tietoevry

Strategic Foresight on the EU's digital policies

How Data, Cloud and Responsible Artificial Intelligence will be regulated in the future

Table of contents

1 Executive summary

The value of data is well understood in the Nordic countries, with companies and public bodies looking to increasingly put their data in good use with the help of innovative technologies. In the meanwhile, the growing legal maze governing the use of data, cloud and artificial intelligence (AI) is often cited as a key obstacle for organisations looking to deploy innovative technologies. With new major EU-level regulatory initiatives under preparation, it is now more important than ever for organisations to proactively analyse and take into account the impact of upcoming legislation in their data, cloud and AI strategies.

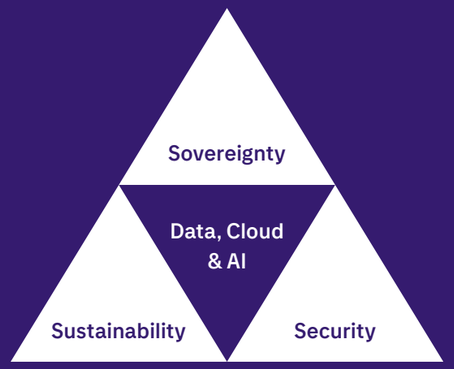
Based on Tietoevry's discussions with key European Union institutions, stakeholder organisations and Nordic decision makers, including security specialists, this Strategic Foresight will offer Nordic public and private organisations foresight into key upcoming EU level initiatives in the field of data, cloud and AI from the perspective of new regulations under domains of sovereignty, security and sustainability.

After the landmark Schrems II ruling in 2020 and the looming risk of foreign authorities' access to critical data, Nordic organisations have experienced a degree of uncertainty around transfers of personal data. The EU Commission is currently looking to relieve these uncertainties with a new data pact between the EU and the US (Data Privacy Framework). At the same time, the EU is preparing initiatives to enhance Europe's digital sovereignty, most notably, through security labelling of cloud services and new risk-based rules on AI products and services. Organisations can adapt to the changes proactively by exploring multi-cloud solutions for different types of data and assessing the ethical and security risks associated with the use of AI.

Security landscape in Europe has changed dramatically after the Russian invasion of Ukraine in February 2022, accelerating the development of new regulation on cybersecurity and critical infrastructures. While security needs are urgent, new legislation takes years to prepare and finalise. It is therefore no longer sufficient for organisations to merely react to new legislation; they should proactively consider their role and responsibilities in the security landscape, preparing for new laws in the making, such as the Cyber Solidarity Act (CSA) and the Critical Entities Resilience Directive (CER).

Sustainability considerations are increasingly impacting the use of data and AI in Nordic organisations as well as their choice of cloud service providers. Currently, the industry and self-regulation are in the driver's seat when it comes to sustainability standards applied to digitalisation and data centres. However, the EU is ramping up its efforts to increase sustainability of these sectors through regulation. The most notable development – the EU Sustainable Finance Taxonomy – divides economic activities into green and non-green categories based on technical criteria laid down in legislation, requiring companies to disclose the percentage of their business that meets these criteria. The Taxonomy framework will be implemented in segments, with parts of it already applicable and reporting requirements gradually growing. Organisations should proactively invest in the collection and analysis of their non-financial data, thereby preparing for the tightening regulation seizing the opportunity to utilise sustainability data for business growth.

Strategic Foresight on the EU's digital policies



Data, Cloud & AI in three domains

Sovereignty

How will drivers on digital sovereignty impact the interconnection of data, cloud & AI for the Nordics

Security

How will the changing cybersecurity landscape impact choices of data, cloud & AI-technologies and human behaviour

Sustainability

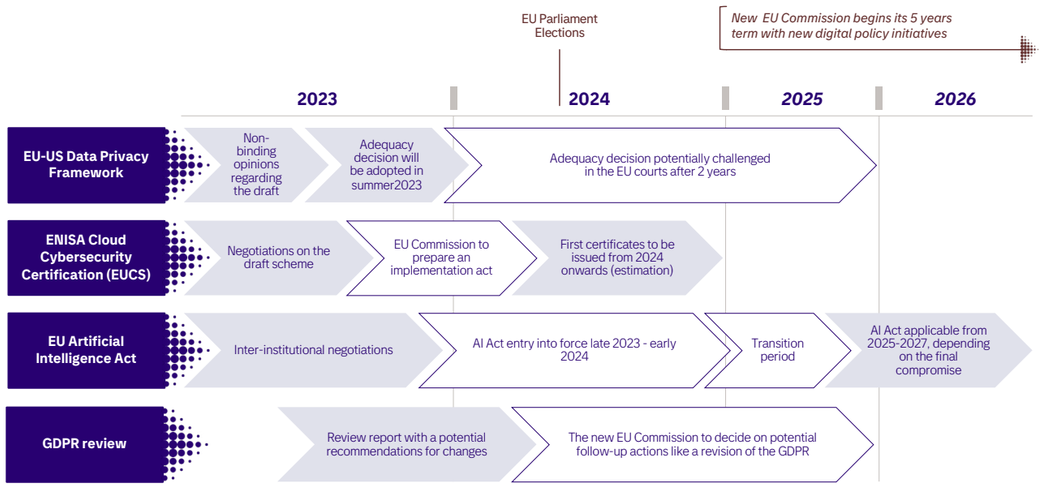
How will sustainable choices of data, cloud & AI-technologies enable innovation and growth

2 Digital sovereignty at the centre of the EU's digital policies

While the global digital race accelerates, the Commission of Ursula von der Leyen is seeking to enhance European digital sovereignty objectives by strenghtening Europe's ownership of its own data and digital capacities, while encouraging and facilitating innovation in Europe. The Commission's work in the digital field from data and cloud services to regulating artificial intelligence (AI) is thus characterised by these sovereignty objectives. As of now, no new initiatives are expected from the von der Leyen Commission, whose 5-years term is soon coming to its end as the next European Parliament elections will take place in 2024. While the Commission has launched a vast amount of digital policy initiatives during the past years, the continuously changing policy environment has proven to be particularly challenging for the users of data and cloud services to navigate. Recently, the sovereignty issues have culminated in legal uncertainty around the transatlantic data flows as well as cloud transformation under the European privacy and data protection rules. Understanding the policy landscape and potential future trajectories is thus essential to anyone working with these topics. The following chapters seek to explain these questions more in detail, by examining the EU's digital sovereignty objectives through the lens of data transfers, cloud services and responsible AI.

2.1 Continuing challenges for transatlantic data flows

Estimated timeline for key digital sovereignty related regulatory initiatives



International data flows play a central role in the daily work of organisations operating in the digitalising world. A growing number of companies and organisations are transferring data across the borders, while navigating in the changing regulatory environment. After the Schrems II decision, the transatlantic data transfers have however fallen into legal uncertainty. As a response, the EU has started to prepare a new Data Privacy Framework with the US. The Commission will now have to adopt the adequacy decision for transatlantic data flows, and according to EU Justice Commissioner Didier Reynders, the process should be completed before July[1] 20231. According to media sources, as of April 2023, the ratification process can however expand until September as the US has taken governmental surveillance practices in the EU under evaluation before opening the redress mechanism for the EU citizens. The redress mechanism is a key part of the EU's aim to respond to the shortcomings of the previously invalidated arrangement along with enhanced safeguards which limit governmental surveillance activities to necessity and proportionality. While the Commission representatives have been optimistic about the success of the framework, both the European Data protection Board and representatives in the European Parliament have already expressed their concern over its legal scrutiny. Therefore, it seems already inevitable that the Data Privacy Framework will be challenged in the EU courts in the near future. For those looking for legal certainty in transatlantic data transfers, the upcoming framework will thus likely offer only a temporary relief as the court decision can be expected to be pending some years before the final decision. The opposing privacy laws and the lack of interopera-bility are some of the main challenges to find a common ground in cross border data flows, as the case of EU-US data flow arrangements demonstrate.

[1] This assessment was made in December 2022.

While the Commission representatives have been optimistic about the success of the framework, both the European Data protection Board and representatives in the European Parliament have already expressed their concern over its legal scrutiny. Therefore, it seems already inevitable that the Data Privacy Framework will be challenged in the EU courts in the near future. For those looking for legal certainty in transatlantic data transfers, the upcoming framework will thus likely offer only a temporary relief as the court decision can be expected to be pending some years before the final decision. The opposing privacy laws and the lack of interopera-bility are some of the main challenges to find a common ground in cross border data flows, as the case of EU-US data flow arrangements demonstrate.

2.2 Sovereignty as a part of new EU cloud security labelling

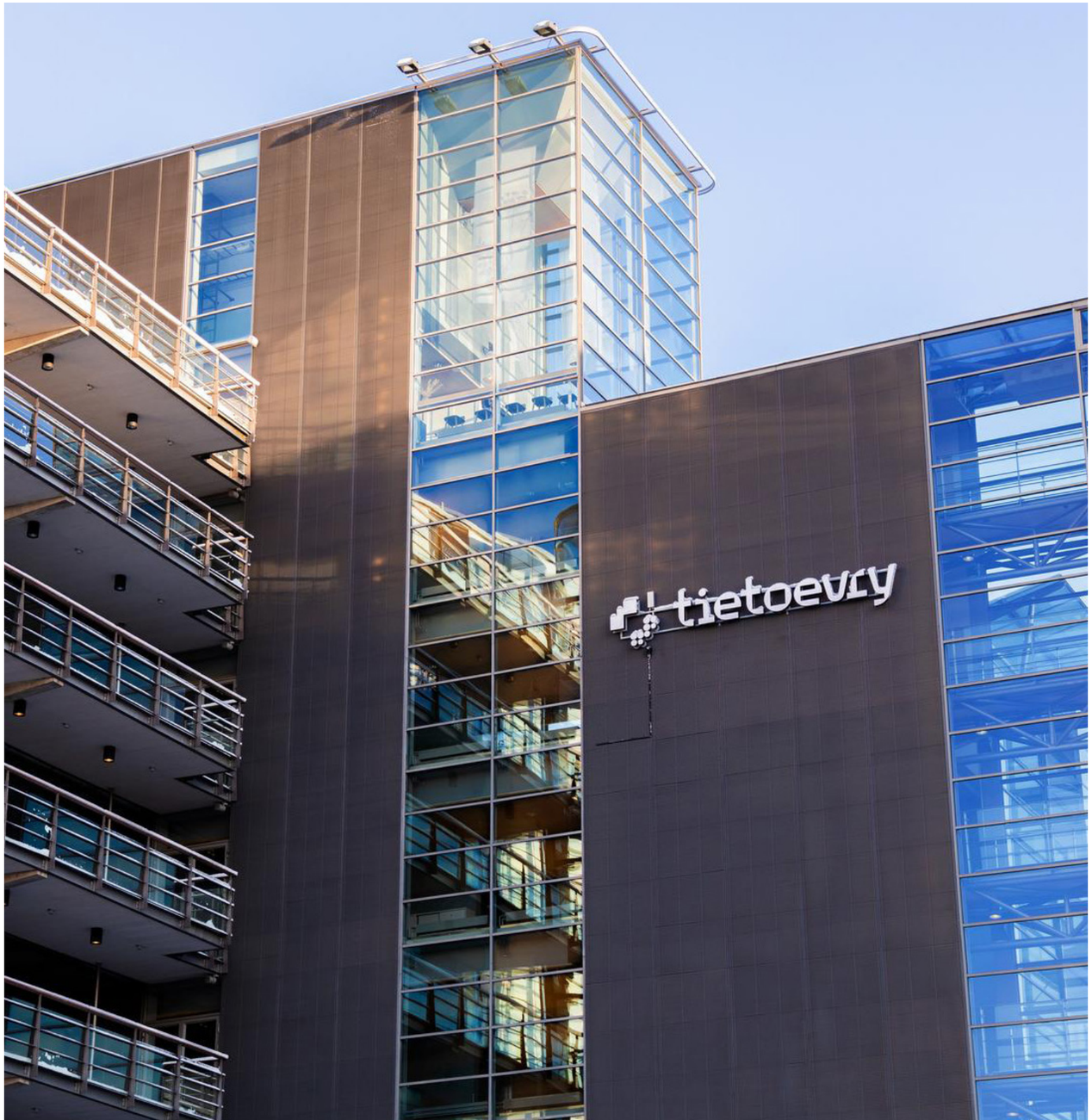
The EU Cybersecurity Certification Scheme for Cloud Services (EUCS) prepared by European Union Agency for Cybersecurity (ENISA) will be one of the most important policy initiatives for the users of cloud services in Europe, as its main objective is to provide harmonised cyber security standards for the European cloud market. The regulative process has however been proven to be slow as the draft scheme is still in the legislative pipeline due to long negotiations. Thus, the EU's ability to efficiently regulate the cloud sector has been questioned by the industry, which has expressed strong scepticism for the overall success of the draft scheme. This has fuelled the creation of self-regulative initiatives, as the industry is increasingly participating in the cloud regulation. As a result, industry-led initiatives such as the GAIA-X are partially overlapping with the EUCS regarding sovereignty, by seeking to provide commonly agreed standards for sovereign cloud. However, according to many key industry stakeholders, these initiatives are yet to reach their full potential. The cloud service users should thus prepare for continuing uncertainty around sovereign cloud standardisation, as the field seems to get more fragmented with competing regulative frameworks.

In the current draft scheme, the highest level cybersecurity certification is reserved for cloud service providers who comply with strict sovereignty requirements. Notably, the providers would need to be in European-based ownership and control, which has sparked debate in the industry. As per the EU Cybersecurity Act, cloud services can be certified at different assurance levels, including basic, substantial and high. While the EUCS draft scheme is currently based on a voluntary nature, individual member states could implement the scheme by requiring the critical sectors handling the most sensitive data to fulfil the highest cyber security standards. This would further fragment the regulative landscape of cloud services.

Major organisations in the finance sector have already expressed some serious concerns regarding the sovereignty requirements, as a total ban of using any cloud services from non-European actors would cause serious harm to their business. Based on the discussions, the inability of non-European cloud service providers to fulfil the sovereignty requirements would result in two scenarios – either the organisations will have to rely stronger on sovereign cloud services for storing and processing the most sensitive data or pause the ongoing cloud transformation completely. The former seems to be a more likely scenario, as sovereign cloud offers a reasonable solution for the current sovereignty issues with the non-European cloud service providers.

While the European sovereignty objectives have sometimes been accused of being protectionist by limiting the market access of non-European companies, the current turmoil in the geopolitical environment has partly challenged this approach. The Russian invasion to Ukraine has raised security issues at the centre of policy discussions. This might make the EU more hesitant to restrict the American cloud service providers from accessing the EU market, which could result in further delays in the EUCS negotiations. This is because partnerships with like-minded democracies appear to be even more important as concerns of cyber-attacks against the member states are rising. It is however worth noticing that the EU's values have been globally challenged, which may increase uncertainty in international partnerships.

Meanwhile, regional actors have been able to make quicker decisions. In 2022, the City of Stockholm decided to opt out from the use of American Microsoft 365 cloud services due to concerns over data protection violations. While considered ground-breaking, stakeholders in our discussions were doubtful whether these kinds of decisions would be seen on a broader national level. Instead, they found that a European-wide sovereign cloud could provide a potential solution for the current sovereignty issues, given that the legal uncertainty with the US continues. The time has passed when data was safe and in exclusive possession of the same sovereign country. Currently, bi- or multilateral agreements that consider holding and keeping critical data from other member states protected are widely supported. Ukraine shows an illustrative example of this: the national data was rapidly transferred outside of Ukraine's boarders when Russia began its attack on the Ukrainian territory.



2.3 The EU pursuing global leadership in AI regulation

The EU's stated goal is to enhance its digital sovereignty in the field of artificial intelligence through setting global standards of regulation. Its key initiative – the EU Artificial Intelligence Act – aims to achieve this goal through a risk-based classification and regulation of AI systems. While the EU Commission is looking to become the global leader in AI regulation, European industry stakeholders are worried about heavy regulation inhibiting Europe's chances of success in the constantly accelerating global technology race. Non-EU country stakeholders are understandably worried about restricted access to the European markets, if the cost of compliance becomes too big of a burden. A general worry by all stakeholders is that the EU's Ordinary Legislative Procedure is such a lengthy process that it could struggle to keep up with rapidly developing technologies. With the AI Act was first announced in 2018 and legislative proposal published in February 2020, the negotiations are now at the final phase and the law is expected to entry into force in 2024-2025. Considering this seven-year span from preparation to entry into force, and the current last minute attempt to address the latest major innovation that has made global waves – namely, large language models – worries about the rigidity and slow pace of the legislative process seem perfectly reasonable.

The question as to whether or not general-purpose AI should be labelled high-risk in the AI Act is a current hot debate in the EU institutions, sparked by OpenAI's release of ChatGPT in December 2022 during the final hours of the EU's AI Act legislative process. The European Parliament, along with multiple EU Member States, including France, are leaning towards more restrictive approach. The question of imposing restrictions on general-purpose AI is at the center of worries of industry stakeholders and could indeed have major implications for the development and use of AI in Europe in the near future. Large language models, such as ChatGPT, would be at the heart of the proposed high-risk classification of general-purpose AI. This means that OpenAI would have to disclose, e.g., any copyrighted material included in the training data of its models, which they have so far been reluctant to do.

Near future will show whether or not the EU manages to achieve global leadership in the regulation of ethical AI, with other countries following its suit, or whether it only manages to regulate itself out of the global technology race. At the moment, both seem realistic possibilities, especially given that the question of regulating general-purpose AI is still under discussion.

2.4 Conclusions and key findings

Recommendations and action points

Organisations should prepare for data transfer uncertainty and conduct regular risk assessments. The upcoming EUUS Privacy Framework can be reliably trusted upon only for a 2-3 years' time, pending an EU-level court decision.

Organisations should consider sovereign cloud for the processing and storage of the most sensitive data to ensure security and compliance with upcoming regulation (such as the EUCS sovereignty requirements).

Organisations should prepare for an increasingly complicated regulatory framework (e.g., the AI Act and the Data Act to co-exist with the GDPR). With increasingly diverse national implementations of data and cloud policies, organisations are recommended to conduct country level compliance strategies.

Organisations planning to utilise AI based applications should implement responsible AI to ensure legality and ethical standards in the development and usage of AI. They should conduct regular impact assessments, as large uncertainties loom with the scope of the upcoming EU AI regulation.

While the EU is pushing forward its sovereignty objectives, the future regulatory landscape is likely to be more fragmented due to the overlapping industry-lead initiatives and decisions made on regional or national level. This demonstrates both the dissatisfaction with the EU's ability to provide fair and timely regulation for the data and cloud markets, and the industry's willingness to step up and define the direction of the future regulation. Furthermore, the security concerns caused by the geopolitical situation and continuing legal challenges between the EU and the US suggest that the data and cloud service users should prepare for prolonged policy negotiations and general uncertainty in the EU decision making processes. In the current circumstances, there seems to be more demand for sovereign cloud solutions due to their ability to respond to the EUCS cybersecurity requirements. However, the EU's sovereignty ambitions seem to cover digital policies more broadly. This is demonstrated by the AI Act which aims to become a pioneering benchmark for AI regulation at the global level. While no new digital policy initiatives are expected from von der Leyen's Commission, the AI act indicates that the EU lawmakers are willing to extend the Union's regulative power further in the digital sector, resulting in heavier regulation in the future.

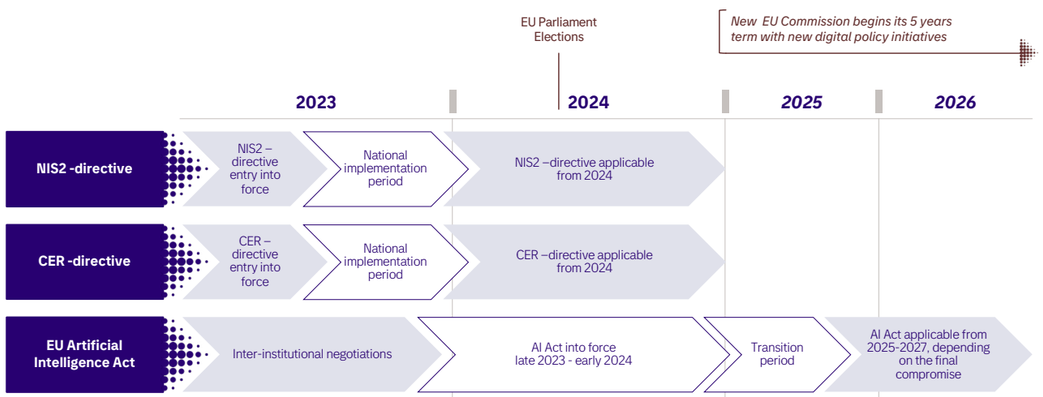
3 Changing security landscape in Europe

Unlike in the public discourse, in reality, the escalation of armed conflict in Ukraine did not start a new era that changed geopolitical security. Hybrid threats, Russian military actions continued the same strategy Russia has been executing since the occupation of Crimea in 2014. The presence of war in Europe has triggered the continent's countries to strengthen their defenses for possible armed conflicts in the region.

Increasingly, people are living their lives online, therefore digital services are at the core of security. Data, cloud, and AI are used to cover and protect critical infrastructure, and for gathering crucial information. Alternatively, they can be used as weapons. As a matter of fact, cyber and hybrid inferences have become rather frequent. This has further blurred the line between acts of aggression that should be reacted to and ones that are to be ignored. It is important to note, digital development cannot only rest on reactivity solely. To efficiently limit damage and save time, development should continuously take place.

3.1 Ensuring the security of critical infrastructure in a growing and complex digital environment

Estimated timeline for key security related regulatory initiatives



World's critical infrastructure needs to be more comprehensive to address the increasing complexity of societies. The private sector is a major producer of critical services that are identified to be the most important services for a functional society. Companies should analyse whether they will be included in the critical infrastructure in the following years. Potential sectors include for example energy providers, transportation, financial institutions and healthcare. As the number of services included in critical infrastructure grows, also the attack surface gets larger. Potential attackers are aware of fragile spots in systems, meaning that the providers need to secure the infrastructure accurately and avoid any security holes in them. The most vulnerable spots are in places where two providers meet. Ambiguities in these mentioned spots, which can, for example, result from overlaps between services, and leave the system exposed to attacks. The specialty of hybrid attacks is that their targets are usually unpredictable and everchanging. Hence, the companies working in the field have to have access to enough resources for setting up security measures that address these kinds of threats.

The Critical Infrastructure Directive (CER) is a significant step towards strengthening the resilience of critical infrastructure by introducing new obligations on entities providing essential services and extending to more sectors in comparison to its predecessor. Companies that provide essential services need to comply with the new obligations set forth in the directive. Furthermore, the Network and Information Security (NIS2) Directive aims to enhance the cybersecurity and resilience of critical infrastructure in the region. It outlines two distinct categories of services: essential and important, each of them with a specific set of requirements to be implemented and reported. Hence, the EU member states are required to have a national framework in place for implementing the NIS2 Directive and in case of a need, helping other member states inside the EU. Therefore, companies should be aware of any additional regulations and requirements that may apply at a national level.
By taking proactive steps to comply with the NIS2 Directive and other relevant regulations, companies can help protect their business from cyber threats.

3.2 Navigating global digitalisation: Challenges and opportunities for Europe

Digitalisation creates new instruments faster than institutions can set directives and frames. Furthermore, institutions produce their own legislations, which are not compatible with their counterparts' ones. The European Union and the United States have separated frame lines for future data and information policies. The divergence of regulations sets forth both possibilities and risks for collaboration. The EU is relying on its relationship with the US when it comes to digital services. However, this relationship should not be fully dependent since the agenda of the US may shift for example towards the Asian market or even become even protectionist. In November 2024, the US has a presidential election that might have an impact on its global interests. Thus, the Union should consider taking a more autonomous role. The EU should consider investing in innovation and bringing services to the market which can compete in quality with both American and Asian products. European providers must strive for a pioneer position in global markets.

Global politics move faster than ever before, and global relations are more complex than in decades. To comprehensively understand and capture these global trends must companies have their own political strategy specialists who can persevere hidden agendas and interests of other global actors. With the help of these specialists, the companies may predict the evolving market and political environment. European countries should not take for granted that European values are globally considered desirable. The global course of development has meant that the core values of the EU are challenged around the world.

Another key player on the global field is China. As the EU Member States are highly dependent on Chinese services and resources, the Union as a whole has to come up with a unified position to China. The lack of a clear strategy has made it easy for China to take advantage of this incoherence. Which has enabled the realisation of partnerships that benefit the Asian state disproportionately. The most vulnerable are partnerships in business as they share crucial information to the other party. To establish what these policies and partnerships should entail, the EU and European companies need to understand the agendas and interests of China in depth.

3.3 Conclusions and key findings

Recommendations and action points

Organisations should assess whether they are likely to be included in the scope of the growing body of regulation aimed at critical infrastructure (e.g., the upcoming CER directive). With the rapid pace of change, those who fail pro-actively plan ahead compliance will risk facing sanctions.

To comprehensively understand the rapidly changing trends of global politics, companies should deploy specialists in hybrid threats and experts in societal changes.

Organisations in critical sector should pro-actively engage in dialogue with both the EU level and national decision makers in order to clarify their role in the changing security landscape and ensure security in collaboration with the public sector.

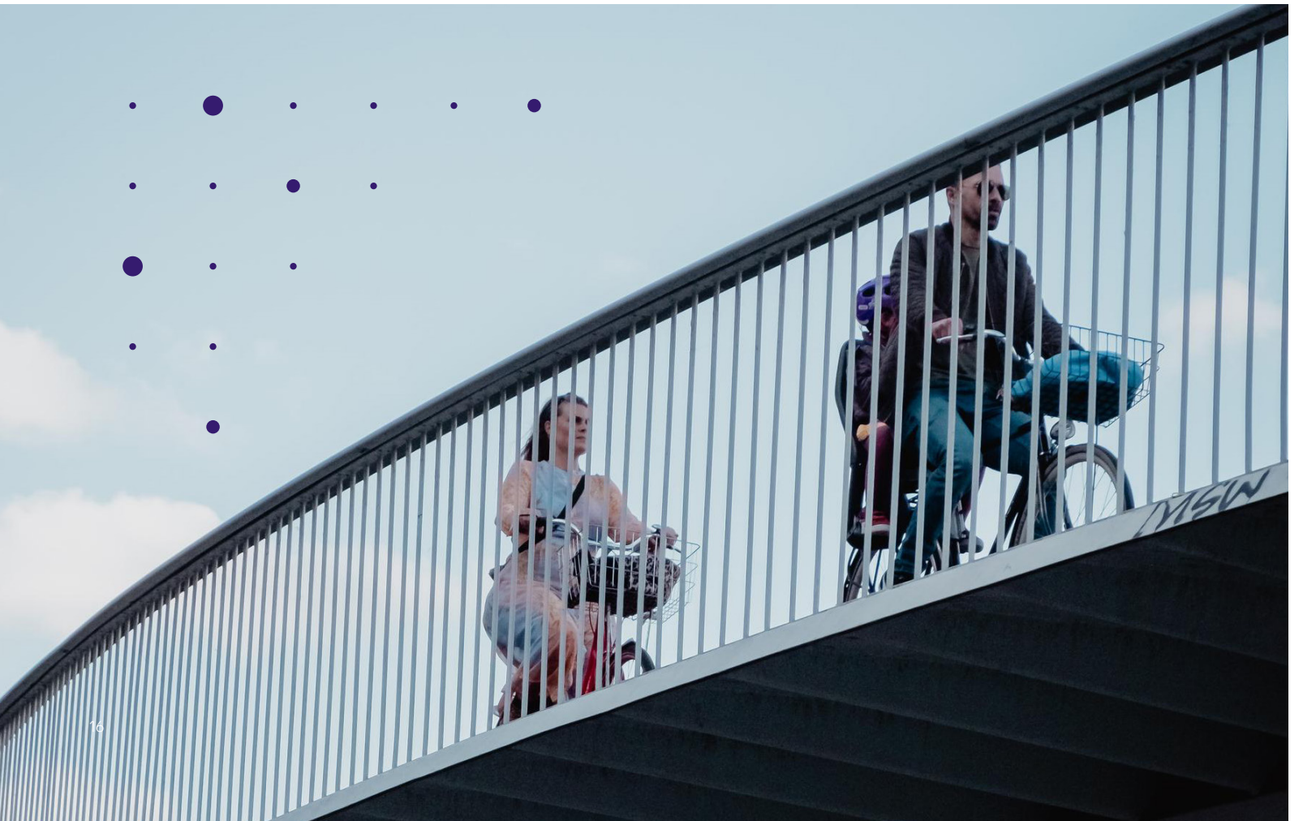
The private sector is more agile than EU regulations to respond to rapid changes in the geopolitical environment, and therefore companies should be confident of participating pro-actively in the security field and take a leading role there.

Geopolitics and security acts have to be included in every single companies' strategic plans. The war in Ukraine has made security topics visible, particularly in the Western world. The high tension in the security dialog should lead to concrete actions and results. Moreover, the critical infrastructure will keep expanding and companies need to be prepared for this expansion. This means, for instance, that private sector authorities are to follow the progression of the security acts closely. The influencing window is currently open for many new legislations in preparation on the field.

4 The sustainability challenges of data, cloud and AI

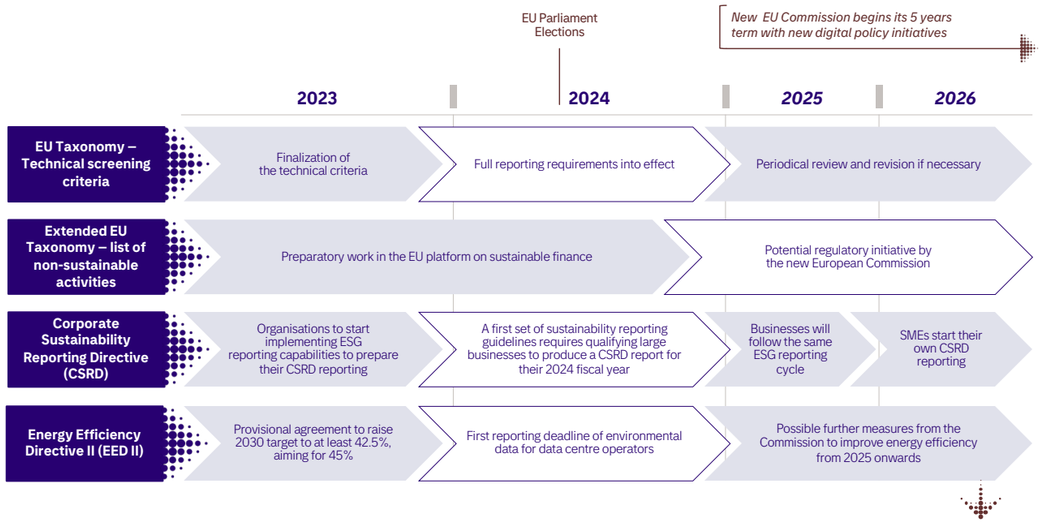
As data, AI and cloud computing continue to revolutionise the way organisations manage their IT infrastructure, sustainability issues related to these sectors become more prominent. Little attention has been paid by the regulators to the sustainability of data and cloud services in recent years, despite the growing need. However, a clear change of direction can be seen from the EU, as the regulatory needs of sustainable cloud infrastructure are currently being examined. Organisations should prepare for changes in the regulatory environment and prioritise the sustainability of data services as an important segment of their operations.

The EU's current regulatory pressure focuses on data centres and their energy performance. This is partly due to the EU Commission's strong roots and expertise in the energy sector. As is well known, the EU generally takes a long time to adapt to change. However, the need for change has been identified, and implications show that sustainability regulation will spread more widely to the data sector. The EU Sustainable Finance Taxonomy is a prominent new regulatory framework, in which data-driven services and software are centrally included as their own category. The Taxonomy is a voluntary framework, but its importance is expected to grow significantly in the coming years.



4.1 The current fragmented, voluntary and industry-driven sustainability standards

Estimated timeline for key sustainability related regulatory initiatives



Although the EU has an interest in increasing sustainability in the field of data, cloud and AI through regulatory means, sustainable development in these sectors has been strongly shaped by industry initiatives, standards, and certifications as well as voluntary frameworks. The operational field is fragmented, and currently there is very little comprehensive regulation at the EU-level on the sustainability of data and cloud services. The industry has a strong interest in shaping regulatory frameworks that affect their sustainability due to the need for flexibility, agility, and cost-effectiveness in responding to rapidly changing technologies and market trends. This has led to the development of voluntary industry-driven standards.

4.2 EU taxonomy for sustainable activities & reporting of sustainability data

The EU Taxonomy for Sustainable Activities is a landmark piece of regulation that divides all economic activities into green and non-green categories based on sector-specific technical criteria. While in principle a voluntary framework, the importance of the Taxonomy framework derives from its usage by, e.g., financial institutions in determining which investments are considered sustainable. Data-driven services, data centers and cloud computing are includedin the EU Taxonomy classification and will therefore count as green business activities if they fulfil the set criteria.

The EU Taxonomy is implemented in small fragments, with parts of criteria and reporting obligations already applicable to large organisations. The importance of the Taxonomy Framework will increase in the future, as the full set of criteria becomes applicable, related reporting obligations gradually expand to smaller companies and the framework will be linked

to other policies, such as funding instruments and public procurement rules. The Taxonomy Framework will also be used as guidance in the upcoming EU-level sustainability regulations. For these reasons, organisations should already take steps to align their business with the Taxonomy criteria to as large extent as possible.

Automated processes for sustainability reporting will be increasingly important to companies in the near future, as the new Corporate Sustainability Reporting Directive will take over the current reporting regime and expand reporting requirements to cover smaller companies. Organisations that are obliged to report sustainability data don't currently report it as frequently as financial data, with the non-financial data being dispersed and hard to gather. Real-time sustainability reporting adds tremendous value as it helps with compliance in the future and at the same time allows companies to take advantage of, e.g., energy savings to drive growth and competitiveness. Adopting these practices prematurely can also offer companies the opportunity to act as pioneers in the change that is coming in the near future.

4.3 Tightening EU Energy Efficient Regulation

The EU Energy Efficiency Directive (EED II) is among the most important current files on sustainable data centers. The EED is a policy framework aimed at reducing energy consumption and improving energy efficiency in the European Union.

The EED affects cloud computing and data centers by promoting the adoption of energyefficient technologies and practices, increasing demand for energy-efficient cloud services and data centers, and improving the energy efficiency of products and equipment used in data centers. It requires member states to implement national energy efficiency targets and measures for data centers, including the use of energy-efficient technologies and the adoption of best practices.

The directive includes a proposal for a mandatory and public energy efficiency register for data centers in each member state. It aims to establish a registry in which EU Data centers are requested to register and provide information on a set of key parameters, which could be developed into a benchmarking tool to monitor energy and resource efficiency progress. This would include for example the reporting of energy consumption data, the proportion derived from renewable energy, water usage and the amount of waste energy reuse.

4.4 Sustainable artificial intelligence – challenges and opportunities

Artificial intelligence has the potential to contribute to sustainability in various ways, such as optimising resource consumption, reducing waste, and improving energy efficiency. However, the fast-growing energy intense technology also presents sustainability challenges, and it is highly possible that these challenges will be addressed in the future on the EU-level.

Although the sustainability of AI is not yet specifically regulated in the EU, the proposed Artificial Intelligence Act aims to address some sustainability challenges. The Artificial Intelligence Act seeks to ensure that AI is developed and used in a more sustainable and ethical manner. For example, the AI Act includes provisions on eco-design for AI systems, which would require AI systems to be designed and operated in a way that minimises their environmental impact. This includes provisions to reduce the energy consumption of AI systems, to promote circular economy principles, and to encourage the use of sustainable data centers for AI training and deployment.

New AI models require incredible amounts of computation. The question is, how far artificial intelligence can be developed before the energy consumption exceeds its limits. As the demand for AI grows exponentially, it is likely that there will be a push for additional legislation in the upcoming years, either on the EU-level or on the national level, as the AI Act does not cover the sustainability aspect of artificial intelligent in detail.

4.5 Conclusions and key findings

Recommendations and action points

As sustainability regulations continue to evolve, companies should plan for future changes by implementing scalable and flexible solutions to adapt to new regulations.

Organisations should strive for early compliance with the voluntary EU Sustainable Finance Taxonomy standards as preparation for the tightening sustainability regulation.

Organisations should take pro-active steps to assess their use of responsible AI from ethics and sustainability perspective. Thereby preparing themselves for the tightening regulation in the field and develop policies and user guidance for responsible AI.

As sustainability reporting requirements are increasing, companies should invest in real-time sustainability data collection. Companies have the opportunity to act as pioneers in the change towards a more sustainable future.

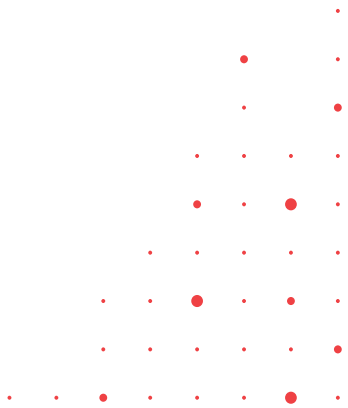
The ambitious sustainability policy cuts through every sector within the EU. What used to be industry-driven before, will become more and more regulated as sustainable digital regulations have started to gain their forms on both the EU and national level. The private sector offering digital services have the privilege to model their products to meet the set criteria. Most of the details in the regulations are still uncovered which holds a possibility for the businesses to still influence the outcome and final wording of the legislations to the desired direction. If companies are focusing on the goal of being sustainable and climate-neutral, the transition to more sustainable solutions can be achieved purely by market-driven actions. Being ahead of the green transition will benefit the whole private sector since the market will adjust the demand of sustainable services, and unnecessary regulations can be avoided.

About Tietoevry

Tietoevry creates purposeful technology that reinvents the world for good. We are a leading technology company with a strong Nordic heritage and global capabilities. Based on our core values of openness, trust and diversity, we work with our customers to develop digital futures where businesses, societies, and humanity thrive.

Our 24,000 experts globally specialize in cloud, data, and software, serving thousands of enterprise and public sector customers in more than 90 countries. Tietoevry's annual turnover is approximately EUR 3 billion and the company's shares are listed on the NASDAQ exchange in Helsinki and Stockholm, as well as on Oslo Børs.

www.tietoevry.com



Contact us:

Wenche Karlstad
Head of Digital Sovereignty Initiatives
Email : wenche.karlstad@tietoevry.com

Learn more about digital sovereignty:

www.tietoevry.com/digitalsovereignty