government portals raise phishing awareness, for example by actively guiding users in recognising phishing attempts and explaining how to verify that a domain is legitimate.

As digital sovereignty remains a priority for the European Union, the infrastructure underlying public-facing websites and email domains is increasingly becoming a point of strategic reflection for governments. This could imply encouraging investments in hosting government websites on EU-owned servers to reduce dependency on non-EU providers. Pilot indicator findings show that more than one third of eGovernment websites and portals are hosted on servers controlled by operators whose ultimate beneficial ownership lies outside the EU. For incoming and outgoing mail servers this is even more than half of the government email domains. The United States is the most frequently appearing non-EU jurisdiction among those providing the network infrastructure through which public sector websites are routed. Although potential risks and impacts related to non-EU ownership of digital infrastructure may be hard to assess, Member States should remain vigilant. In theory such ownership could expose EU digital governments to vulnerabilities or interruptions in providing online information and services to citizens and businesses. While these risks are not inevitable, proactive monitoring and mitigation strategies are key to future-proof the integrity and resilience of EU digital public services.

Collectively, these key priority areas are positioned as foundational to achieving secure, efficient, and resilient digital public services. This year's analysis shows the importance and potential of AI, cybersecurity and sovereignty for eGovernment, but also uncovers their current shortcomings.

6.4. EU policy recommendations

The following EU-wide policy recommendations, possible actions and investment priorities are based on the eGovernment Benchmark findings and conclusions:

1. **For the EU Member States to provide key public services fully online,** with a focus on accelerating growth in digital public services for citizens. Attention should be paid to the ministries of justice, courts, healthcare providers, employment agencies, municipalities and other competent authorities providing services related to justice (starting a small claims procedure), health, career and family, which are the least available online. Member States should sustain efforts in digitalising public services for businesses as well as for citizens moving, using (public) transport and studying, to maintain positive momentum.

2. **For the EU Member States to upscale initiatives and programmes for digitalising public services for national users towards cross-border users.** Investments should be directed towards removing barriers, in particular for Europeans that need medical treatment, employment services, business permits and legal proof abroad. The procedures listed in Annex II of the Single Digital Gateway Regulation should be prioritised to pave the way for other services and demonstrate direct benefits.

3. **For the EU Member States to actively support cooperation and pinpoint necessary reforms needed for regional and local authorities in the efficient digitalisation of key public services** under their responsibility. Different types of civil registries by municipal bodies are a priority area including child, parental and marital registration.

4. **For the EU Member States to explore investing in common interoperable eGovernment solutions,** especially for implementing national and cross-border authentication systems compatible with notified eIDs and trusted digital service output solutions, in line with the Once Only Technical System (OOTS) and similar European pilot projects (e.g. for digital wallets).

5. **For the EU Member States to upscale eGovernment AI capabilities,** including those for enhanced user support, and foster data solutions for the provision of proactive services and pre-filling government forms, based on information already known by the competent authorities.

6. **For the EU Member States to increase digital government sovereignty,** by exploring investments for hosting government websites on servers from EU providers and reducing dependency on non-EU providers, e.g. via potential European Digital Infrastructure Consortia (EDICs).

7. **For the EU Member States to promote and ensure government compliance with cybersecurity standards and protocols,** while raising cyber awareness on government portals to the wider public.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

KK-01-26-045-EN-N

Publications Office
of the European Union