

010
1100101 1000110100 0100001
0101100 1 001101110001 0101111
0100000 0 0101 1 0110 1 0100001
0100011 011100011000100 00100011100 1011101
010001011 011100001001001001001 01001100001100000 01000110
01000111 0000010110000 0 1 0 1 0 0 11000110100001 110000111
01000110 11001010000010 1 1 1 0 1 0 11011100011001 011110001
01000101 10011010010010 0 1 1 0 1 100101011100 110010111
01011100 0010100110001 1 0 0 1 0 0 11000000101001 010110111
01010110 1011010010100 0 0 0 1 0 0110100011001 000100000
110010101 1001100100101 1 0 1 0 0 0 010000000110 00101011
01010110 101000101011100 1 1 1 0 1 0 0011100000101 00001111

THE VOTE FOR DIGITAL 2021 . . .



Internet Policy Agenda

Statements and recommendations for action for an
Internet with Responsibility



Content

Introduction	2
A Framework for Digital Policy in Germany and Europe	4
Foundations for Infrastructures and Innovation	8
Trust and Security on the Internet	12
Guidelines for a Trustworthy, Functioning Internet	16
A Sustainable Internet Industry in Open Competition	21
Importance of Data for Society and the Economy	24
A Digital Society: Interconnected, Democratic and Sovereign	26

Introduction

The Internet is the engine of our information society. It connects people and machines across the entire world. It has engendered new business models and revolutionised existing ones. Up until the advent of the Internet, the world's economy and society had not experienced such a fundamental change since the time of industrial revolution.

The Internet industry – operators of digital infrastructures, services and business models – is therefore a key industry and growth engine of our time. Its importance for the entire economy is steadily expanding, and its revenue volume in the European economic and financial zone has grown in recent years. We are experiencing a structural transformation that offers tremendous opportunities. More than ever before, we can say: The future is digital.

The spread of the SARS-CoV-2 virus and the associated pandemic have shown that digital technologies are not only of central economic importance, but that the Internet has also become enormously important for society as a whole. The Covid pandemic has highlighted just how important high-performance digital infrastructures are. Digital technologies are helping to sustain economic, political and societal life. The operators of digital infrastructures and the Internet industry are more system-relevant than almost any other industry branch. At the same time, however, Covid times made it obvious that there is still a need to catch up in digitalisation in multiple economic, societal and governmental areas.

The significance of the Internet industry has steadily grown. Its share of the overall economy has been rising continuously for many years now. In Germany, the Internet industry is expected to account for around seven percent of the country's gross domestic product in 2025. Meanwhile, despite a temporary decline in revenues due to the pandemic, these revenues are expected to rise to approximately 254 billion Euro by 2025.¹ As such, the Internet industry is one of the most dynamically growing economic sectors in Germany.

The growing significance of digitalisation for the economy, the state and society is also accompanied by increasing responsibility. Companies are being scrutinised more closely in their actions and must not only be accountable to shareholders, but also – more and more – to a critical public. Citizens are questioning their actions on the Internet and there are open debates about the role and status of digital technologies in the modern information society. Politics is also faced with the challenge of finding solutions to the issues of digitalisation. Sustainable location development, investments and the right balance for favourable framework conditions in digitalisation are the prerequisites for the competitiveness of Germany as a business location and, beyond that, for an open and democratic society that knows how to use digital technologies in a sovereign and self-determined manner. The

¹Source: "The Internet Industry in Germany 2020 -2025" from eco – Association of the Internet Industry and Arthur D. Little, weblink: https://international.eco.de/internet_industry_Germany_2020-2025/

decisions made in Berlin and Brussels set the course for further digitalisation in Germany and throughout Europe. In order to harness the opportunities and potential that the digital transformation offers for society and the economy for the benefit of general public welfare and public

interest, a modern Internet policy is imperative. With its Internet Policy Agenda, eco – Association of the Internet Industry sets out to highlight its views and ideas on digitalisation and, to this end, has compiled the most pressing demands of the Internet industry.



A Framework for Digital Policy in Germany and Europe

A future-oriented Internet and digital policy is emerging and developing dynamically. It is interdisciplinary and not tied to traditional ministerial boundaries. Internet and digital policy develop from the interaction and interplay of different actors and interests in politics, public administration, business and civil society – nationally, at the European level, and globally. Such a high degree of openness, transparency and interactivity poses special challenges for all those involved. Technical possibilities, future technological advances, and developments that cannot yet be foreseen and whose effects cannot be conclusively assessed must be taken into account, as well as the interplay of national regulations in a cross-border context. Time and again, the question therefore arises as to how the associated challenges and issues can best be managed on a consolidated basis, and where specific national aspects must be taken into account.

Germany needs a Ministry for Digitalisation

In the past years, the sheer importance of digitalisation has become quite clear. The political importance and strategic relevance of a modern and future-oriented Internet policy and the digitalisation of the economy, society and public administration go far beyond the mere provision of access to the Internet and broadband roll-out. The fact is that digital issues and challenges arise in all policy areas. With advancing digitalisation, new intervention points and possible fields of application continue to emerge, for example for electronic ID cards, digital identities, applications for public safety and healthcare (such as the Covid warning app) or digitalisation in the health sector – to

name just a few of the applications and to illustrate the breadth of the overall spectrum. In addition to numerous detailed regulations which are dealt with in the various ministries, there are, however, overarching central issues regarding the handling of data, services and networks, which require clear, efficient and rigorous regulation. What is called for here is a consistent and agile Internet and digital policy which is managed under one roof. In order to prevent attrition and achieve a coordinated, consistent approach, a piecemeal approach in this field must be avoided. The central and strategically relevant decisions must be made from a single source. This must be reflected in the distribution of responsibilities at the federal government level. This requires a restructuring within the federal government. The effects and

requirements of the strategically relevant topics of digitalisation must be consolidated within the German federal government and dealt with by one department as the lead ministry.

The work of such a Ministry for Digitalisation must also be mirrored at an institutional level. In this regard, it is imperative that a corresponding steering committee be set up in the German parliament. The past years have shown that central debates on Internet and digital policy in Germany have been discussed between the various ministries and have often been delayed and sometimes even blocked by differing views. An inconsistent digital policy overshadowed by departmental disputes – as has frequently been the case in central debates in Germany in recent years – must not be allowed to continue. It is quite clear that a paradigm shift is needed.

We need a structured and ambitious digital strategy for Germany

With the Digital Agenda from 2014, the German federal government for the first time compiled and defined priorities and goals for digitalisation in Germany. With the Digital Strategy 2018, the formulated goals were outlined and further concretised through numerous projects and plans. In order to advance digitalisation in Germany and to conduct a related meaningful public debate, clear priorities and focal points with measurable targets are needed. These should be set out in an ambitious digital strategy, which should include clear guidelines for

implementation, responsibilities and execution. The competitiveness of Germany as a business location will largely depend on this.

Internet policy must be approached from a European perspective

A fundamental concept of the European Union is to bring its 27 Member States closer together and to dismantle internal borders. This includes intensifying and expanding the political and economic links between the individual Member States and, at the same time, lowering or completely dismantling barriers and obstacles. A common European Single Market is stronger than its 27 submarkets and offers companies with a market of around 450 million inhabitants an excellent starting position and opportunities for economic success. However, a prerequisite for this is ensuring that standardised framework conditions prevail. European startups and SMEs in areas such as telecommunications or cloud can only operate competitively in a European Single Market and survive in a global environment if the following are in place: a consistent and standardised coordinated approach among regulatory authorities, clear geographical responsibilities for companies, and an assurance that the size of a legal department does not determine the success of a company in Europe. Therefore, a common European approach is vital and for the same reasons national go-it-alones must be avoided. Digital services and data must know no borders within the EU.

Common European values and standards can thus have an impact which goes beyond the Single Market. This is underscored by the increasing international awareness and significance of data protection beyond European borders, which has been clear since the adoption of the GDPR.

The free, open, decentralised and technology-neutral structure of the Internet must be retained and promoted. The Internet can only function if it is managed collectively in line with multi-stakeholder principles and cannot be dominated by individual actors or governments. In the course of the IANA Stewardship Transition, the German federal government has explicitly committed itself to the multi-stakeholder principle. We call on the German federal government to reflect this commitment in its actions. In this respect, the German federal government must also focus on international Internet policy and play an active role in shaping it. It is therefore important to build on and maintain the positive commitment that has been shown thus far. The German federal government and the ministries involved should expand their commitment at the European and international level and continue and intensify the activities undertaken to date with the relevant organisations and standardisation bodies.

When it comes to debating issues relating to the future design of the Internet, technical standards and interoperability, the necessary institutional framework is provided by bodies such as ICANN, IETF, other international and European

standardisation organisations, and groups and forums such as the Internet Governance Forum. In the case of international treaties that do not explicitly deal with the self-governance of the Internet, it must be ensured that the Internet's basic principles are maintained.

○ The European Digital Single Market must be seen as the goal and the central factor of all policy measures

When individual Member States of the European Union recognise challenges of digitalisation and, in response, try to resolve these at the national level, they do not create solutions that have long-term viability. On the contrary, specific national approaches and regulations create additional challenges and offload them to the company level. It is understandable that national solutions are easier to implement at the level of only one Member State. However, the resulting consequences and implications for all Member States must not be disregarded. The success of European companies depends to a large extent on the homogeneity and strength of the European Single Market.

The more standardised and harmonised the regulations in the Member States are, the stronger and more attractive the European Single Market will be. To allow European SMEs and startups to be set up and companies to open up new markets across internal borders and survive in international digital competition, harmonised framework conditions are essen-

tial. It is therefore important that the goal of a common European Digital Single Market is placed in the foreground of the Member States' political measures. Member States must prioritise European regulations and not pre-empt national measures – especially when European proposals are already on the horizon. The vision for a European Digital Single Market can only become a reality if the EU institutions – the Parliament, the Commission, or also the Council – and the Member States work together and pursue a common goal. National legislative projects such as the German Network Enforcement Act, the Austrian Communication Platforms Act, the French Avia Act or the various forms of digital taxation in France, the Czech

Republic or Austria exemplify the different approaches and trends at the level of the nation states, which run counter to a coordinated and harmonised approach at the European level. When it comes to regulations of international relevance, no specific national approaches should be taken, but viable European solutions must be forged in a global digital environment. Only if the Single Market is given precedence will companies have a real chance to prove their worth in international competition. Multiple regulation in the Member States causes companies to remain restricted to individual nation states, or to not even venture into other markets in the European Economic Area.

Foundations for Infrastructures and Innovation

Digital infrastructures and services must not only be available and accessible to users, but also to society, the state and the economy. Innovation can only emerge in an ecosystem that comprehensively covers and addresses digital infrastructures and the services which are based on these. Otherwise, applications that are built on these infrastructures cannot be meaningfully deployed, nor can their potential be realised. But there must also be clear and comprehensible framework conditions for technologies and applications. Innovation can only emerge in an environment that offers the foundations and incentives for development and testing and at the same time creates acceptance for the use and implementation of digital technologies.

○ Technology must be ubiquitous and accessible

In order for digitalisation to be accelerated in Germany, the necessary technology must be accessible and available for use throughout the country. Germany and Europe have a structural disadvantage here due to their distinctive economic structure, which is made up of many small and medium-sized enterprises with complex supply chains and supply structures. In contrast, Asian and North American countries, whose economies are predominantly characterised by large, well-financed corporations, are more easily able to accelerate technologies and their widespread application and thus set technical standards. Against this background, a critical success factor for digitalisation in Germany and Europe is access to technology which is as open as possible via appropriate interfaces and common standards. Projects such as Gaia-X

exemplify how collaborative and open innovation can be developed and prosper. With Gaia-X, the potential is created to be able to offer services and products throughout Europe. In particular, it creates an opportunity for SMEs to operate beyond national markets in the Digital Single Market – together in a network.

In addition to the technical framework conditions, when it comes to access, technical regulation should also not present a barrier. The complexity and granular nature of regulations and standards, especially when it comes to future technologies with a high cross-sectional significance for society and the economy, are often the critical factors that prove to be an obstacle to innovation. For strong digital sovereignty, it is important to find a balance for regulation. Elementary digital technologies of the future must therefore not be subject to more stringent regulation than comparable analogue

services and products. To ensure access and availability of digital technology, the European market should respond appropriately to supply chains and corresponding needs and challenges. One key success factor for this is also the import of knowledge and technology, as well as the use and deployment of technology from other markets and countries.

○ Artificial intelligence must be subject to the same rules as other products on the market

As a key technology, artificial intelligence (AI) has meanwhile attracted prominent attention and gained significance in the political debate. Numerous matters raised by modern AI systems are already regulated in corresponding specialist laws, for example for the financial market. In addition, the general regulations for data protection and the field of IT security also apply to systems and applications based on artificial intelligence. The cross-sectional technology of artificial intelligence is now entering into a well-developed regulatory environment.

In spite of this, new rules for artificial intelligence are not just being discussed in Germany – for example, by the Data Ethics Commission – but also in Europe. Such cross-sectional regulation only takes limited account of the various use scenarios of AI and the specific challenges and risks associated with these. As such, further regulations should be developed primarily with regard to selected sectors and use scenarios.

The application of a blanket AI regulation on top of existing rules should be rejected. The German federal government has held out the prospect of a related approach in the update of its AI Strategy 2020. While taking into account the existing general rules, such as the GDPR, this pragmatic and purposeful approach should be pursued, should support standardisation, and should also be promoted and taken into account at the European level.

○ Net neutrality is an important principle for both safeguarding the open Internet and for competition

With the adoption of the European Telecoms Single Market Regulation at the end of 2015, Europe set a milestone for the safeguarding of the open and free Internet (net neutrality). Accordingly, networks must be connectable and accessible for different providers. There must be no unjustified discrimination against individual services. At the same time, there should be room for the development of new and special offers and for fair competition. Regulation must continue to strike an appropriate balance between the interests of end users and those of all access and content providers. This principle must remain intact in the future and be secured by the political actors in Berlin and Brussels. Net neutrality is a guarantor and essential cornerstone that has enabled the Internet to develop into a digital ecosystem which has low-threshold access and a multitude of digital services and business models built on it.

○ The Gigabit Society must become a reality in Germany by 2025

The growing trend is for devices to be connected and to become intelligent by linking and analysing data, and the associated emergence of new digital ecosystems and business models. Connected cars, the Internet of Things, Smart Cities, artificial intelligence and the 5G mobile communications standard provide just a few examples of where we are heading. Digitalisation and the Internet have become an integral part of our everyday lives. The structural transformation affects almost all areas of industry, the economy and society. For this digital transformation to succeed, the gigabit roll-out is the most important infrastructure project for Germany and must be resolutely driven forward. Both the European Union and the German federal government have set themselves the goal of having the Gigabit Society come to fruition in the next few years. In Germany, the Gigabit Society needs to become a reality by 2025. To this end, many projects have been initiated and schemes launched – but this must not be the end of the story. The roll-out of high-performance digital gigabit infrastructures must be driven forward even more resolutely, with this remaining the most important infrastructure project for the coming years. In order to achieve a technology-neutral Gigabit Society which also functions as a driver of innovation, digitalisation and Industry 4.0, there is a need for clearly defined milestones and target-oriented priorities. The societal and economic importance of digitalisation and

efficient technology-neutral infrastructures has been strongly highlighted by the impact of the Covid-19 pandemic. Germany can only maintain and increase its competitiveness on the strength of the Gigabit Society.

○ Network operators need fair framework conditions that support competition, roll-out and innovation

It goes without saying that we need universally available, high-performance digital infrastructures to achieve the goal of a Gigabit Society. In order to actually bring about the infrastructures needed for this, what is needed are financial resources and considerable efforts on the part of the companies that construct and roll out the infrastructures. The challenge is to set a sensible political course, because a politically proclaimed goal of “fast Internet everywhere” will not be realised on its own and will not automatically lead to a nationwide fast Internet. In order for the roll-out to progress, companies need legal and planning certainty.

The transposition of the European regulatory framework for telecommunications must create fair framework conditions that support competition, roll-out and innovation, while at the same time taking consumer protection demands into account. A practicable implementation of the regulations on co-investments and collaborations would stand to accelerate broadband roll-out while ensuring fair and effective competition. To achieve this, it would

make sense to streamline and accelerate the construction and funding procedures.

The approvals needed for the construction and roll-out of gigabit infrastructures at the municipal level must be accelerated and simplified. In this regard, a notification obligation instead of an approval procedure would make a decisive difference. State-funded support for network roll-out should continue to be applied only in cases where self-funded roll-out will not take place due to a lack of economic viability, even in the long term. Subsidies must not displace, distort or even devalue the self-financed roll-out on the part of the companies. A

forward-looking and Europe-wide coordinated frequency strategy, including the provision of further mobile network frequencies, is necessary for the further development and roll-out of the mobile network infrastructure. The future orientation of frequency regulation must create more legal and planning certainty in order to improve the conditions for mobile network roll-out. Any funding of mobile network sites must be competition-neutral in order to close remaining gaps. With the funding of new 5G/6G technologies (OpenRAN), a manufacturer-independent and open-interface approach can be pursued that contributes to the goal of digital sovereignty.



Trust and Security on the Internet

Trust and security are basic prerequisites for the success of digitalisation. If users do not trust the technologies they use, digitalisation cannot be long-term and sustainable. If companies are unable to provide trustworthy and secure services and applications for their customers, digitalisation cannot succeed. This makes IT security the fundamental cornerstone and central element of the debate on the trustworthiness of digitalisation.

○ Civil rights must be respected in online investigations and prosecutions

Criminal prosecution via the Internet is presenting a constant challenge for the police and investigating authorities. The seemingly simple possibility of collecting and assessing information and data is seen by them as an opportunity in the fight against crime. Against the backdrop of combating particularly serious forms of crime such as terrorism or drug trafficking, the rights of law-abiding citizens are increasingly being affected and civil rights are being put to the test. For example, in the case of the planned electronic preservation of evidence, as is currently being developed with the European Union's e-Evidence Regulation, care must be taken to ensure that the regulations meet the fundamental rights standards for the integrity of the sphere of private life and that those affected are also given the opportunity to take legal action. In view of the developments in some EU Member States on the constitutional principles, corresponding laws and regulations should contain an effective provision that makes it possible to temporarily suspend the application of the respective legal act.

eco is opposed to blanket data retention without cause. This represents a disproportionate encroachment on fundamental rights and imposes enormous costs on the Internet industry. It is regrettable that the German legislature has not taken up on the opportunity of ongoing legislative procedures in order to finally repeal the data retention regulations which have applied to date. Instead of capitalising on this opportunity, the existing legal regulations on data retention have ultimately been upheld and further applied. This is not acceptable for either societal or economic policy. To send a clear political signal regarding the renunciation of the data retention without cause, it is imperative that the legal regulations on data retention are finally revoked. In view of the current case law of the European Court of Justice, the German federal government is obliged to repeal the German regulations and to conduct evidence-based and credible research into alternatives.

○ The security and integrity of networks and services must be systematically strengthened and rolled out

Trust in digital services and products and their integrity are the central factors and elements for a successful digitalisation and Internet policy. In order to build trust in services, they must be designed as securely as possible, in keeping with their importance and relevance for the economy and society. Aside from the challenge presented to service and product providers and developers in developing and adapting these services with the most up-to-date state-of-the-art technology, politics also has a special responsibility in this domain.

Time and again, demands for central access to services and the issuing of passwords are made by politics and law enforcement agencies. These demands are a critical and neuralgic aspect for IT security as a whole, as they systematically undermine trust in digital services and the security of personal data. The security of services and networks must always be guaranteed. State measures that can potentially affect the security and integrity of services and networks may only be undertaken if they are based on generally transparent and comprehensible rules on which users can rely and which take the importance of such services and networks into account. Only in this way can the state ultimately ensure that trust in the security and integrity of digital services is maintained.

○ The deployment and application of encryption technologies must be rolled out and funded

Strong encryption is a key factor for secure services and products. At the very least, almost all messengers and services now use transport encryption, and many also use particularly secure end-to-end encryption. But there are still challenges and, in some cases, a need to catch up. For example, many websites are still unencrypted and do not have suitable certificates for authentication. Here, in addition to industry endeavours, politics must also act. The deployment of current, state-of-the-art security technologies and their consistent application for the encryption of websites, services and products should be actively funded and supported by politics.

Likewise, security authorities, state actors and public administration bodies must not take any measures or initiatives that threaten or structurally undermine encryption. The issuing of keys or regulation of encryption standards, as repeatedly discussed at European and national level, must be strenuously avoided, as must measures that force companies to lower encryption standards or undermine encryption in their services.

Here, politics is called upon to consistently strengthen the trust of citizens in digital technologies. State interests must be secondary to the integrity of services and networks as well as the needs of society and the economy for secure and trustworthy communication.

○ With the involvement of all stakeholders, the IT security standard should apply an equal balance to responsibility and capabilities

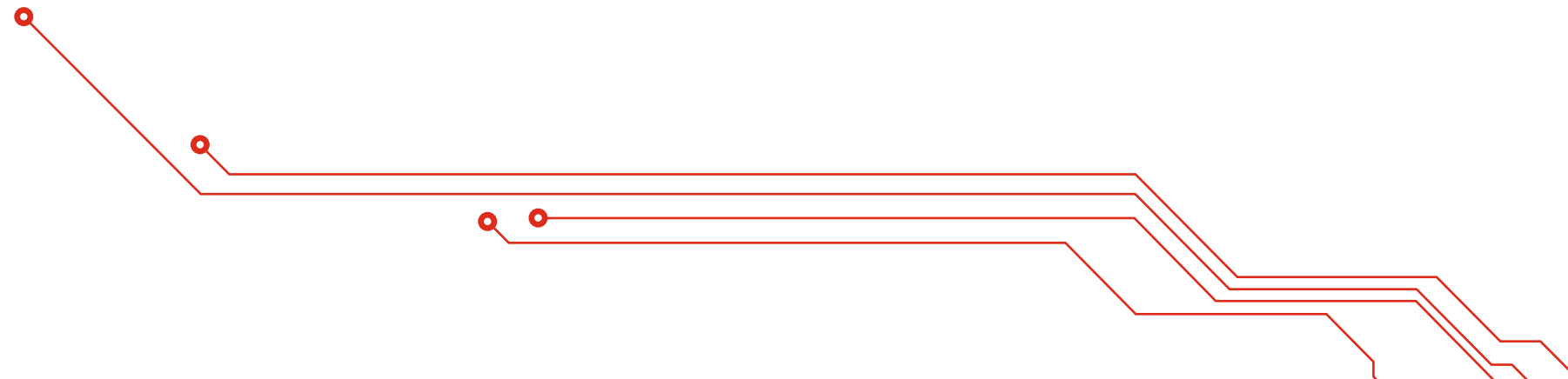
As the economy and society continue to digitalise, the need for protection and the importance of IT security also increases. Against this background, and in order to strengthen trust in digital technologies, the field of IT security and IT security technologies must be rolled out and funded. This requires a related awareness throughout the economy and society, as well as the development and consistent use of IT security technology in German business and industry. Ideally, security concepts (Security by Design and Security by Default) should already be included in the development of services and products in order to be able to guarantee a high level of security.

IT security is a challenge for everyone involved: operators of services and networks, manufacturers of devices and components, but also users. Time and again, the question arises as to who should bear the responsibility for the security of these services and products. There

is no simple, general answer to this, because IT security as a whole can only ever be as strong as its weakest part.

Responsibility for the security of services and products can only be taken on in a joint capacity. It cannot be attributed to one actor alone. This is especially the case where actors are working on the basis of services, devices and products that are connected via an open Internet – one that is accessible to everyone – and that can be connected and combined with each other as desired by users.

It is therefore important that politics assumes a joint approach to IT security in dialogue with users and providers. Mutual, interdependent and complementary contributions and responsibilities can sustainably increase the overall level of IT security. IT security cannot be designed to be centralised; it must be decentralised. This is necessary for improved resilience, especially in view of the fact that digital applications and services are becoming increasingly important and thus more relevant for society and the economy.





Guidelines for a Trustworthy, Functioning Internet

The discussions on legal regulation and enforcement on the Internet are a challenge for the Internet industry and users alike. The attempts to date by politics to develop stringent rules based on clear principles are constantly being confronted with new challenges. From the point of view of the Internet industry, there is a need for more in-depth discussion about which principles have proven themselves to be effective and which rules need to be made more concrete, especially in view of the upcoming reorganisation of the legal framework and thus of the fundamental digital rules at the European level.

o The Notice and Take Down principle is the basis and foundation for law enforcement on the Internet

The Internet has developed at a steady pace over the last two decades: New services have emerged, user patterns have changed, and the Internet has now penetrated all spheres of business and society. This raises questions as to whether the previous assignment of responsibilities and the liability structure are still up to date. The background here was technological development, a broader range of services, and changes in user behaviour. This has all led to a debate on the further development of the legal framework.

The Notice and Take Down (NTD) procedure, as introduced by the 2000 E-Commerce Directive, has proven its worth as a standard procedure. It provides a solid basis for law enforcement on the Internet. Internet service providers are obliged to remove illegal content as soon as

they become aware of it. This is coupled with corresponding liability. Supported by the work of hotlines such as the eco Complaints Office, illegal content is taken down within a few hours or days in Germany, as well as abroad via international networks. This procedure is much more effective than the repeatedly called-for Internet blocking, which only presents a minor technical hurdle.

At the EU level, a core topic currently under discussion is an update of the E-Commerce Directive: namely, the Digital Services Act. In this regard, the EU Commission has presented an ambitious draft. The proposal, which is attracting a great deal of international attention, is to adopt the liability rules and the ban on general monitoring obligations from the E-Commerce directive, transfer the NTD principle into a legislative procedure, and introduce additional obligations for either all online platforms, or for those that are very large.

It stands to reason that companies in the Internet industry are opposed to their services and offerings being used and abused for illegal and illicit activities. Accordingly, Internet Service Providers (ISPs) have a vested interest in preventing illegal use of their services and in promptly removing illegal content from their systems. The concept of giving large online platforms more responsibility – as long as the regulations are clearly designed, and legal certainty is ensured – is understandable. This is also enhanced by the clarification that ISPs will in future be able to undertake an explicit active search for illegal content on their systems without simultaneously losing the liability limitations.

However, the EU's proposal is being undermined by national initiatives. In addition to the French proposals, these include in particular those from Germany, such as the Network Enforcement Act (NetzDG) or the Act on Combating Right-Wing Extremism and Hate Crime. In addition, terms such as "illegal content" or "legal but harmful content" must be clearly distinguished from each other and defined in a legally secure manner.

The discussions on the Copyright Directive also contribute to the NTD topic. eco regards the mandatory use of filters to block (re)uploading of content as serving little purpose. In order to filter content, it is in principle technically necessary to check all content and to verify its compatibility. The ECJ has repeatedly ruled against this mandatory use of filters, due to its

massive encroachment on fundamental rights. In Germany, too, the Copyright Directive was planned to be transposed without the use of upload filters; a political declaration of intent that is obviously not being followed up in the transposition. And planned exemptions are being unnecessarily restricted to the detriment of the online world, and arguably in contravention of the directive's stipulations.

Companies in Europe are increasingly faced with the challenge of different regulatory approaches in the various Member States. There is a need for aligned and harmonised regulation within the Single Market. Standardised regulations that apply throughout the EU, with clear allocation of responsibilities, are a prerequisite for the functioning of the Digital Single Market. In addition, users must be given an appropriate understanding of how to deal with online media and technology. Internet Service Providers must – and want – to make their contribution when it comes to taking down illegal content. But forcing them to take on the original role of the judiciary cannot be the right approach. There is also a need for a judiciary and executive apparatus with the appropriate technical and financial resources.

Efforts at national and European level should focus on the further development of a reliable legal framework for the Internet industry, which is at the same time flexible enough to incorporate technological and economic developments and to promote further innovations.

○ The state must ensure law enforcement and assume responsibility for law enforcement on the Internet. Governmental tasks should not be offloaded to private companies

For an effective and sustainable fight against illegal and illicit Internet content, consistent law enforcement is indispensable. The judiciary and law enforcement must therefore rectify existing deficits in law enforcement systems – from a personnel, financial and technical perspective – to ensure effective and long-term law enforcement. It must not be the sole responsibility of private sector Internet service providers to assume responsibility for law enforcement, as that would mean assuming responsibilities originally assigned to the state and bearing associated risks. This also applies to proactive reporting obligations of network operators, such as those provided for in the German Network Enforcement Act.

The continuous offloading of law enforcement to private providers in this sensitive area is problematic. It is not a manifestation of the state's legal capacity and does not correspond to the state's claim to sovereignty. Here, the state must exercise its right to shape the law. Proactive initiatives by the industry can provide important support and make an important contribution, but they cannot replace sovereign measures such as law enforcement and criminal prosecution by the state.

○ Copyright needs an upgrade to meet the Digital Age

Digitalisation and the increasing availability of digital content via the Internet both pose a challenge to existing copyright law. One of the most important and largest projects has been the amendment of copyright law at European level. After more than two years of discussions, a compromise was reached under considerable time pressure to finalise the copyright amendment. Regrettably, the opportunity was not seized to arrive at an amendment for a modern copyright law that does justice to the Digital Age. The ancillary copyright and the controversial upload filters illustrate just how divergent the views are and how far copyright law has distanced itself, not just from the everyday lives of citizens, but also from digital development.

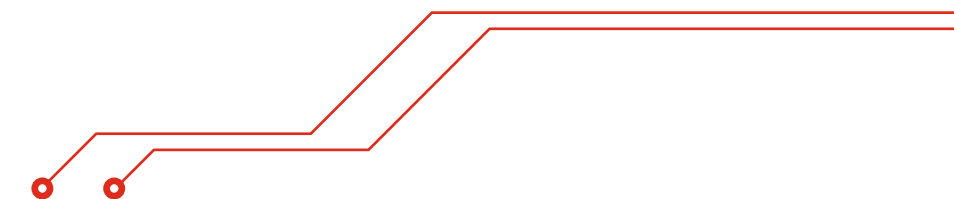
Copyright law is still regulated and structured differently in the 27 EU Member States. Different protection periods, divergent areas of application and variant exemptions present a challenge that is almost impossible to overcome in practice, not only for large Internet service providers operating across borders, but also for SMEs in particular. Even the users of these services are ordinarily not aware of the different treatment or the variant legal bases. They are frustrated when services are not offered or available in their country due to national restrictions. The European Union has made initial attempts at legal harmonisation through various legislative measures. During brief stays in other EU countries, users can now at least return to

the previous normality of accessing various streaming services.

The licensing of sports and films continues to take place primarily at national level. The continuing fragmentation of copyright law and the divergent approaches in the Member States must be critically questioned.

This is also accompanied by an ever-growing problem of acceptance. With the increased use of the Internet and the spread of digital services, the interaction of citizens with copyright law – whether in a social, private, or professional context – has increased considerably. Whole generations are now growing up with the Internet. At the same time, most of the population is not familiar with the regulations on dealing with copyright-protected content on the Internet or considers them to be difficult to understand. This tends to illustrate how far copyright law has moved away from the realities of life and how outdated the regulations are and reveals how little the current status quo is digitally appropriate and future-proof.

In this context, the developments concerning filtering regulations and antiquated ancillary copyright are also alarming and make it clear that in these areas, too, we should not orient ourselves to the past; instead, we should track developments, identify synergies, and openly discuss possibilities for adaptation and improvement to the practices and wishes of the population, with the involvement of all stakeholders. A rethink must take place here: for the benefit



of Internet users as well as the German and European digital economy. We need a digitally suitable update of copyright law that creates a fair balance of interests between authors, users, and companies.

○ Users also must take responsibility and develop an understanding of right and wrong on the Internet

Based on a voluntary pledge, in 2018 the operators of social networks active in Europe made a commitment to the EU Commission to engage more strongly in the fight against false information in the digital space. Due to the continuing spread of false and misleading content, including in reports on the Covid pandemic, the EU Commission presented the European Action Plan for Democracy at the end of 2020. The Action Plan aims to strengthen democracy in Europe.

In detail, measures are planned to promote free and fair elections, to strengthen media freedom and media pluralism and to combat disinformation. From a content and timing perspective, the development of concrete measures has not yet been defined in more detail, but these factors are also complex due to the sensitive nature of the topic. Freedom of expression must be safeguarded, while the potential for social and societal tension arising from false news poses challenges for governments and, increasingly, for law enforcement agencies. At the national level in Germany, illegal content by

users is regulated by the Network Enforcement Act (NetzDG). The NetzDG obliges the operators of social networks to check reported content and to take it down or block it if it violates the German Criminal Code (StGB).

The transparency reports of the operators of social networks show that they take targeted action against illegal content in accordance with the German Criminal Code. Due to the general and Europe-wide importance of the

topic, the Internet and digital industry call for the development of common standards to combat disinformation, hate speech and incitement at the European level. In principle, the legislature should more intensively promote initiatives for educating users – especially on applicable rights and obligations in the digital space – and intensify its commitment to educating people about the use of digital media – for example, by taking measures on digital education and ethics.

A Sustainable Internet Industry in Open Competition

It is now impossible to imagine economic life without digital technologies. These technologies have led to structural transformation and disruption in traditional economic segments and created new business models. This has often posed challenges for established industries as well as for politics, with the response being regulation. Competition regulation for digital companies is a central issue here. In parallel, the cross-border activities of digital companies raise the question of appropriate taxation. And more and more frequently, the question arises of the extent to which digital technologies can contribute to a more ecological shaping of the economy.

○ Harnessing the sustainability potential of digital technologies for climate change

Germany and Europe will only be able to achieve their ambitious climate goals through the rigorous use of digital technologies. If existing innovation potential is consistently harnessed, digital technologies will make a significant contribution to achieving the climate targets. To take just a few examples: CO2 savings potentials will be derived from the mobility transition and from efficiency increases via Industry 4.0, Smart Cities and other application scenarios.

For digital technologies and applications to continue to have a positive influence on the climate footprint of the future, accelerated digitalisation is indispensable. Digital technologies and infrastructures are a central contribution to an ecologically sustainable digitalisation. In order to harness the sustainability potential of

digital technologies, an integrated approach is needed that combines digital infrastructures and technologies into an ecosystem. The prerequisite for this is a functioning digital ecosystem consisting of energy-efficient data centres, cloud-based applications, a nationwide gigabit network, a rapid roll-out of 5G networks and energy-efficient software.

However, sustainable and climate-neutral digitalisation can only succeed with political support. This requires a politically managed phase-out of fossil fuels in Germany, the resolute expansion of renewable energies, enabling the systematic utilisation of waste heat from data centres, a nationwide roll-out of gigabit infrastructures, and the deployment of 5G technologies. In addition, the increased use of “Power Purchase Agreements” (PPA) can also lead to a reduction in CO2 emissions from the use of digital infrastructures in Germany.

○ Standardised and consistent regulations and taxation for all companies and business models

The past few years have shown that, due to their significance for competition and their economic performance, digital companies and business models such as platforms have become the focus of state regulation projects at national and European level. This focus has led to projects to regulate platforms and the introduction of a digital tax.

Various regulatory projects show that the regulatory approaches applied to date that are based on the "one size fits all" principle do not lead to applicable legal provisions for digital companies and business models. Instead of striving for a detailed and sweeping regulation of digital business models, framework conditions must be created that guarantee companies' planning and legal certainty for investments and innovations. Regarding the taxation of digital companies, products and services, there is a need for a coherent international regulatory framework, on the basis of which no special taxes are levied and the risks of double taxation are minimised, and where analogue and digital business models are treated equally. On these grounds, the development of a common and internationally agreed taxation framework for revenues from digital business models, with the support of the Organisation for Economic Cooperation and Development (OECD), is an effective approach that should be further pursued.

○ We require a modern and competitive legal framework for digital business models that enables innovation and investment

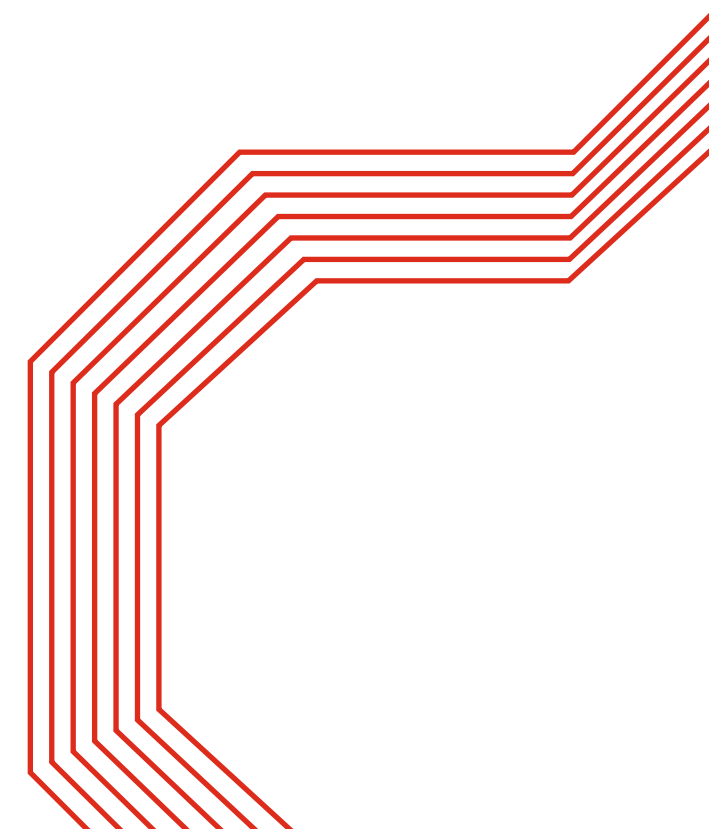
In addition to regulatory frameworks that must be foreseeable and manageable from a planning perspective, bureaucratic hurdles should be removed for the development of digital companies and business models. The "one-in, one-out" rule established by the German federal government for reducing bureaucracy should be expanded and existing regulations should also be reviewed for opportunities to further lower bureaucracy.

In parallel to the current funding programmes, efforts should be made to improve the legal situation for private investors, and also to further strengthen the relationship between founders and entrepreneurs and investors. To prevent the outflow of companies founded in Germany and national innovations, framework conditions must be created for venture financiers, insurance companies, investment companies and public or private pension funds, making it easier for companies to invest in future technologies. The focus should be on innovation and investment-friendly framework conditions. In addition, applying a focus to an ease-up of the bureaucratic burden is advisable. In the context of these innovations, a greater focus should be applied to competition law, while the 10th amendment to the German Act against Restraints of Competition (GWB) should be critically reviewed once again to determine the extent to which it is associated

with obstacles to growth, especially for small and medium-sized enterprises that take up on the market's first-mover advantages. The legal uncertainty that the 10th GWB amendment has specifically created for digital companies must be taken out of the equation.

Rather than seeking further amendments at national level to regulate competition in digital business models, the efforts of the German federal government should instead be applied to further negotiations on the Digital Markets Act (DMA) at European level. The DMA should pursue the goal of implementing a harmonised, binding and proportionate competition framework for digital business models. Legal uncertainties and the associated negative effects on innovation and growth should be avoided on the basis of clear and carefully designed regulations. A key element in this regard is the shaping of appropriate legal protection.

Harmonised rules and a participatory dialogue, as already established in the GWB, would also help to ensure that future obligations of companies are described clearly and precisely and are in line with consumer interests and benefits. These would also promote legal certainty. As such, future obligations should be harmonised, developed and further specified in a participatory process before they become applicable on a European level and binding for specific digital products.





Importance of Data for Society and the Economy

In the Digital Age, data is not only a central factor for economic value creation but can also make a significant contribution to overcoming societal challenges. Demographic change, the energy transition, the digitalisation of the healthcare system, or concepts for Smart Cities or connected mobility: all of these provide an outlook on the growing importance of data for the economy and society. Digitalisation has created a new impetus for the discussion on how to deal with data – especially personal data – and has elevated its importance. The focus is on issues arising from the increasing data-centricity of value chains: be it access, use or sharing of data. Rarely before has it been so easy to evaluate large amounts of data and to derive decisions from this data, which have already been partially automated. This not only raises the question of how to deal with such personal data, which is closely linked to the sphere of personal life. The question of which data should be made accessible to citizens and companies must also be discussed in the context of shaping a functioning community and a more data-driven economy.

○ Consistent and standardised data protection rules for all stakeholders

Data protection remains a central issue of digitalisation for politics, even after the adoption of the General Data Protection Regulation (GDPR). Since the GDPR came into force in 2016, Germany has also taken significant steps to advance the national transposition of the regulation. However, the transposition of the GDPR and further debates, such as those on transatlantic data exchange, have made it clear that further efforts and more consistent steps towards harmonising data protection in Germany and Europe are necessary. The data

protection rules should be applied as uniformly as possible across the board and be comprehensible, transparent, and practicable for all parties involved. The one-sided prohibitive data protection supervision that has prevailed so far must be extended and supplemented by clear proactive support from the data protection authorities for companies, developers and service operators. The complexity of data protection regulations can only be implemented in a practicable and manageable way if the supervisory authorities also provide support and advice. Even after the entry into force of the GDPR, the consistency of data protection regulation has continued to be the central challenge in this

area. The considerations on establishing further regulations for a digital world within the framework of an ePrivacy Regulation can – similar to other area-specific regulations – further concretise the framework of the GDPR and develop it in a practicable way.

At the same time, however, the discussions that are underway also raise concerns that, if they largely undermine existing principles and create specific regulations for digital services and products, this could further increase already existing ambiguities and uncertainties for citizens, businesses and service providers and developers. Data protection rules should be transparent, comprehensible, fair and proportionate and apply equally to all market participants.

○ Access to data for citizens, companies and public administration bodies should be clarified through transparent authorisation criteria

Data is contributing to the digital transformation of the economic sectors of production, energy, logistics, mobility and health. Access to data, also from public institutions, can create more societal benefits. Today, data not only forms an important basis for data-based digital business models but is also becoming increasingly important for the services sector and for industry.

Advancing automation and the start of automation are playing an important role in the economy and society as a whole, and their significance will increase exponentially in the

coming years. The General Data Protection Regulation has established a solid and strict regulatory framework that restricts the processing of data and thus also protects citizens' rights to privacy.

In addition, there is a need for research and development of further approaches and solutions for the intelligent use of data, for the secure and legally compliant use of data, and for the use of baseline technologies such as AI-based systems, innovative data management and distributed data systems. In this context, it is imperative to clarify what form of data is involved and to what extent legally compliant processing of non-personal data, in particular, is possible. This means that, in the future, there will also be greater clarity for companies concerning, for example, the possible uses of M2M data or metadata.

In order to achieve the goal of a connected digital society that responsibly uses services and products developed in accordance with German and European data protection rules, application and usage scenarios must be further specified. This is as much the task for the legislatures in Germany and Europe as for the authorities and agencies entrusted with the supervision of data protection. For the development of digital technologies to proceed in a legally secure manner, there is a need for clear authorisations that set appropriate standards within the framework of European and German data protection law, and that accompany and enable the further development towards a data-centric and data-based economy and society.

A Digital Society: Connected, Democratic and Sovereign

Digitalisation brings with it new challenges for society. We are experiencing an age of upheaval and transformation that will fundamentally alter our society in terms of its social and cultural structure. The structural change of society is a dynamic process in which digitalisation is acting as a catalyst for societal transformation. Digitalisation will fundamentally shape, determine and ultimately transform our way of life. In order to shape this far-reaching transformation and associated changes, solutions must be found for politics, companies and citizens. Ultimately, it is about harnessing the opportunities of digitalisation to improve quality of life and maintain well-being.

○ Access to digital education at all levels of the education system and during all phases of the educational path is a fundamental prerequisite for the successful digitalisation of the working world

In an increasingly digitalised working world, there is a need to achieve as much participation as possible in the new forms of work and to integrate those whose tasks are becoming increasingly automated. This requires an education system that takes into account the principle of lifelong learning and, in doing so, establishes teaching and learning via digital media and digital technologies at all levels of the education system. A broad and easily accessible curriculum for teaching digital skills in all areas of school learning, a permeable education system, and the additional promotion of further and professional education rounds off the picture of a sustainable education system. In order to secure the innovative strength of the German economy and the availability of

suitable skilled workers in the long term, it is not only necessary to teach IT skills and the basics of computer science across the board, but also to place the ability to make judgements and solve problems in the focus of education policy efforts and to ensure greater educational equity.

○ Digitalisation opens up additional opportunities for more equal opportunities and diversity

In keeping with an opportunity-oriented working world and the long-term securing of suitable skilled workers, digitalisation enables additional opportunities for the participation of candidate groups that have so far been under-represented in the labour market. Digitalisation and interconnection are creating new and different working environments that act as a catalyst for equal opportunities and diversity. In order to further expand and intensify the com-

mitment and efforts of politics and business to having more female professionals and managers, framework conditions must be created that enable a better work-life balance (better childcare options, more all-day schooling, a more equitable distribution of family responsibilities) and the further development of career opportunities for women. At the same time, it is also important to open up the opportunities of the digital working world to other applicant groups by means of a broad range of educational opportunities and the quick and smooth integration of foreign and immigrant skilled workers into the labour market. Finally, thanks to automation, digital work processes and the decreasing importance of physically demanding jobs should facilitate the employment of people with disabilities and older people.

○ Newly evolving worlds of work require flexible frameworks

During the times of the Covid pandemic, it is not only daily life that has become more digital. In these times, employers and employees have also had practical experience with connected and digital work processes; in some cases, this has been something new and unfamiliar, while in others, it has gone well beyond what had seemed to become the norm in the past. The trend towards digital and connected working will continue, not least because of the pandemic-related experiences.

As a result, companies that have increasingly relied on mobile working during the restrictions

imposed by the pandemic and the tightened company regulations will in the future also want to enable and offer their employees hybrid working models, as well as more flexibility and independence. These companies need legislation that addresses the realities of the digital working world and takes the interests of employers and employees into account.

This is less about introducing additional regulations and more about adapting existing labour laws to the requirements of mobile working, while at the same time safeguarding occupational health and safety. Examples in this area include not just working hours, break regulations, occupational health and safety measures, insurance law aspects, tax issues (workrooms more easily deductible for tax purposes, tax benefits versus commuter allowance), but also legal certainty with regard to equipment, the borderline to teleworking, and the consideration of how to protect workers from being constantly available and from physical and mental health risks. Flexibility, the possibility to work independent of time and place, home office and mobile working will shape the working world of tomorrow. Legislation must be adapted to the new circumstances of the more flexible working world (working time, occupational health and safety, tax aspects) and set a legally secure framework for mobile working.

○ Competences and handling of digital technologies and information are a central building block of a digital society

Open and modern societies must give people opportunities for mobility, access to education, and participation in society, the economy and politics. Moreover, any initiatives that eliminate existing inequalities in existing programmes and systems should be strengthened and supported. Digitalisation can also make an important contribution to making existing inequalities and injustices in the economy, administration and society visible, with this enabling solutions to be developed.

Due to advancing digitalisation, media use has also changed greatly in recent years. Individuals are increasingly stepping forward – usually with the help of platforms for blogging, for example, but also in the field of audio and video production – and becoming creatively active themselves. It is becoming increasingly difficult to draw a classic separation between sender and receiver. With increasing numbers of users, the Internet is becoming more and more a mirror of society. However, the increased interconnection of citizens and digitalisation also makes negative social developments visible. The discussions about hostility and hate messages on the Internet highlight worrying tendencies that must be resolutely countered.

Germany and Europe need a functioning media system for the Digital Age. Digitalisation places new demands on how people interact professionally and privately in a society and how they perceive the world. It also changes the way people learn things and what things they learn.

In order for people to master digital technologies in the future, there is a need from the very outset for an all-round strengthening of education and training in media and IT competence. An education system that covers the entire spectrum of digital education is therefore something that we cannot do without. Starting at primary school age, pupils must be taught step by step how to handle and process information. In this way, they will learn to master digital technologies and understand how they work and what they do.

Last but not least, the education system in Germany must undergo a digital transformation.

The Covid pandemic has made the existing deficits in the area of digital education patently visible. Concepts for the nationwide implementation of digital education are necessary. Pupils and teachers need digital learning platforms and, above all, a learning and education concept that enables home schooling. In addition to investments in modern information and communication technology, as initiated by the Digital Pact for Schools, the focus should also be increasingly on lessons and teaching staff.

The experience of the Covid pandemic has shown that the virtual classroom must not only be a supplement to face-to-face teaching but must be an equitable elementary component of the education system.

○ The state and public administration must actively contribute to a digital society

Digitalisation is not only a challenge for the economy and society. It is also a challenge for the state and public administration. Central challenges for our society, such as demographic change and increased urban sprawl, make modern e-government and the accelerated digitalisation of the care sector and the health system decisive factors for a state that is capable of acting across the board and for a society that is adequately taken care of – even in times of crisis. The state and public administration can also take on a pioneering role in digitalisation in Germany through tendering and award processes and their own applications, and also – given that they set and address demands – can trigger new ideas and momentum.

The strengthening and promotion of standards for secure digital identities, ideally in a Europe-

an or international framework, is a significant factor for consistent and successful digitalisation, along with the development and provision of open standards for digital administrative applications and corresponding investments by the government and public administration. The Covid pandemic has also highlighted existing deficits and shown that the state and politics must become more digital in order to develop a higher degree of resilience. Public administration, agencies and authorities must take on a pioneering role in digitalisation. Of central importance here are the supplementation of existing services with digital options and concepts and the digitalisation of entire administrative acts. Digital solutions also enable stronger and more extensive participation and involvement opportunities for citizens, so that not only the public administration, but also politics can benefit from new and open formats.



eco – Association of the Internet Industry

Capital Office

Französische Strasse 48

10117 Berlin, Germany

Tel: +49 30 20 21 56 7-0

Fax: +49 30 20 21 56 7-11

email: berlin@eco.de

international.eco.de

CEO & Managing Director: Harald A. Summa & Alexander Rabe

© 2021 eco – Association of the Internet Industry