EuroISPA

ANNUAL POLICY REPORT 2024
BRUSSELS OUTLOOK 2025

EUROISPA

EuroISPA is the world's largest association of Internet Services Providers (ISPs), representing the interests of over 3,300 ISPs across the EU and EFTA countries.

EuroISPA has an active role in EU-level discussions on digital policies on behalf of its members with the aim of ensuring that the ISP industry's voice is at the forefront of decisions impacting the future of the Internet.

CONTENTS

2024: A YEAR IN REVIEW

HIGHLIGHT OF 2024

For EuroISPA, the year 2024 has been extraordinarily shaped by the run up to the 2024 European elections, a crucial moment for all European citizens and industry representatives such as our association to stop and think about what we want to achieve in the next five years.

But the EU elections are only the beginning: their outcome has changed the regulatory landscape we navigate, a new European Parliament and a new European Commission are in place, and ISPs must be ready for a renewed wave of legislation that will impact our sector greatly.

Throughout this extraordinary year, EuroISPA has focused on ensuring that the voice, the views and the needs of the ISP sector were heard and taken into account by all stakeholders, old and new, that are going to be setting the European digital scene for the next five years.

European ISPs views and hopes for the new EU legislative mandate are summarised in EuroISPA's Manifesto, the guiding document of our work in 2024.

The result of a collaborative effort by its members, the Manifesto advocates for putting innovation and fairness in the European Internet ecosystem at the core of EU policymaking in the digital sphere.

It includes asking EU legislators to commit to the joint implementation of actions towards:

- a fully functioning internal market
- a long-term vision on privacy online
- a harmonised European strategy for cybersecurity
- legislative coherence for digital infrastructure

By focusing on these issues, the EU can enhance its competitiveness, safeguard fundamental rights, and unlock the benefits of new technologies.

Click and read the EuroISPA Manifesto on our website.

2024: AN OVERVIEW

TIMELINE

20	20
meetings with policymakers and EU institutions/bodies	position papers, letters, recommendations, and consultations

29	4	1
topical meetings with industry associations	EuroISPA General Meetings	EuroISPA Industry Forum Meeting

Q1

JANUARY

- Published joint statement on swift adoption of the ePrivacy derogation extension
- Hosted a webinar on DNS4EU with Whalebone
- Attended EIF event on "Future of electronic communications and connectivity"
- Met with industry associations on data protection and cybersecurity and on online content moderation

FEBRUARY

- Held Officers meeting and Industry Forum meeting in Brussels
- Participated in ISPA Belgium New Year's Event
- Met with the European Commission and the EUIPO on piracy of live content
- Participated in IT decentralized system (e-Evidence) WG meetings on workflows
- Provided feedback to the call for evidence of the GDPR Review
- Participated in the Public Consultation Meeting of the High-Level Group on Access to Data for Effective Law Enforcement
- Held Online Content Committee meeting
- Met with industry associations on data protection and cybersecurity, on online content moderation and on DSA

MARCH

- Published position paper on AI
- Held Data Economy and Cybersecurity & Infrastructure Committee meetings
- Participated in IT decentralized system (e-Evidence) WG meeting on data mapping and transformation
- Held EuroISPA General Meeting in London
- Attended eco Spring Reception
- Met with industry associations on GDPR, on online content moderation and on data protection and cybersecurity

APRIL

- Participated in EIF General Assembly and Spring Drinks
- Published position paper on Data Retention
- Participated in IT decentralized system (e-Evidence) WG meeting on Architecture and Design
- Met with industry associations on data protection and cybersecurity, on online content moderation and on GDPR

MAY

Q2

- Participated in the Digital Partnership Workshop, Strasbourg
- Held EuroISPA Officers meeting and Industry Forum meeting in Brussels
- Met with the European Commission on AI and Copyright
- Met with the European Commission on DNA
- Met with industry associations on EU-US policy developments, on GDPR and on data protection and cybersecurity

JUNE

- Published joint statement on protecting encryption in the Child Abuse Regulation
- Met with Hungarian Permanent Representation (Council Presidency)
- Held Online Content, Data Economy, Cybersecurity & Infrastructure Committee meetings
- Held EuroISPA General Meeting in Rome
- Met with industry associations on online content moderation, on AI, on data protection and on EU-US policy developments

JULY

- Published feedback on European Commission's White Paper on Digital Infrastructure
- Published opinion on EU Payments Services Regulation
- Met with industry associations on Consumer REFIT and on AI

AUGUST

- Published joint industry request to extend deadline for Trustworthy General-Purpose AI Consultation
- Met with industry associations on data protection and cybersecurity

Q3

SEPTEMBER

- Welcomed new members: Point Topic and Whalebone
- Held Online Content, Data Economy, Cybersecurity & Infrastructure Committee meetings
- Held Officers Meeting and General Meeting in Brussels
- Attended event organised by MEP Axel Voss (DE, EPP) on AI and Copyright
- Met with Policy advisor to MEP Markéta Gregorová (CZ, Greens)
- Met with Policy advisor to MEP Bart Groothuis (NL, Renew).
- Met with industry associations on High-Level Group on Access to Data for Effective Law Enforcement and on data protection and cybersecurity

OCTOBER

- Attended EIF Welcome Reception for the new European Parliament
- Held EuroISPA Officers Meeting in Brussels
- Published reaction to the 42 Recommendations of the High-level Group on Access to Data for Effective Law Enforcement
- Met with industry associations on data protection and cybersecurity and on AI

NOVEMBER

Q4

- Published joint industry statement on personal data and AI models training
- Attended EUIPO Working Group Meetings
- Attended SIRIUS Conference in The Hague
- Participated in Expert Group on the E-evidence Decentralized IT System Closure Meeting
- Held EuroISPA General Meeting in Brussels and elected new Board
- Met with industry associations on data protection and cybersecurity

DECEMBER

- Participated in a workshop by the Council of Europe on the Implementation of the Second Protocol to the Convention on Cybercrime
- Signed open letter in response to the 42 Recommendations and Report of the High-level Group on Access to Data for Effective Law Enforcement
- Met with industry associations on digital fairness and consumer protection, on AI and on data protection and cybersecurity

EuroISPA
The world's largest association of Internet Service Providers

2025: WHAT'S AHEAD

BY ELINA USSA

EUROPEAN SECURITY AND COMPETITIVENESS – TIME TO MOVE FROM WORDS TO ACTIONS

Leading the EU's digital development requires a strong vision for a competitive Europe, where the internal market operates effectively and continues to evolve. It is time to shift from ceremonial speeches to decisive actions driving digital development. This requires a pragmatic approach, centered on concrete actions. **Henna Virkkunen**, the executive Vice-President of the European Commission, thanks to her experience, expertise, and personal qualities, is an excellent choice for leading Europe's efforts in shaping a competitive, resilient and inclusive digital future. It is anticipated that, instead of engaging in public posturing, issues will be addressed through dialogue.

This year, the EU Presidency of the Council will be shared between Poland and Denmark, two dynamic reformers within the Union and strong performers in digital development. We can expect progressive and dynamic action during both of their tenures.

Security undoubtedly stands out as a key issue for the current term of the EU leadership. Bringing an end to Russia's aggression in Ukraine and establishing lasting peace will be critical for Europe's future. Comprehensive security depends on strengthening Europe's preparedness and resilience, with a strong economy as its foundation. At the same time, the rapid evolution of the global digital market creates an urgent need to enhance Europe's competitiveness.

For years, there have been concerns that Europe is falling behind the digital development pace of the U.S. and China. Now, more than ever, swift and concrete actions are needed to prevent Europe from being permanently overtaken by these nations.

Historically, the EU has primarily focused on creating regulatory frameworks, while less attention has been paid to the overall operating environment. Europe must foster conditions that encourage innovation and attract investments to advance its competitiveness. Recently, Columbia University law professor Anu Bradford has pointed out that Europe faces significant challenges, including an incomplete internal market, fragmented capital markets, a shortage of skilled labour, and insufficient incentives for risk-taking. Strengthening Europe's strategic competitiveness is a major priority for **Ursula von der Leyen's** second Commission term and there is much work to be done.

Recent reports, including **Thierry Breton's** white paper, **Mario Draghi's** competitiveness report, **Enrico Letta's** internal market report, and Sauli Niinistö's document on comprehensive security, lay the groundwork for the next Commission's work program. All these reports emphasise the telecommunications market as a key priority.

While there is broad consensus on the objectives, some of the proposed measures rely on outdated and rigid concepts. For example, a common EU frequency management system is unlikely to improve agility. Additionally, company consolidations could already take place under the current framework. Promoting them through Commission Directives feels misplaced in a market-driven sector and does not adhere to the well-established principle that intense competition leads to better services for consumers.

Commissioner Virkkunen highlights the importance of joint efforts to promote the construction of sea cables. While financial support is already forthcoming, it is equally important that the Commission adopts measures that reduce the administrative burden of their construction. Across the EU, slow permit procedures and lengthy construction timelines are a significant bottleneck. The key to securing international connections is ensuring enough cables to effectively replace the damaged ones.

THE INTERNAL MARKET: THE FOUNDATION OF EUROPE'S COMPETITIVENESS

A major challenge facing the EU is the inconsistent implementation and interpretation of legislative acts across member states. For example, the national implementation of the telecom package is still pending in some countries. The administrative burden of GDPR on European businesses is finally being publicly acknowledged. It is quite peculiar that despite being an EU regulation, it is interpreted differently across member states and within Germany, even between federal states. It is imperative that the past mistakes are not repeated with the upcoming AI Act.

It is evident that poor regulation leads to uneven development and hampers the smooth functioning of the internal market. Rigid legislation makes business operations more challenging and reduces investment willingness. As Letta notes in his report on the internal market, the EU's internal market is far from operating at its full potential.

Strengthening the internal market requires emphasis on the proper implementation and enforcement of major data economy and cybersecurity regulatory reforms. The telecommunications sector is heavily regulated in the EU. Obsolete provisions and obligations must be carefully reviewed during the upcoming revision of the European Electronic Communications Code, to eliminate regulatory barriers to investment.

REGULATION: A BARRIER OR AN ENABLER OF INNOVATION?

All legislation must ensure technological neutrality while being implemented effectively, proportionately, and in ways that promote competition. Often, additional national regulations or differing interpretations lead to inconsistent practices across member states.

Despite good intentions, many regulatory requirements are technically challenging, or in some cases, even impossible to meet. Close collaboration with businesses, genuine consultation, and joint problem-solving are necessary to understand what is technically feasible. Impact assessments must become an integral part of legislative work to fully grasp the implications of regulations on industry, business, and citizens. Too often, impact assessments are insufficient or, in some cases, not conducted at all.

The delegation of powers to the European Commission also requires a critical approach, as it has become more common, which is often seen as a way to avoid challenging decisions. However, delegated powers reduce transparency and exclude businesses from influencing decision-making. Ensuring greater inclusivity and transparency in the legislative process is vital for achieving balanced and effective outcomes.

Elina Ussa
President of EuroISPA and Managing Director of FiCom

OUR POLICY

FOCUS AREAS

In order to have impact and focus our energies, EuroISPA has different committees to which members contribute their expertise and where discussions take place on specific topics.

ONLINE CONTENT

Online content moderation (DSA, TCO, etc.), piracy of live content, copyright, geo-blocking, AVMSD, online safety (Child Sexual Abuse Material), payments fraud, encryption

DATA ECONOMY

GDPR, AI and emerging technologies, ePrivacy, data transfers, data access and data retention, Digital Fairness Act

CYBERSECURITY AND INFRASTRUCTURE

Law enforcement, cybersecurity and critical infrastructure (NIS2 Directive implementation, Cyber Resilience Act), digital infrastructure and connectivity (EECC, 5G, 6G, spectrum, EECC, DNA, net neutrality), Internet governance, sustainability

ONLINE CONTENT

EuroISPA focuses on promoting an online environment that is safe, fosters transparent practices, and has the respect of fundamental rights at its core. EuroISPA seeks the establishment of balanced legal obligations for Internet intermediaries in all areas of the online content framework, calling for appropriate liability protection.

In 2024, the committee focused on defending our views on the proposed EU framework to fight CSAM and addressing the issue of fragmentation in the child safety space while following closely the changes to the recast CSA Directive 2011/93. We also supported our members on the implementation of the Digital Services Act at national level and raised concerns on the issue of liability in the context of impersonation fraud during the discussions around the Payment Services Regulation (PSR).

The committee was also particularly active on the ongoing preparation of the recommendations in the area of piracy of live content.

INSIGHT

BY DALIA COFFETTI

PIRACY SHIELD: A FLAWED APPROACH IN THE FIGHT AGAINST ONLINE PIRACY

ISPs understand the need to protect copyright and fight piracy. However, it is critical that the administrative, legal and technical systems deployed to achieve this shared goal are proportionate, efficient, non-discriminatory and not harmful to the proper functioning of the Internet network.

Italy was one of the first EU Member States to be equipped with a filtering platform, called “Piracy Shield”, whose primary objective is to tackle online piracy related to live broadcast sporting events. It was introduced by Law No. 93 of 2023, amended by the so-called Omnibus Decree (DL no. 113 of 9 August 2024) and completed by two AGCOM resolutions that better detail its functioning. In a nutshell, Piracy Shield is an asynchronous platform designed to allow copyright holders (so-called flaggers) to quickly report domains or IP addresses hosting pirated content. Upon receiving the report on the portal, AGCOM can order Italian ISPs to block access to the sites involved within a maximum of 30 minutes.

Leaving aside the fact that this sort of “mega-firewall” is easily bypassed by means of VPN or by switching from a private DNS to a public DNS, and that it entails considerable costs for ISPs, it goes without saying that, from the very beginning, its functioning has revealed many limitations and criticalities, which have been exacerbated by the recent change in the law:

- there is a high risk of affecting lawful resources, since AGCOM can order the blocking of IP addresses that are predominantly (and not uniquely, as originally intended) used for unlawful activities;
- filtering obligations are potentially unlimited, after the legislator intervened to remove the filtering limits on IP/FQDN addresses agreed between the NRA and the operators during the technical tables;
- ISPs are found to perform filtering and tasks that collide with individual freedoms. This is contrary to European legislation that qualifies fundamental ISPs services as mere-conduit and therefore exempt them from liability. On the contrary, in Italy criminal liability has been expressly established for ISPs;
- marked asymmetry between the blocking procedures that must be carried out in a timely manner and total uncertainty as to the timing for unblocking: Uncertainty that disproportionately affects small operators or foreign providers who - not always being aware of the EU Member State's regulatory framework - have difficulty enforcing their rights.

While we are witnessing initiatives that aim at combating piracy, it is useful to remember that any system activated at national level has strong impacts outside the borders, as content and resources located in third countries are filtered.

In addition, a massive multiplication of asynchronous platforms would pose threats and create vulnerabilities to the proper functioning of the Internet, as intervening with potentially unlimited filtering creates high collateral damage even greater than the social benefit of combating piracy.

There are better tools to fight piracy, including criminal Law, cooperation between States, and digital solutions that downgrade the quality of the signal broadcast via illegal streaming websites or IPTV.

European ISPs are ready to play their part in the battle against piracy, but the solution certainly does not lie in filtering and blocking IP addresses.

Dalia Coffetti
EuroISPA Board Member and Head of Regulatory and EU Affairs of AIIP – Association of Italian Internet Providers

INSIGHT

BY ASKO METSOLA

TELECOM OPERATORS MUST NOT BECOME CONTENT POLICE

Telecommunications companies are the backbone of the Internet, akin to road maintenance operators tasked with ensuring smooth and functional infrastructure. Just as road operators are not expected to monitor vehicles for illegal goods, telecom operators should not be burdened with policing Internet content. Their role would shift drastically from facilitators to enforcers if tasked with such responsibilities.

INTERMEDIARIES ARE NOT RESPONSIBLE FOR DATA CONTENT

Under the EU's Digital Services Act (DSA), intermediaries like telecom companies are not liable for content transmitted or stored by their users under certain conditions.

The DSA also prohibits general monitoring obligations. However, recent EU legislative initiatives have started imposing new responsibilities on intermediaries, stretching the limits of this limited liability.

For instance, under Article 17 of the DSM Directive, online content-sharing service providers might be held accountable for copyright infringements. Other regulations increasingly require telecom operators to block or monitor online content, such as those addressing terrorist content or child sexual abuse. Even seemingly unrelated laws, onto the operators, like those governing payment services, propose shifting liabilities—such as financial losses from spoofing.

PROTECTING COMMUNICATIONS SECRECY

Commission proposals like the CSAM Regulation suggest requiring all communication services to inspect users' messages, undermining encryption. Scanning messages before encryption negates its purpose, much like obliging postal workers to read letters before sealing them. The European Court of Human Rights ruled in Podchasov v. Russia (2024) that weakening encryption violates human rights. Yet, Europol and Member States' police chiefs recently called for breaking encryption for investigations.

These proposals often lack technical understanding, expecting telecom companies to assess the legality of all communications—an impossible and intrusive task. Content regulation should target platforms or sources, not infrastructure providers.

Legislation that weakens communication secrecy threatens human rights, risking a surveillance state akin to China. Good intentions cannot justify such erosion of freedoms.

Asko Metsola
Legal Advisor of FiCom

DATA ECONOMY

EuroISPA aims to set the right foundations for Europe to become a successful data economy, a leader on emerging technologies, while maintaining the interests and trust of users at its heart. Strong data protection, privacy and open international data transfers are the fundamental pillars.

In 2024, the committee focused on data access and data retention topics, building up a solid position, answering to public consultations and following closely the activities of the High-Level Group on Data Access for Effective Law Enforcement, also participating in joint activities with the industry.

Alongside this, throughout the year the association built a solid network with industry and policy makers in the field of AI to foster exchange and develop the association's first positioning on the topic, with a particular attention to the interplay between copyright and AI, personal data and AI, as well as sustainability and AI.

The same exercise started in the last quarter of the year on consumer-related matters, in particular on the upcoming Digital Fairness Act and its potential impact on ISPs.

INSIGHT

BY STEFAN EBENBERGER

THE E-EVIDENCE-REGULATION AND ITS FUNDAMENTAL CHANGES FOR CROSS BORDER INTERACTION BETWEEN AGENCIES AND SERVICE PROVIDERS

Criminal investigations nowadays rely heavily on digital evidence, which is often stored by service providers in other EU member states. To access such evidence, law enforcement agencies currently need to request legal assistance from the authorities in the service provider's member state. While this is an established process, it can lead to delays and potential loss of evidence.

Regulation (EU) 2023/1543 ("E-evidence Regulation") aims to change this. Once in effect, authorities in EU member states will be able to issue production orders for certain data and preservation orders directly to service providers in other EU member states, without requiring their own national authority to act as an intermediary. Service providers will be legally required to produce or secure the requested data, facing significant administrative penalties if they fail to comply. However, for certain categories of data, the authorities in the service provider's member state may object to the order but only based on specific grounds for refusal.

The E-evidence Regulation applies to a wide range of service providers, including electronic communication services, IP and domain name communication services, IP and domain name services, and various other information society services. Since the regulation does not exempt small service providers, all companies, regardless of size, must comply and establish the necessary procedures to receive, process, and respond to orders.

To facilitate secure communication between authorities and service providers, the European Commission is currently developing a decentralized IT system. This system is being designed in close collaboration with industry experts, including EuroISPA, to ensure that service providers' expertise is considered.

The regulation will take effect on August 8, 2026. Before then, member states must designate their competent authorities, and the European Commission must adopt implementation acts for the decentralized IT system. However, several open questions remain, particularly concerning the regulation’s scope, the specific obligations of service providers, and the interaction between the decentralized IT system and similar national systems. Addressing these issues is essential to ensure the smooth implementation of E-evidence.

Stefan Ebenberger
Secretary General of ISPA Austria

INSIGHT

BY PHILIPP EHMANN

ARTIFICIAL INTELLIGENCE AND ITS INTERPLAY WITH PRIVACY

With the evaluation of the GDPR due in early 2024 and Large Language AI Models on the rise, data protection again came into the spotlight of regulatory debates. This culminated in the European Data Protection Board (EDPB) being asked to give its opinion on data protection in the training of artificial intelligence models. The debate about the possible recommendation of the EDPB highlighted a central question revolving around data protection in disruptive technologies.

AI-specific, detailed ex-ante regulation may prove to be a hazard to the inception and development of the technology. Because of this, room for experimentation and regulatory sandboxes need to be established as soon as possible in order to boost the application of AI systems in the EU. Beyond that, regulation should be well advised to critically reflect its purpose.

With the GDPR, the AI Act and the European Data Act in place, the alleys to convey technology to citizens and companies in Europe have repeatedly narrowed. Meanwhile general guiding principles as e.g. set out by the GDPR. become opaque through legal practice and further national and European legislation, leaving the Internet economy with little room for innovation, product development and the ability to compete in a global tech race.

Legislators and regulators are well advised to observe developments in the United States and the People's Republic of China in order to avoid a total rollback on the European data protection regime, which has been regarded as a success so far and will hopefully weather time and global turmoil. Its principles are based on the building blocks of democracy and provide a generally proportionate framework for companies to thrive and citizens to rely on. Furthering data protection rules may prove counterproductive in this light.

Philipp Ehmann
Head of the Capital Office & Head of the Policy, Law and Regulations Division of eco – Association of the Internet Industry

CYBERSECURITY AND INFRASTRUCTURE

EuroISPA strives for a harmonised and resilient framework for digital security in Europe that respects encryption, values intermediaries' expertise, and strengthens the cooperation with law enforcement authorities. All this while supporting Europe's connectivity quest to become a strong and stable gigabit society.

In 2024, the committee focused on connectivity issues by building a position and replying to the White Paper Consultation on "How to master European Digital Infrastructure needs?". The committee has prioritised the upcoming Digital Networks Act and the revision of the EECC. In that vein, the committee has been delving deeper into topics of infrastructure resilience, such as subsea cables. Through the committee, EuroISPA has also built its first ever position on sustainability emphasising the importance of making our infrastructure more energy efficient.

Finally, the committee also focused on Internet governance by replying to the targeted consultation by the European Commission on the matter, an effort that will continue with the planned attendance to several events, such as the IGF or the Web 4.0 conference.

INSIGHT

BY ROMAIN BONENFANT

THE FUTURE OF DIGITAL INFRASTRUCTURE: WHAT'S NEXT AFTER THE EUROPEAN COMMISSION'S WHITE PAPER

With the publication of its White Paper on digital infrastructure in 2024, the European Commission has finally launched a long-overdue debate on the future of the telecom regulatory framework. EuroISPA has taken an active role in these discussions, committed to shaping an ambitious vision for the sector.

Engaging with policymakers to highlight the essential role of Internet Service Providers (ISPs) in fostering innovation, resilience, and the twin transition, we reaffirm our dedication to keeping telecom networks at the heart of Europe's economic and technological leadership.

As we move towards 2030, unlocking the necessary investments to achieve the Digital Decade connectivity targets remains a top priority. To this end, Europe must establish a regulatory framework that incentivises investment, notably through a comprehensive Digital Networks Act, ensuring a robust, sustainable, and competitive telecom ecosystem for the future.

Achieving true internal market integration will largely depend on harmonising and streamlining regulations across multiple areas, including infrastructure investment, spectrum management, and taxation.

This also requires assessing the relevance of existing sectoral rules alongside broader horizontal frameworks. The regulation of our sector must adopt a more coordinated approach and foster investment-friendly conditions while preserving effective national frameworks and ensuring fair competition.

Prioritising network sustainability is also crucial to supporting the green transition of our economy. The telecom industry plays a key role in driving sustainability gains across sectors and reducing its own environmental footprint by replacing legacy technology with more energy-efficient infrastructure. The inclusion of connectivity networks in the EU Taxonomy for sustainable finance is a positive step toward securing funding for greener networks. Additionally, engaging with equipment suppliers and digital service providers across the entire value chain will be essential to adopting the most efficient technologies, achieving net-zero emissions and ensuring optimal network efficiency.

Looking ahead to 2025, we believe the Digital Networks Act must serve as a cornerstone for turning these priorities into concrete action. By simplifying regulation, securing investment, and strengthening network sustainability and security,

Europe can build digital infrastructures that are both competitive and future-proof. EuroISPA and its members remain committed to working alongside European stakeholders and institutions to ensure these vital reforms become a reality.

Romain Bonenfant
EuroISPA Board Member and Managing Director of FFTélécoms – Fédération Française des Télécoms

INSIGHT

BY LARS STEFFEN

PROMOTING SUSTAINABILITY THROUGH DIGITAL INFRASTRUCTURE

EuroISPA, the pan-European association of Internet Services Providers (ISPs) associations has just published its Position Paper on Sustainability. This underscores the crucial role that digital technologies and infrastructure play in driving environmental responsibility across the economy. From reducing energy consumption in telecom networks to encouraging investments in sustainable data centres, the paper presents actionable strategies for driving a greener future powered by responsible digitalisation.

Digitalisation already plays a key role in sustainability, replacing outdated, energy-intensive technologies with more efficient alternatives. For instance, 5G networks consume 80% less energy than 4G, and fiber optic cables use five times less energy than copper. This high-performance connectivity creates opportunities for energy savings across all sectors.

However, more can be done. EuroISPA advocates for proactive measures, such as phasing out aging 2G and 3G equipment, fostering industry collaboration, and sharing best practices to optimise data distribution. Consistent regulation and increased investment in renewable energy infrastructure are also vital in ensuring that Europe's digital ecosystem remains both competitive and sustainable.

Data centres as the backbone of digitalisation, key to decarbonising the EU economy. EuroISPA encourages further investment in EU-based data centres, supported by renewable energy, to enhance both competitiveness and environmental sustainability.

The digital infrastructure sector holds the key to a greener future, and we at EuroISPA are committed to leading that transition. By promoting energy-efficient technologies and investing in sustainable data centres, we can drive decarbonisation across Europe, ensuring both sustainability and digital resilience.

By embedding sustainability into every level of the digital supply chain, EuroISPA envisions a future where responsible digitalisation powers a greener, more prosperous Europe.

Learn more in EuroISPA's full Position Paper on Sustainability.

Lars Steffen
EuroISPA Vice-President and Head of International, Digital Infrastructures & Resilience of eco – Association of the Internet Industry

THE ISP SECTOR

THE INTERNET ECOSYSTEM

The Internet ecosystem is a complex network of networks, composed of layers and actors working together to facilitate global connectivity and communication and ensure functionality.

Internet Services Providers (ISPs), in particular, play a central role in providing internet access and maintaining the integrity of the network infrastructure.

ISPs come in various shapes and sizes: from an SME to an international corporation, even the smallest of these organisations is crucial for the functioning and stability of the Internet.

They connect users to the Internet through technologies such as cable, fiber optic, DSL and wireless networks. ISPs manage the necessary infrastructure for connectivity, directing data between user's device and the Internet.

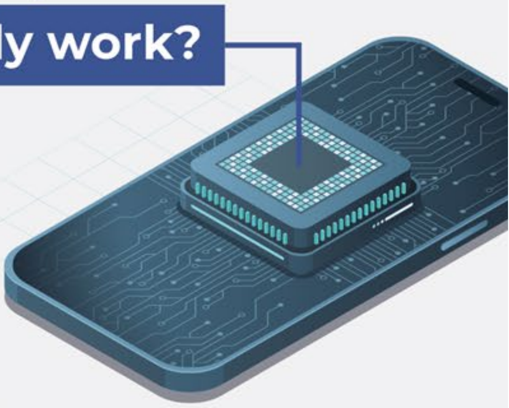
ISPs also play a crucial role in implementing Internet regulations and policies set by regulatory bodies like the European Union.

- ISPs maintain and upgrade the network infrastructure to ensure reliable connectivity and cybersecurity.
- ISPs make it possible to timely detect and take down illegal content online and are a key partner of law enforcement authorities in promoting a safer Internet
- ISPs are key drivers of Europe's innovation in the data economy era, balancing the adoption of new technologies and the protection of fundamental rights.

Learn more about our sector on our website: https://www.euroispa.org/about/about-our-industry/

EuroISPA

The Internet ecosystem: how does it really work?



THE USER YOU!

Anyone who has access to and utilises the Internet for various purposes such as communication, information, and entertainment.
Examples: Individuals, Organisations, Businesses, Governments

Step 01

The user requests to access content by typing a URL into his browser, like **www.euroispa.org**

THE DEVICE

The user's device connects to the Internet using various connection methods such as Wi-Fi, mobile data, or wired connections

Step 02

Connecting to the ISP
The connection method links the user to an ISP: the Access Provider

While Internet access providers are responsible for providing Internet access to the user, other ISPs play different roles in this process - find a list of different types of ISPs and what they do in the insight page

INTERNET SERVICES PROVIDERS (ISPs)

Small or large companies that provide Internet access to the user. They connect users to the Internet through various technologies such as fibre optic, cable, DSL, and wireless networks. ISPs manage the infrastructure needed for connectivity and direct data between the user's device and the Internet

+

NAMING AND NUMBERING LAYER:

When the user types a web address (URL) into their browser on their device, the Domain Name System translates this human-readable address into an IP address, which is used to locate where the content is hosted

Step 03

The user's request is directed from the ISP to the hosting server that holds the content

THE HOSTING SERVER

It stores and serves the content. It handles requests for content and delivers the requested data back to the user's device

Step 04

The request is processed by the hosting server and the content is sent back to the user's device

THE DEVICE

The user's browser or app receives the content and displays it

Step 05

Enjoy!

THE USER

Can enjoy the content they were looking for

OUR MEMBERS

COUNCIL AND INDUSTRY FORUM

EUROISPA COUNCIL MEMBERS

The Council members are ISP associations from EU and EFTA Member States. EuroISPA is managed by its members. Each member appoints a representative to the EuroISPA Council.

This body meets on a regular basis each quarter and in special sessions, as required by the members, to formally discuss policy, matters of importance to the EU Internet industry and the administration of the organisation.

@iip Associazione Italiana INTERNET Provider

amsix

cz.nic SPRÁVCE DOMÉNY CZ

eco

FÉDÉRATION FRANÇAISE DES TÉLÉCOMS

FiCom

ispa Internet Service Providers Austria

ISPA

linx

EUROISPA INDUSTRY FORUM MEMBERS

The EuroISPA Industry Forum allows individual companies with a legitimate interest in the Internet industry to participate in EuroISPA's activities and work groups.

The Industry Forum meets regularly to discuss policy issues and matters of importance to the EU Internet industry. The Industry Forum acts in a purely advisory capacity to the Council.

amazon

facebook

freedom internet

Google

Microsoft

POINT topic

SEZNAM.CZ

verizon

whalebone

WORLDSTREAM IT INFRASTRUCTURES

INSIGHT

BY OLIVER JOHNSON

THE EUROISPA COMMUNITY

Point Topic was founded in 1998, just a year after EuroISPA itself. Focused on fixed internet and broadband, we have been counting and collating data since there were fewer than a million internet subscribers. Today the world has just surpassed one and a half billion subscribers (https://www.point-topic.com/post/global-fixed-broadband-subscriptions-milestone), with well over two hundred million of them in Europe.

As applications for the internet have exploded, our work, supporting suppliers and reporting for everyone, has broadened. EuroISPA members are increasingly on the front line for customer service, as more and more of our lives are online. Even a few minutes offline, or milliseconds in some instances, can be disruptive, costly and will usually trigger contact with the ISP.

It has never been more important to provide that interface and to maintain control of the portals that enable those services. In fact, it is a strategic and moral imperative.

Supplying those who provide that service and helping people, business and government function efficiently, fairly and without fear of theft or attack is central to our mission. Being members of EuroISPA and taking part in the shared effort to make fair, equitable, affordable access to the Internet available is a significant plus. Knowledge sharing, discussions and organisation are key to the continued spread of the Internet and the benefits it offers.

Oliver Johnson
CEO of Point Topic

EUROISPA AT GLANCE

WWW.EUROISPA.ORG

Established in 1997, EuroISPA is the world's largest association of Internet Services Providers (ISPs), representing the interests of over 3,300 ISPs across the EU and EFTA countries.

EuroISPA is a collection of trade associations and companies from across Europe who work together to find common views on the main discussions on EU digital policy.

With a membership of 10 national associations of ISPs, EuroISPA is recognised as the voice of the European ISPs industry and its success lies in its reflection of the views of its members regardless of their shapes and sizes.

MISSION

- To secure Europe's leading position in the Internet industry and protect and promote its interests within it.
- To help deliver the benefits of the Internet to individuals whilst meeting the legitimate concerns around the more vulnerable members of society.
- To encourage the continued development of a free and open telecommunications market, which is essential to the healthy development of the Internet.

EUROISPA BOARD

Elina Ussa
President

Lars Steffen
Vice-President

Alex De Joode
Treasurer

Romain Bonenfant
Board Member

Dalia Coffetti
Board Member

EuroISPA

Rue de la Loi 38, 1000 Brussels secretariat@euroispa.org
EuroISPA @EuroISPA
EU Transparency Register ID: 54437813115-56