Republic of Estonia
Ministry of Economic Affairs
and Communications

Estonia's Digital Agenda 2030

Development agenda
of the field

2021

Table of contents

Overview of the agenda

Estonia's Digital Agenda 2030 includes a vision and an action plan concerning the development of the Estonian economy, state and society with the help of digital technology in the next decade.

With regard to digital society, there still persists an ambition to use information and communication technology, i.e. digital solutions as astutely and as much as possible in order to achieve the objectives of 'Estonia 2035'[1]. Namely, contributions are made via the following sub-objectives:

+ The Estonian economy is innovative and knowledge-based, using new technologies and business models as well as flexible forms of work. The contribution of the development plan lies in the creation of favourable conditions for business research and development and innovation. The Estonian economic environment invites people to work here, establish companies or do business virtually, invest, create and test new solutions which benefit the society at large.

+ The needs of all people are taken into account when shaping the living environment and the foundations of high-quality spaces and principles of inclusive design are consistently followed when making decisions in order to ensure the accessibility and convenience of spiritual, physical and digital space for everyone. The activities of the development plan contribute through the use of innovative technologies and environmentally friendly solutions which reduce the impact of climate change and the time required for covering distances and ensure a good living environment all across Estonia.

+ Estonia is an innovative country which values the creation and use of knowledge and where social life is organised by means of new human-centric and efficient technologies. The contribution of the development plan is reflected in the fact that the governance set-up promotes social cohesion, the adoption of new solutions, innovation and flexible governance. Public services function in the background and are proactive, and the data space is protected. The organisation of governance and people's participation in it in Estonia is trendsetting and sets an example to other countries.

According to the vision of the Digital Agenda 2030, Estonia should be full of digital power. This encompasses the following:

+ our way of life is impressive — it is easy to accomplish what we need or want;

+ we are protected by the power of digitalisation — our digital life is safe and we make bold advances in digital development;

+ our economy is empowered by digitalisation — digital solutions are the engine of the entire economy;

+ supported by the power of digitalisation, we value every person and contribute to co-creation;

+ fertile conditions have been established for the creation of future solutions in Estonia.

To implement the vision, more specific goals have been set in this development plan and lines of action have been planned in three areas:

+ the development of digital government, i.e. the use of digital solutions in the public sector, since no other development plan includes the general development of digital government and the public sector also leads and sets the direction for the development of the Estonian digital society. The main goal is to strive for the best experience when using public services, so that our way of life can be impressive, as has been highlighted in the vision. For this purpose, we plan to take the next leaps in the development of digital government and ensure the sustainability of the established solutions;

+ the development of electronic communication, i.e. connectivity, because the sufficient availability of connections forms the foundation of the use of digital solutions, be it in everyday life or business. The main goal is the availability of fast and affordable connections throughout Estonia.

+ the development of national cyber security, since we can boldly move forward on the journey of digital development formulated in the vision if sufficient trust has been guaranteed. This area includes the provision of cyber security in the public sector and more broadly in the economy. The main goal is to keep the Estonian cyberspace reliable and secure. Considering the growing risks and the established basis, it is a rather ambitious target on its own.

The implementation of the vision of digital society also depends on a number of other areas and policies covered by other development plans. Therefore, this development plan also **separately formulates expectations for other policy areas** because development plans should not overlap, but at the same time it is reasonable to partially address the measures of other areas.

The expectations constitute a 'request' stemming from the broader vision of digital society, so that we should clearly outline the needs and foundations, on the basis of which we can plan support activities for the implementation of other development plans or direct their alignment with one another. This development plan does not include specific targets or activities for promoting the introduction of ICT in various walks of life and business fields because all development plans of specific fields must encompass such plans.

When implementing the vision, **it is important to consistently follow the principles** highlighted in this development plan **with regard to all of the sub-objectives.**

The implementation and updating of this Agenda and its alignment with other development plans is guaranteed by means of the **organisation of management which has a steering group at its centre,** headed by the minister responsible for the development of digital society. An advisory committee including state authorities and other partners directs the accomplishment of the sub-objectives of this Agenda. In addition, the Cyber Security Council is active in the field of cyber security as a subgroup of a government committee. When it comes to implementation, various formats are used to organise cooperation, plan activities and carry out monitoring.

The development plan is implemented by means of a digital society programme which is prepared for four years and updated along with the budget strategy once a year. The programme includes specific measures, metrics, responsible agents and a budget, etc. which are required as an action plan for achieving the targets and aims of the Agenda in the coming years. Advisory committees of specific fields and, naturally, the steering group of this development plan update the programme and monitor its implementation.

A more specific analysis of the current situation and the justification for the selected lines of action are presented in the chapters of the main part of the development plan. However, we present the 'larger picture' of the current situation in the development of the Estonian digital society here — the main conclusions of the baseline analysis for the Agenda, including an international comparison, where possible.

Vision of Estonia's digital society 2030

Principles of implementing the vision

Digital government sub-objective

Connectivity sub-objective

Cyber security sub-objective

Expectations in connection with other development plans

Organisation of management

The authority generally responsible for the implementation of the programme and therefore also the development plan is the Ministry of Economic Affairs and Communications (MEAC) or in the case of specific activities its subsidiary bodies and/or other state authorities or participants.

The total cost, i.e. the overall funding needs of the development plan make up **around 1.2 billion euros over ten years.**

Current state of the development of digital society

A more specific analysis of the current situation and the justification for the selected lines of action are presented in the chapters of the main part of the development plan. However, we present the 'larger picture' of the current situation in the development of the Estonian digital society here — the main conclusions of the baseline analysis for the Agenda, including an international comparison, where possible.

The main characteristics and challenges of the Estonian digital society are currently the following:

1) Estonia has achieved a lot with regard to the development of digital government, but a great deal remains to be done: we have to reach a new level and maintain what we have already created.

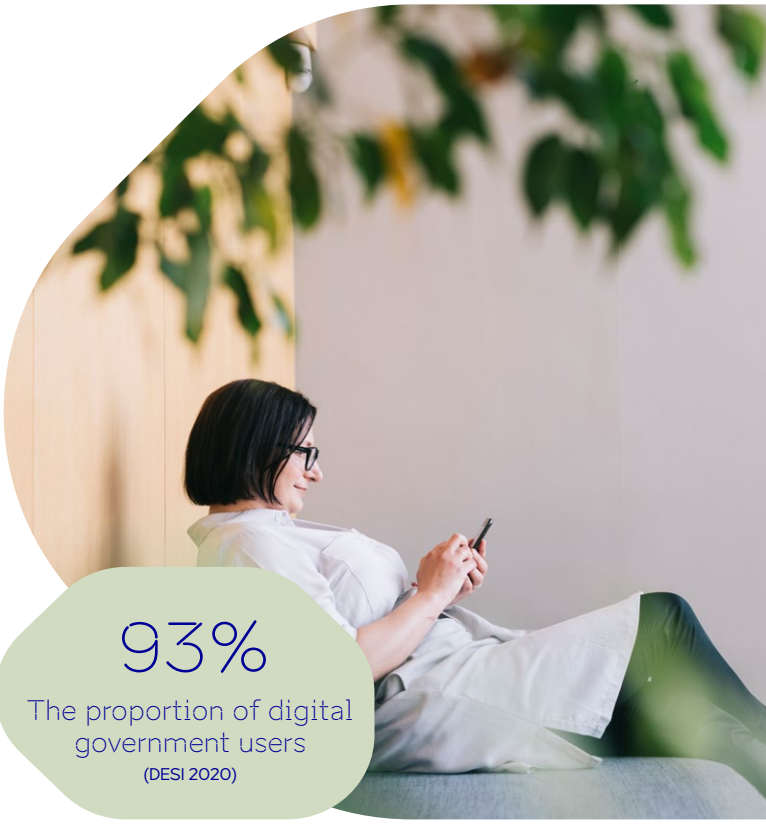
Estonia ranks among the first in many international comparisons (e.g. the DESI 20202 ranking of EU Member States or the eGovernment Benchmark 20203, the United Nations E-Government Survey 2024, etc.). What differentiates us is the fact that we have an actually functioning and widely used digital government.

Digital services and solutions are broadly used by back-office officials in public administration as well as private persons and entrepreneurs when dealing with state authorities. The proportion of the users of digital government services is among the largest in the EU (93%) (DESI 2020). Nearly all direct public services have been digitalised one way or another by now, i.e. they are now available via digital channels. The Estonian digital government has been established on a strong foundation, such as our national digital identity and the X-Road which has made the development of digital services in various fields safer, quicker and more affordable.

However, there are also concerns:

+ the ease of use of services does not meet the expectations of users, requirements or best practices — even if digital services are used, the processes are often cumbersome and the value they produce is therefore limited;

+ the sustainability of services, i.e. their constant renewal and maintenance at the required level has not been guaranteed when it comes to technology, procedures or resources;



+ the arrival of new larger updates in digital government has not been sufficiently known or has not been as fast and widespread as necessary;

+ cross-border services are underdeveloped, including at the level of the European Union, and there are still obstacles with regard to data exchange between countries and the establishment of common services.

However, it should be taken into consideration that states inevitably compete with one another when it comes to talents, export or investments. The quality of the business environment and services is an increasingly important factor which has been in favour of Estonia this far. If we fail to resolve the concerns of digital government, we will be left behind in the competition — many EU and other countries in the world have taken powerful steps to launch the digital transformation of their public sector in recent years, which has been propelled even further by the COVID-19 pandemic.

2) Estonia has a developed telecommunications market, but a fast Internet connection is far from being available to everyone and everywhere across the country.

The telecommunications market is highly competitive despite its small size. It is particularly noticeable with regard to mobile communications where the prices are among the lowest in Europe and the number of users

The number of mobile broadband users exceeds the average of the EU by one and a half times
(DESI 2020)

57%
of households have access to very high capacity networks
(DESI 2020)

is large (there are one and a half times more mobile broadband users than on average in the EU according to DESI 2020). Estonia was among the first to deploy 4G. The deployment of 5G has been somewhat delayed due to legal reasons but is starting up.

We are close to the average of the EU with regard to the general availability of high-speed Internet: 57% of households have access to very high capacity networks (DESI 2020), even though large investments have been made in the relevant backhaul network and more than 7000 km have been added with the support of the state in the last decade. There is a market failure outside larger urban areas: building a network is extremely expensive and often requires support from the state due to dispersed housing and a small population. Consumers themselves still use the possibilities of high-speed Internet very little.

14% of households
with a fixed broadband subscription of at least 100 Mbit/s
(DESI 2020)

14% of households have a fixed broadband subscription of at least 100 Mbit/s (DESI 2020). The demand and actual need for higher speeds is likely to increase in the future.

3) Estonia has skilfully ensured cyber security, but the risks are increasing and basic abilities must be considerably improved.

Digital services are actively used in the Estonian digital government and society owing to great trust in them and service providers. Among others, the secure structure of the Estonian digital government, the comprehensive approach to cyber security, the awareness of the significance of risk prevention and reduction and their gradual development have contributed to it.

However, there are significant gaps in the organisation of cyber security and the basic abilities if we take into account the fact that risks are increasing. Both cybercrime and geopolitical attacks in cyberspace are on the rise — technology is increasingly used to attain political interests. At the same time, we rely on the solutions of external technology creators and providers to a considerable extent. If we cannot foresee and manage risks, we are made vulnerable by the vulnerability of such providers. It is inevitable that we cannot do and check everything ourselves, which is why it is important to be able to choose reliable partners and solutions. Maintaining a high-level basic cyber-security capacity is unavoidable for Estonia, since otherwise we cannot continue to rely on digital solutions to the extent we have done so far. Estonia has a highly developed digital society which, unlike many other countries, is already vitally dependent on digital services and the infrastructure enabling them every day: network and information systems, hardware and software, the devices of ordinary users and other technology. Digital dependence also concerns the providers of vital services, a large part of whom consider their technological dependence critical. Furthermore, various information systems are interconnected, using data from one another. International cooperation is much-needed because incidents spread across state borders and hazards are growing in general in the world. Collective action in the field of cyber security has increased at the EU level, but we have a long journey ahead to secure an equally high level of digital safety across the entire EU.

4) The Estonian economy has not undergone a larger digital transformation yet, but we have a strong IT sector and community of technology-based start-ups.

The Estonian digital society has been marked by controversy for a long time: although we have a highly developed digital government, i.e. digital solutions are widely used in the public sector, the same has not taken place more broadly in the economy. At the EU level, the Estonian private sector ranks average or sometimes even below average in terms of its general digital development and the use of the opportunities of e-commerce (export) (DESI 2020). Nevertheless, there are signs that the situation is about to change. For example, the demand for the support measures of digital transformation has increased and the COVID-19 pandemic has led to significant advances in e-commerce.

Next to the traditional economy with a low level of digitalisation, there is a strong, internationally outstanding and thriving IT sector and community of start-ups in Estonia. The IT sector has been one of the drivers of economic growth in the last ten years and the field of start-ups has overtaken agriculture in terms of volume by now.

At the EU level, we are at the forefront when it comes to the digital skills of residents and the proportion of ICT specialistss
(DESI 2020)

5) The greatest obstacle to development is the lack of IT competences and specialists.

At the EU level, we are at the forefront when it comes to the digital skills of residents and the proportion of ICT specialists (DESI 2020). Nevertheless, there is a chronic lack of sufficient numbers of IT specialists, hindering digital transformation in the economy, the development of technology companies and the enhancement of digital government or cyber security. The more the entire economy and the world move along the digital road, the greater this shortage will be in the future. In short, we have more ideas and development opportunities than people and IT skills to use these opportunities and turn the ideas into services or products.

The basic digital knowledge of residents is sufficient for the Internet to be used widely. At the same time, there has been no significant increase in recent years: it has stabilised at 90% and international surveys (e.g. PIAAC) reveal that higher digital skills are an issue of concern. For instance, it hinders participation in the digital transformation at the workplace or the introduction of newer technologies in various sectors or may cause structural unemployment. The lack or incompatibility of digital skills is one of the largest obstacles for companies when making digital investments (DESI 2020).

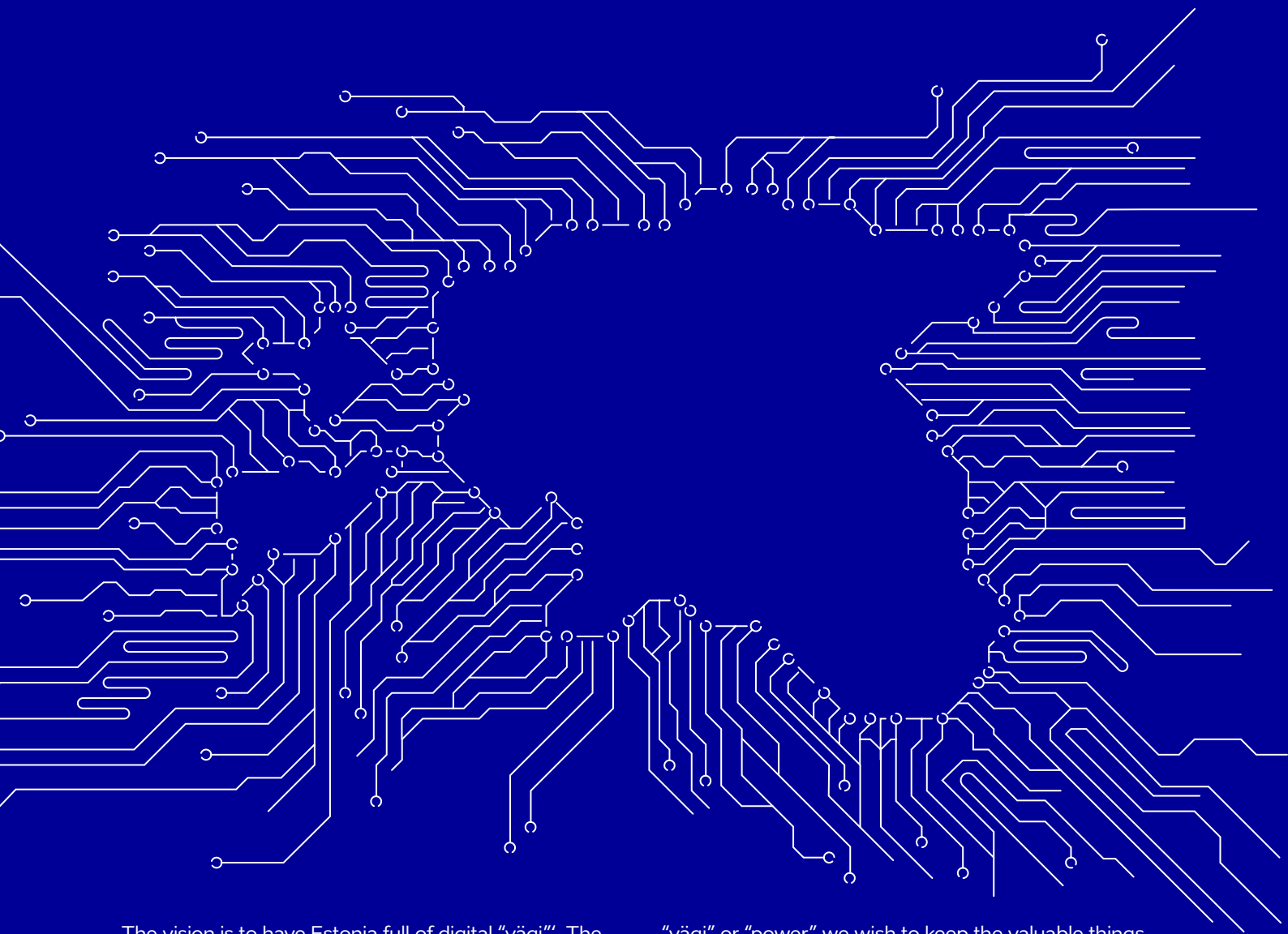
6) Technology continues to develop — it opens new opportunities, but also poses risks

There is an unbreakable megatrend in the world: the rise of digital technology continues. New solutions and technological opportunities are added more and more quickly and exponentially. On the one hand, it provides Estonia with the opportunity to continue making progress in its digital development, since new technology creates new areas of use or opportunities to recreate something that has been digitalised to make it even better.

There is an unbreakable megatrend in the world: the rise of digital technology continues.

At the same time, technological innovation is always accompanied by new cyberthreats. It should be noted that digital solutions become increasingly complex and specialised. Seeing, preventing and mitigating related risks thus requires more and more (special) competence. Complex risks caused by the rise of cloud computing, artificial intelligence, cryptography, quantum computers, the Internet of things, augmented reality and robotics, etc. can no longer be sufficiently resolved with the help of universal experts.

Vision:
Estonia, empowered by digitalisation



The vision is to have Estonia full of digital "vägi"'. The closest word to vägi in English is 'power'. *Vägi* is an evocative word with a long history as it is among the 300 oldest words in the Estonian language. In Estonian mythology, many things can have "vägi": trees, songs and words, even rocks. It's an invisible and somewhat magical power that the item or person possesses. And so it is an appropriate word to describe a digital society: aided by invisible and intangible power that gives us tools to be more. It is somewhat even magical and a power that needs to be carefully mastered. With digital "vägi" or "power" we wish to keep the valuable things we have established but believe that the Estonian digital society can be further improved. Estonia is already known as a strong digital society in the world, but we are capable of so much more.

We want Estonia to be full of digital power - competent and more powerful than anyone could otherwise expect for such a small country. Therefore, we can always make the best use of the possibilities of digital technology.

A digitally powerful Estonia is characterised by the following:

1. Our way of life powered by digitalisation — it is easy to accomplish what we need or want

+ Services function exactly according to my needs, and are available when I need them and in the manner I prefer.

+ Unnecessary procedures are a thing of the past both in the private and public sector, leaving me more time to carry out more valuable work or enjoy a more pleasant everyday life. The complexity of the functioning of the state is invisible for private persons and entrepreneurs.

+ I can access necessary services with a good connection everywhere and at any time, irrespective of whether I am in Tallinn, a remote village called Obinitsa or travelling around the world.

2. We are protected by the power of digitalisation — our digital life is safe and we make bold advances in digital development

+ My data are secure, but at the same time data can be easily used to create new smart solutions.

+ It is safe to use digital space; there is no need to fear misinformation, cyberbullying or cybercrime. I behave in a manner that does not involve digital risks; at the same time, I am unnoticeably provided with protection in the background.

+ The Estonian state and important services are always protected in cyberspace. It also gives our economy a competitive advantage.

3. Our economy is powerful thanks to digitalisation — digital solutions are the engine of the entire economy

+ The core companies of all sectors have completed the digital transformation in their operation or offer digital products and services. We have also made the economy environmentally friendly with the help of digital solutions.

+ Transactions are made, invoices are paid and reports are prepared completely digitally, automatically and in an instant — it saves us time and money.

+ People and companies from all over the world find it easy to do business in Estonia thanks to convenient procedures. Estonia has more active e-residents than permanent residents.

4. We empower people by valuing every person and their contribution to co-creation

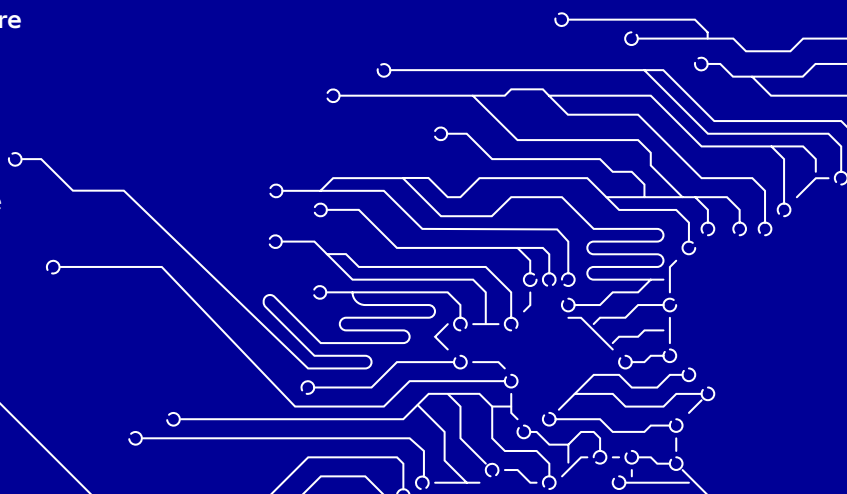
+ We are a technological nation: always and in all aspects ready to create new solutions and use them everywhere. We acquire new knowledge and skills eagerly and quickly throughout our lives.

+ Smart solutions make us even more connected and integrated, enable us to close gaps and support everyone in the required manner, where necessary. We contribute to the welfare of the state and the community; we are a society.

+ Estonian culture is easily accessible via digital channels throughout the world, preserved for the future and actively (re)used. The Estonian language is alive and developing in digital space.

5. Fertile foundation for the creation of future solutions in Estonia

+ There are excellent conditions for creating and testing innovative solutions in Estonia and taking them to the world — it is like a smart village of the world. People come here from other parts of the world to create solutions for the future; new producers emerge and existing ones continue to operate eagerly.



Principles

We adhere to the following principles when developing our digital society and planning and implementing activities within the framework of this development plan:

We protect and promote the fundamental rights of people. We ensure that everyone has an equal opportunity to participate in digital society and we maintain indispensable freedoms, starting with Internet freedom. We guarantee that people have the opportunity to manage the use of their personal data and protection of privacy.

We preserve the Estonian language and culture. We promote the viability of the Estonian language and culture in digital society and space. It is particularly important that everyday devices and services can be used in familiar Estonian.

We maintain our reliability. When launching initiatives and development activities, we immediately consider the related risks, and plan and carry out activities to reduce them — this way, we can make bold advances in the development of digital society. We prevent and resolve concerns in a transparent manner. We prefer to focus on prevention instead of dealing with consequences.

We are technology-neutral. In our initiatives and development activities we concentrate on results and choose the best technology to achieve them. If at all possible, we prefer open standards and solutions based on them. We establish common policy instruments (support, legal acts, etc.) which apply to all suitable solutions.

We build our digital society together. We join forces as early as possible to make the best decisions and find the most suitable solutions using our collective knowledge, resources and efforts. It may involve cooperation with domestic and foreign technology companies and universities, public sector institutions, various government levels and the third sector or other countries. We reuse good solutions and share our own.

We are innovative. When tackling challenges, we always consider whether and what we could do differently. Where possible, we test a new approach because it may yield more later on. We know that solutions are never complete; they can and must be constantly developed and designed to be flexible for this purpose.

We are climate and environmentally friendly. We do things digitally, promoting the conservation of the environment, contributing to the mitigation of climate change and helping to adapt to its impacts.

General objective and metrics

Based on the vision, the goal for the next decade in terms of the development of digital society is to increase Estonia's digital power: **digital government guarantees the best experience, high-speed Internet is available to all those who request it in Estonia and our cyberspace is safe and reliable.**

We measure the achievement of this objective on the basis of the development of four metrics as follows:

(satisfaction of private persons with public digital services + satisfaction of entrepreneurs with public digital services + availability of high-speed Internet + resilience and trustworthiness of cyberspace)/4 = X

Initial situation of the development plan:

(69% + 47% + 58% + 96%)/4 = 67,5

Objective for 2030:

(90% + 90% + 100% + 96%)/4 = 94

I sub-objective. Digital government[5]

Target based on the general objective: to ensure the best digital government experience by 2030.

This sub-objective is directly related to the implementation of one of the axes of the vision of digital society 2030: creating an impressive way of life in Estonia by means of digital solutions. While the previous aim set for the development of digital government was to primarily increase the efficiency of public administration, the quality and human-centricity of services is the next level of maturity in digital government. This does not mean that things should not or cannot still be done more efficiently — it must be done in addition to and while improving the quality of services.

In addition, the implementation of this objective contributes to the progress of other axes of the vision. Public services that provide the best experience and are of high quality help to make the economy more digitally powered because they simplify procedures for all entrepreneurs — among other things, it increases the number of e-residents. In order to ensure the best experience of digital government, steps have to be taken to establish favourable conditions for the creation of future solutions that improve our experience, as has been highlighted in the vision.

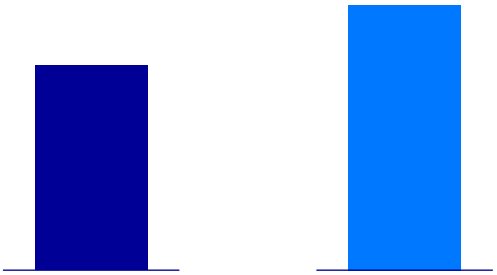
metric:

Satisfaction with public digital services[6]

Among private persons:

69%

90%



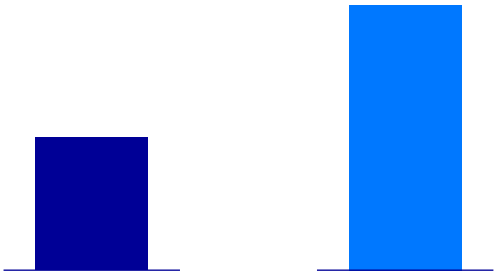
As of 2019

Objective for 2030

Among entrepreneurs:

47%

90%



As of 2019

Objective for 2030

This metric measures the satisfaction of private persons and companies with public services which have been used via electronic channels (electronic self-service, websites, e-mails, applications, social media).[7] The result is sent as an extract from the catalogue of public services[8] and it is measured once a year.

The lines of action required for achieving the sub-objective are divided in two because we are tackling two challenges at once: taking digital government to the next stage of development by means of new solutions and keeping the established solutions sustainable and updated.

1. Leaps in the development of digital government in Estonia

Promises: the greatest results by 2030 at the latest	Line of action
In Estonia, public services reach you just when you need them and you can complete all procedures at once.	Switch to life and business event based and proactive services
All procedures concerning the public sector can be carried out using chatbots in Estonia	AI-powered government
Another leap has been taken in increasing efficiency in the public sector by means of AI	AI-powered government
The fundamental rights of people are protected in digital government and people and companies have control over their data and the opportunity to actually share them	Human-centric digital government
Estonia is the greenest digital government in the world	Green digital government

2. Directions which enable us to take a leap in development and ensure the sustainability of digital government

Promises: the greatest results by 2030 at the latest	Line of action
All public services are human-centric and designed, managed and measured in a uniform manner	Introduction of the management and user-centricity of public services
All the decisions of the state are made on the basis of high-quality data	Data-driven governance and reuse of data
The common solutions[9] of digital government are futureproof	Future-proof digital government platforms
Digital government is cloud-native and standard services are of high quality	Centrally provided standard IT services
Estonia is a pathfinder and an eager experimenter	Systematic experimentation with new ways
The private sector makes a significant contribution to the innovation of digital government and solutions can be taken to the world	Open innovation
We have the knowledge, skills and funds required for bold and large-scale digital changes	Empowering digital change in public sector
There are more and more cross-border services.	Targeted international cooperation

Next leaps in the development of digital government

1. Switch to life and business event based and proactive services

Current situation:

+ For people, services do not seem to be or function as a seamless service, based on their life and business events (e.g. childbirth, marriage, founding a company). Instead, they are fragmented between state, local government and private services. Information concerning public services is available and services are offered in various channels and there is no common approach from the viewpoint of users. It is often difficult to understand where to find information about or how to use a certain service.

+ Public services are generally provided at the initiative of users and the same data are unnecessarily requested a number of times. At the same time, the state often has all the data required for offering a service, e.g. for the proactive provision of aid.

+ Although life and business event services[10] have been discussed as a goal for a number of years, we are still at the beginning of our journey when it comes to creating them. The situation is similar with proactive services[11] where only one proactive service based on offers (provision of family benefits) has been launched in addition to a few automated services (e.g. aid to retired people living alone).

Results:

+ In Estonia, public services reach you when you need them. Where possible, the state notifies people and entrepreneurs if they have the right to receive certain benefits or must fulfil an obligation. Proactive services are provided automatically or with the consent of a person, giving them the opportunity to withdraw from using the service or select the manner in which it is used.

+ Public services are provided to people and entrepreneurs as a single seamless service based on their life or business events; the complexity of the functioning of the state (e.g. cooperation between various authorities and levels) is invisible to the recipients of services.

+ When using public services, users are asked the same data only once, except if repeated data requests are reasonably justified.

Activities:

+ We develop an event service for every life event included **in the development plan of event services for private persons** and constantly update the development plan[12].

+ We support **the development of business event services for entrepreneurs,** including e-residents (i.e. improving the business environment according to the Estonian Research and Development, Innovation and Entrepreneurship Development Plan 2021-2035).

+ We initiate and carry out a **programme for developing proactive services** in order to make other services apart from those gathered under event services proactive.

2. AI-powered government[13]

Current situation:

+ Artificial intelligence has been adopted in the public sector on the basis of Estonia's national artificial intelligence strategy[14] and the first results have been achieved. As of the end of 2020, approximately 80 AI projects have been implemented or are ongoing. Nevertheless, competences related to artificial intelligence and data science are lacking, the level of implementation of Estonian language technology is still low and there are legal obstacles to the use of data (for example in connection with interpreting data protection requirements). Algorithmic trustworthiness has not been systematically guaranteed in the implementation of AI yet.

+ The possibilities to use AI are much wider than those that have been implemented so far — it requires changes in work processes and information systems. AI is a great opportunity for Estonia to take user experience and the functioning of the state to a new level of development, as has been reflected in the first experiences.

+ Public services, the environments where they are provided and the websites of institutions have been designed and developed based on a different kind of logic and style. Therefore, users find it confusing and difficult to navigate between various portals and environments. People expect simplicity and support from the state, but it is still too difficult to find information on where to turn to if you need to contact the state. Digital communication with the state requires a good level of digital literacy but it should not be like this. At the same time, the technology of virtual assistants and other AI applications to tackle problems like this is developing rapidly in the world.

Results:

+ Estonia is a leading user of AI solutions in the provision of public services in the world: our digital government is AI-powered. Another leap has been taken in increasing efficiency in the public sector by means of AI and other modern routine automation technologies, and the AI applications deployed are trustworthy[15].

+ All procedures concerning the public sector can be carried out using virtual assistants in Estonia. The major digital services of all administrative fields meant for people or entrepreneurs have been linked to the national ecosystem of virtual assistants called Bürokratt[16]. As such, users can access all public without special knowledge, using any common form of communication, channel or device.

Activities:

+ We implement and constantly update the national artificial intelligence strategy, i.e. our action plan in order to expand the use of AI applications (including robots) in the public sector and increase the relevant capability. Among other things, we engage in active cross-border and EU-level cooperation to share and reuse experiences and AI solutions.

+ We implement the concept of Bürokratt to make public services available via virtual assistants.

+ We develop the legal space to enable a more widespread and reliable use of AI applications (including guaranteeing the protection of fundamental rights). We also advocate this in AI-related policy and law-making at the European Union and international level.

3. Human-centric digital government[17]

Current situation:

+ Users usually have a high degree of confidence in the Estonian digital government but it is not guaranteed. The awareness of people and the general public of the functioning of digital solutions (including data processing) and the transparency of solutions has been low, which may reduce trust in the future and create a digital divide (a growth in the proportion of non-users and sceptics).

+ It is especially important to ensure transparency and reliability when implementing new technology with great potential which may have an adverse impact on the fundamental rights of people (e.g. AI, data analytics, etc.). Trust in digital government is dependent on whether fundamental rights are guaranteed but not enough attention has been paid to ensuring and promoting such rights when introducing digital solutions.

+ Estonia has stood out with the fact that people get an overview of who uses the data included in some important databases and how such data are used (e.g. health information in the Patient Portal). A Personal Data Usage Monitor has been created but is still in its early stages. The state does not provide a complete overview of when and how the data of private persons or companies are used. Users thus have an incomplete overview of who uses their data and when and how they are used.

+ Private persons have the opportunity of requesting access to and obtaining their data in order to provide access to other parties. However, it is not possible to give your consent to other parties, so that they can request data automatically. In addition, no profit can be made when allowing the use of your data, which could encourage the private sector to create new solutions. Therefore, it is difficult for the private sector to use the data of private persons and the collection of their data is duplicated, which slows down the development of the digital economy.

+ There is no functioning solution for managing and withdrawing given consents. Therefore, it is rather difficult or even impossible for private persons and entrepreneurs to find out whether and how their data are used for the purposes of decision-making (including decisions concerning them) or service provision.

Results:

+ The society's trust in the use of digital solutions in the provision of public services is maintained and grows. It is based on people's increased awareness of the connections between technology and fundamental rights, the reliability of technology and their role in service design as well as the transparency of the creation and use of digital solutions.

+ When developing and implementing digital solutions in the public sector, the fundamental rights of people, democracy and the rule of law are protected and the opportunities provided by technology are used to promote them.

+ When developing and offering public services, it is guaranteed that everyone has an equal opportunity to participate in digital society and use digital services.

+ Private persons and entrepreneurs are in control of their data and can actually share them in Estonia. They have an overview of the data collected by the state in connection with all services and the purposes of the use of their data.

+ Private persons and entrepreneurs can use digital solutions to decide who can use the data shared by them and determine the purposes and conditions of use (for a fee if they wish).

Activities:

+ We develop and implement **relevant risk management measures** to ensure the reliability and human-centricity of digital solutions, and manage the impacts on fundamental rights.

+ We raise **the awareness of people and the general public** of human-centric digital government and the reliability of technology.

+ We introduce the opportunity to obtain a **complete overview** of all of your data held by the state in the state portal.

+ We introduce a **consent service**[19] all across the state and expand it to include the data of entrepreneurs.

+ **We develop the Estonian legal space** to ensure the human-centricity of digital government and the reliability of digital solutions and promote the fast-paced introduction of new technologies for the benefit of the society.

+ We increase **the ability of the owners and creators of digital services** to develop and offer human-centric and reliable digital solutions.

+ We adopt a **Personal Data Usage Monitor**[18] all across the state and expand it to include the data of entrepreneurs.

+ **We shape EU and other international activities,** promoting the cross-border and global exchange of (personal) data between countries in a manner that provides people with more control over their data (e.g. within the framework of international treaties), and activities which help us advance and ensure the global development and use of human-centric and reliable technology.

4. Green digital government

Current situation:

+ No attention has been paid to the environmental compatibility of solutions and climate change when developing digital government in Estonia. The environmental footprint of the use of digital solutions is constantly increasing in Estonia and elsewhere in the world. The ICT sector together with data centres makes up an estimated 2% of global greenhouse gas (GHG) emissions which is comparable to the proportion of the aviation sector. If this tendency persists, the proportion of the ICT sector in GHG emissions may rise above 14% by 2040. The awareness of customers, users and developers of technology and their attempts to act in a more environmentally sound manner are lacking. + The exchange of information on paper has decreased and environmental monitoring has become more efficient thanks to digital solutions, but the environmental impact of the Estonian digital government (water, energy and resource consumption more widely, GHG emissions, impact on nature and waste generation) and ways of reducing it have not been analysed.

+ A green way of thinking is increasingly popular in the world (including the technology sector) and provides Estonia with the opportunity to become a pioneer as a green, environmentally friendly country with digital government. In terms of user experience, it is also more and more important whether services are provided in an environmentally sound manner.

Results:

+ Estonia has the greenest digital government in the world and sets an example to others.

+ This does not imply the greenwashing of current solutions, but rather the development and management of digital government are based on climate and environmental friendliness. Where possible, the option that is more climate and environmentally friendly is chosen when introducing a new solution and the environmental footprint of digital government is reduced.

Activities:

+ We initiate and implement the **climate and environmental friendliness and green IT[20] action plan.**

+ **We analyse** the environmental impact of the Estonian digital government and ways to reduce it.

Directions which enable us to take a leap in development and ensure the sustainability of digital government

1. Introduction of the management and user-centricity of public services

Current situation:

+ The fragmentation of the provision of public services and unnecessary bureaucracy show that public services either have not been designed or provided in a user-centric manner or the quality of the services of various institutions is uneven in relation to this. There is no common standard for services, focusing on users. The requirements concerning the design, development, management and measurement of services are fragmented or inadequate.

+ It is more difficult to access and use services if a person lacks skills, has special needs, comes from a foreign country or has a different cultural background;; there is also a greater risk that they miss important services.

+ Public services often do not have an owner or if an owner has been assigned, it is a mere formality and the services lack substantial management. Furthermore, most ministries have a coordinator of such services but service development is not systematically managed at the level of the area of government.

+ The quality of public services is measured by means of various methodologies and solutions which do not allow for comparisons. The quality of services is often measured manually or left unmeasured, since it is regarded as an additional obligation and expense, rather than something of value. A catalogue of public services has been created to measure and compare services but it has limited functionality and finds little use. Therefore, data are mostly updated in the catalogue only once a year during a special campaign. In addition, it does not include all services and institutions.

+ Due to all these reasons, there is no clear understanding of the quality of services within public sector institutions or all across the country. Decisions concerning the development of services are based more on subjective perceptions than actual (monitoring) data.

Results:

+ All public services are human-centric — designed and provided on the basis of users and their needs and preferences, while guaranteeing their fundamental rights. The needs of people with poorer digital skills or special needs as well as foreigners residing in Estonia and e-residents are taken into account.

+ The practices of service design, development and management are at a high level across the public sector. All public services are measured and monitored in a comparable way throughout the country. Decisions concerning service development are made on the basis of (monitoring) data.

+ Every public service has a substantive owner who is responsible for the day-to-day development and quality of the service, including measuring and monitoring it. In addition, the services are centrally developed and the portfolio is managed in every ministry.

+ The central catalogue of public services is easy to use and data are forwarded automatically.

Data of higher quality have enabled comparison of services and their quality across the country. Furthermore, abundant tools are available to the owners of services.

Activities:

+ We develop and introduce a common **standard for user-centric services** which includes the design, development, management and measurement of services.

+ We **introduce the practice of measuring services** and a common methodology in public sector institutions.

+ We create and provide service owners with **service management tools**; among others, we make the state-wide central catalogue of services easy to use.

+ We further develop the **role, knowledge and skills of service owners and coordinators** and service management in public sector institutions.

+ **We promote the removal of obstacles in the development of cross-border services on the EU internal market.** We invest in the cross-border availability of Estonian digital services and participate in relevant joint initiatives, especially in the framework of Nordic cooperation and within the EU.

+ **We invest in improving the user-centricity and accessibility of services,** including the development of digital services for e-residents as a special focus.

2. Data-driven governance and reuse of data

Current situation:

+ The possibilities of data analysis are far from being sufficiently used for decision-making in governance. Uneven data literacy among managers and specialists is one of the reasons behind it, i.e. the inability to see data as the source of answers. Another reason is the fact that even though a large amount of data has been collected in digital government over the years, their findability and quality are points of concern.

+ The overview of data collected by state authorities and local governments is insufficient. It is available in databases but even there the descriptions of data are uneven and the timeliness or meaning of data is frequently difficult to identify. The tools meant for managing data descriptions are not sufficiently implemented. This makes the reuse of data more difficult and is the reason why the 'once-only' principle has not been consistently implemented. The opportunities related to 'linked data' which would enable us to make advances in the development of service design and provision have not been used.

+ The quality and degree of development of data management, including responsibility, organisation and competences, are highly uneven among institutions. The content and quality of too little data can be determined. There are many procedural systems but the data are based on statements almost everywhere and it may happen that they are not trusted by other data users and are therefore insufficiently reused. The data life cycle has not been implemented; therefore, destruction deadlines are not observed systematically and inspected unnecessary data are not destroyed.

+ Legal and information security restrictions are applied to the cross-usage and reuse of data, particularly in connection with personal data. Technology itself should be implemented more to reuse these and other sensitive data to a greater extent but securely and privately: so-called privacy technology[21] solutions should be developed, tested and adopted. First steps have been taken in Estonia for this purpose, albeit slowly.

+ Many public sector institutions still exchange (digital) documents instead of machine-readable data and the primary focus is on structured data. This hinders the introduction of machine learning and modern data analytics.

+ There is an insufficient overview of the raw data of state decisions and analyses and of calculations, decreasing the transparency of the state. Changing this would help restrict the spread of misinformation.

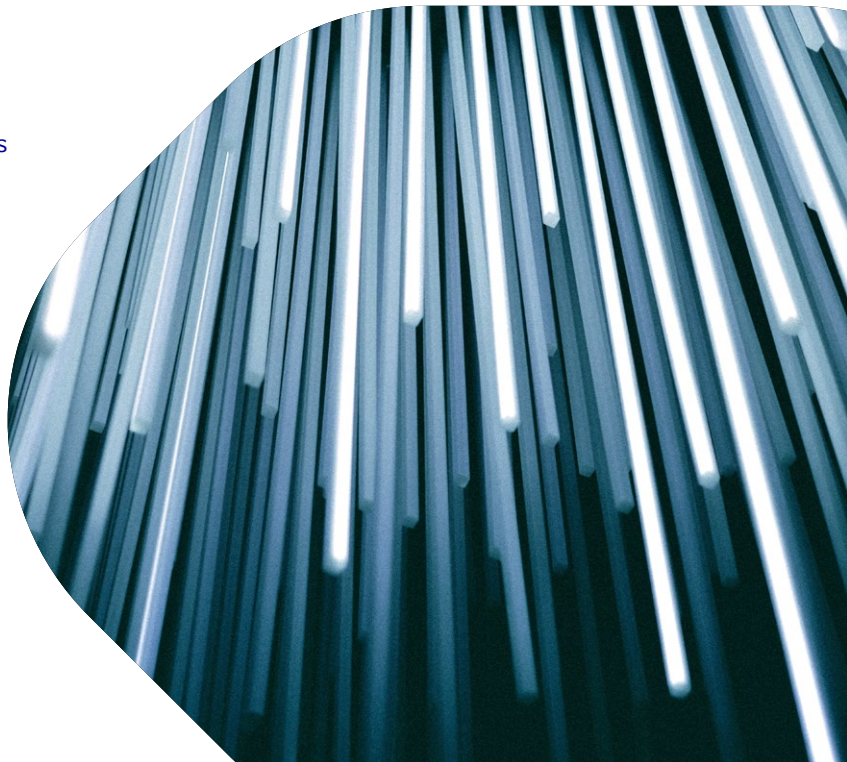
Results:

+ We make all the decisions of the state using high-quality data. The findability, quality and speed of use of data provide decision-makers with analytical support and make processes more efficient.

+ There is an updated and complete overview of data at the level of databases and datasets. Data can be linked to one another. The 'once-only' and data reuse principles[22] are applied.

+ The reuse of personal and sensitive data in service provision and decision-making increases significantly with the implementation of privacy technologies.

+ The public sector uses data in a transparent manner. The basic data of public sector decisions and analyses, and calculations are published as much as possible.



Activities:

+ We develop the **legal space for the purposes of data science and analytics,** including relevant instructions.

+ **We develop the competence of data science and analytics** and their use in the public sector.

+ We develop **the competence and organisation of data governance** and introduce best practices in all public sector institutions. We create and offer necessary tools, including for the adoption of linked data.

+ We develop an **interinstitutional data governance and data science competence centre** to gather and make available relevant know-how and offer support to institutions.

+ We develop further and expand the use of **the administrative system of the technical services and databases of the state information system,** which ensures an updated overview of data and the state information system.

+ **We support and, where necessary, initiate EU and international activities** promoting cross-border and global data sharing and reuse among states and sectors.

+ We develop and introduce a system of guaranteeing the **transparency of the source data of state decisions and analyses, and of calculations.**

+ We initiate and carry out a **national privacy technology implementation programme.**

68%

of Estonian residents would prefer it if all digital services were accessible in a single central state portal.

3. Future-proof digital government platforms

Current situation:

+ One of the foundations and success factors of the Estonian digital government has been development based on strong platforms, i.e. central infrastructure components and services. This has sped up the development and introduction of digital services throughout the country and society. Existing platforms must constantly be adapted to the development of technology and the needs of users, and developed further.

+ Digital identity is a good example here. Identity cards and Mobile-ID have withstood the test of time so far and are the safest eID carriers but users prefer simpler solutions. Their usability is also influenced by the development of user interfaces and devices, which makes it more difficult to rely on a separately issued physical medium or request special devices for users. Technology provides access to potential new options for authentication and signing, for instance by means of biometrics. eID is an important enabler of international business and cross-border services but its implementation at the EU level is still in early stages. The basic software of eID must be compatible with primary software and hardware platforms for our digital services to function but these solutions are constantly updated.

+ The X-Road[23] is a long-term mandatory data exchange layer of digital government. Making the X-Road compatible with the world of cloud computing and big data or establishing it as a cornerstone of AI-powered services is a challenge to be tackled when future-proofing the X-Road. At the same time, the X-Road is used more and more widely across the world. Estonia has joined forces and combined its resources with Finland to develop this core technology, establishing a relevant consortium called NIIS[24]. This makes it easier to find solutions.

+ 68% of Estonian residents would prefer it if all digital services were accessible in a single central state portal. However, the development of the state portal has been project-based and several attempts of relaunching it have been left unfinished. In a world based on search engines or Bürokratt, the state portal still has a place as a single back-up platform for the information and services of the state. In addition, the state portal does not meet the needs of entrepreneurs at the moment, so they do not have a single service channel. When looking towards the future, eesti.ee has been determined as a reference point for Estonia in developing the single European digital gateway, which creates a basic cross-border interoperability of digital services at the EU level.

+ Based on eesti.ee, an initial version of a state digital mailbox has been created but it currently functions as a voluntary address for forwarding e-mails. Solutions for a central delivery service are being developed.

+ In order to make digital government function better and more (cost-)efficiently, other common needs can be met by means of platform solutions or services but the creation and development of platforms has not been consciously managed. Platform services have not been provided at an evenly high and sustainable level.

Results:

+ The basic platforms of the Estonian digital government are future-proof: they are sustainable and change flexibly according to the changing needs of users and technological possibilities.

+ The Estonian national digital identity does not have a physical medium and it can be used in all common devices and environments, including all over Europe.

+ The X-Road is still better for domestic and international data exchange than its alternatives when it comes to quality and compatibility.

+ Eesti.ee is an updated service and information gateway for private persons and entrepreneurs, and also a single contact point in cross-border operations.

+ All notices and documents that need to be forwarded are delivered by default via the state mailbox and are always accessible to people.

+ The common needs of state authorities and sectors have been met by means of platforms and the management of platform services is at a high level.

Activities:

+ We develop the eesti.ee state portal further, including as a joint service channel for entrepreneurs and a single point of contact for the EU digital gateway.

+ We continue to develop the core software of the X-Road and promote its domestic use.

+ We support **the joint development and reuse of digital government platforms in the EU and Nordic countries**, especially for promoting cross-border data exchange. We ensure the compatibility of the Estonian digital government with the European interoperability framework and contribute to the further development of this framework.

+ We implement and update the **action plan concerning digital identity**. Based on this, we continue to develop the national digital identity, its carriers, basic software and applications in order to move towards a convenient and secure manner of identification without using tools.

+ We prepare, implement and constantly update a development plan for new platform services. We improve the quality of the management of platform services.

+ We develop a state mailbox and legalise it as the main channel for delivering notices and documents from the state instead of letters on paper.

+ **We contribute to** the legal space of **digital identity and digital signatures in the EU,** and the further development of interoperability and common solutions to increase cross-border usability.

4. Centrally provided basic IT services

Current situation:

+ The provision of a number of standardised IT services, such as computer workstations and server hosting services, has been organised separately in each area of government. The competences in the provision of these services and their quality are uneven and it is difficult to combine services, which hampers cooperation between authorities and the reorganisation of tasks in the course of state reform. The level, volume and capacity of outsourcing services to the private sector is uneven.

+ Standard IT services are too costly for the state in their current dispersed state. At the same time, the technological and financial sustainability of digital government is a more general point of concern, encouraging us to look for opportunities to increase efficiency. Servers, data centers, licenses and qualified staff are required for every new digital government service.

+ A large part of the core infrastructure of digital government is not state-of-the art; for example, modern cloud solutions and opportunities to link to the common infrastructure of the EU are underused. Cloud competency is poor in the public sector. Furthermore, the implementation of modern cloud services in information systems or the readiness to do that is lacking. The quality of public services is therefore also reduced (e.g. availability and accessibility at peak times).

+ A data embassy[25] pilot project has been implemented in digital government, ensuring the secure storage of data which are vital for the functioning of the state outside its territory. The functionality of the data embassy has been minimal so far and it does not function as an extension of quickly switchable public server infrastructure yet.

+ Access rights, roles and identity management are unevenly dispersed across administrative fields in digital government and are not compatible, hindering the use of services beyond single administrative fields. This also causes security risks because there is no overview of who has access to various systems and whether access rights change upon changes in the role of a person.

+ Although the provision of public communications services has been consolidated, it has been undermanaged and the quality of services has not met the expectations of users. The future directions for the development of public communications (the concept) have been determined and await implementation.

Results:

+ Standardised IT services are centrally provided. As a result, the quality of services related to computer workstations and server hosting, including the user experience of public sector employees, has improved (making joint work easier). In addition, the provision of these services is more (cost-)efficient and the introduction of modern technologies is quicker. Standard services are outsourced to the private sector to a greater extent.

+ Digital government is in the cloud: every new development is designed to be cloud-native and all older digital services have been transferred to cloud infrastructure, unless contradicting information security.

+ The data embassy functions as a complete service and can be used as a technical extension of critical digital services in the case of major interruptions.

+ Digital government infrastructure is compatible with EU and other international cross-border initiatives, e.g. the infrastructure for cloud and blockchain services.

+ Rights and roles have been determined in a uniform manner in digital government. Changes of user roles in decentralised systems are made uniformly and according to similar principles across the country.

+ Public communications services are guaranteed to users at a sufficient level (including availability, integrity, confidentiality, coverage, data speed and volume).

Activities:

+ **We consolidate the provision of computer workstation and server hosting services,** so that it is organised by a single competency centre across the public sector in order to ensure the best possible quality and cost-efficiency of the base layer of digital government services. In relation to that we introduce integrated administration of central roles and rights management.

+ **We launch a digital government marketplace**[26] in order to outsource standard services and software solutions to the private sector uniformly, more broadly and quickly.

+ We cooperate at the EU level and invest in the **interoperability of our digital government infrastructure with the common EU infrastructure.**

+ We adopt **cloud solutions** in the public sector as a whole, also combining public and private solutions according to needs and opportunities.

+ We implement and update the **data embassy action plan.**

+ We implement the **concept of developing public communications:** we build capacity with regard to managing public communications and improve the quality of services.

5. Systematic experimentation with new ways

Current situation:

+ Even though Estonia is esteemed as a digital country in the world, our attention and resources are largely directed to the management and development of existing digital services. As a result, the proportion of new approaches, technologies and experiments, i.e. disruptive innovation[27] in digital government has decreased.

+ There is no systematic development of new skills or mapping of technological development in the public sector. At the same time, the private and academic sectors offer knowledge and solutions which could be more broadly deployed in the development of digital government, including in the rapidly growing Estonian start-up community.

Results:

+ New technology and approaches are eagerly adopted in the Estonian digital government: Estonia is a pioneer in the world when it comes to implementing new solutions. We address and resolve major social and economic concerns in an entirely innovative way.

+ Estonia is one of the first countries to test the possible use and value of emerging technologies[28] in the ecosystem of digital government and the development of digital services.

+ The public sector collaborates to a greater extent and more systematically with the academic and private sector to create new knowledge and competences. The Estonian technology community is more competent in developing digital government owing to this.

Activities:

+ We initiate and fund pilot projects, promote relevant innovation-related cooperation with the private sector and participate in international initiatives where possible. Among others, we **launch mission-based**[29] initiatives for the adoption of entirely innovative solutions.

+ We increase and coordinate the **commissioning of digital government-related research and development activities** across the country and disseminate and put to use their results. Among others, we carry out systematic monitoring of the development and adoption of technology.

+ We initiate and implement **programmes for the adoption of new technologies that have a significant impact,** and participate in joint initiatives at the EU level.

6. Open innovation[30] and development of govtech community

Current situation:

+ The technical components and developments of digital government are largely non-transparent between administrative fields and for the private sector. Too little is known of what already exists or is being developed in the public or private sector, what is duplicated or what lacks the necessary synergy.

+ The current manner of developing digital government and the organisation of service management in the public sector restrict the private sector's opportunities of providing components and services which the state could outsource instead of developing and managing them. The private sector community using digital government developments is small, which hampers competition and the spread of competence.

+ Separate working environments which are incompatible or do not meet the state's expectations are used within the public sector and when partnering with the private sector. Expectations and requirements regarding developments are fragmented and insufficiently communicated, rendering cooperation and developments inefficient.

+ The services and components developed for digital government find little reuse. The solutions that have been created for digital government so far, particularly business services and related information systems, are exportable to a very limited extent.

+ The amount of open data has been rapidly increasing in recent years, but making them available has not become a widespread everyday practice, nor do they find much reuse.

Results:

+ The quality of Estonian digital services has been taken to a new level in cooperation with the private sector: the private sector makes a major contribution to digital government innovation with joint developments, sectoral links and complete solutions.

+ The govtech community is active and growing. Participants use tools that ensure the required information security and allow for flexible cooperation at the same time.

+ There is a transparent, exhaustive and updated overview of digital government services and technical components, relevant requirements and frameworks.

+ Separate software developed for digital government which is funded using taxpayers' money and includes intellectual property of the public sector is published with an open source license — as long as it is not significant with regard to national security.

+ The development of digital government relies on an architectural principles that allow for reuse. Solutions created for the Estonian state based on this can be adapted more easily both with regard to business and technology (including by means of cloud technology), increasing the export of digital government solutions.

+ All machine-readable open data are available and reused as actively as possible.

Activities:

+ We introduce **modern architectural principles and patterns which enhance reuse and support scaling** in the architecture of digital government. Among others, we adopt the approach of event-driven microservices and domain-driven design[31] as well as the API-first principle[32].

+ We promote **cooperation and forms of cooperation with the private sector** (including start-ups and foreign companies), and outsource more solutions as full services.

+ We establish **a single information space** for publishing the principles of the development of digital government services and technology, including a development and interoperability framework that provides guidelines. We keep the information space and frameworks updated.

+ **We expand the govtech community,** in other words the information field and the circle of foreign experts involved in development, relevant joint activities and information exchange.

+ We adopt and continue to develop **tools and platforms for reuse and cooperation,** including a technical services and database management system (the current RIHA), a code repository[33] and artifactory[34], collaborative applications, etc.

+ We implement and constantly update the **action plan for the reuse of data** with the aim of supporting the improved accessibility and reuse of data, including the use of confidential data for scientific purposes, the availability of open data and consent-based data processing.

The continued development of technology keeps creating new opportunities

7. Empowering digital change in public sector

Current situation:

+ Paper-based service provision has been replaced with digital services in Estonia but we can put digital solutions to even better use to improve public services and provide them more efficiently. Large-scale digital changes still have to be made in a number of fields: using digital possibilities, we can reform the logic behind the functioning of public administration and services.

+ We lack the knowledge and skills required for the initiation and successful completion of more substantial digital changes. The competences of public sector employees which are required for digital management and development have not been systematically increased or taken into account in recruitment decisions.

+ Another problematic issue is the uneven level of the adoption of digital services and solutions among local governments. There is a shortage of funds and people, making it impossible to do it at an equally good level separately in every city and municipality. The establishment of a single centre of competence on the basis of the Association of Estonian Cities and Municipalities has been launched to create and implement a common digital strategy of local governments but the capacity and tasks of this entity are still limited.

+ The continued development of technology keeps creating new opportunities of taking current information systems and services to a new level. In addition, new business needs keep emerging due to policies and the evolution of the state, e.g. in connection with overcoming cross-sectoral barriers to development. Therefore, it pays off to continuously develop and invest in digital government services and solutions

+ Keeping existing information systems and IT infrastructure up to date presents another challenge, and consistent attention and investments are required to update and maintain them.

+ In order to maintain the sustainability of the established digital government and introduce new solutions in the best way possible, it is practical to join forces across the state and share experiences and solutions with one another. Common guidelines and requirements must also be in place to ensure interoperability, avoid duplication and make sure that the solutions being created have the best possible technological basis. There have been renewed attempts to strengthen the management of the state information system and its architecture in recent years but only the first steps have been taken.

Results:

+ Digital government is maintained sustainably: important information systems are up to date and continue to be developed; relevant consistent funding is guaranteed. At the same time, a new wave of digital transformation has taken place in various fields (new large-scale changes have been launched and carried out). Among other things, the quality and sustainability of the digital services of local governments has improved.

+ We have the competences, support and funds required for bold and needed digital changes and the development and maintenance of services. The focus has shifted to the creation of value and especially to user-centricity and user experience, including cross-sectoral cooperation for this purpose. However, efforts are also still made to increase efficiency.

+ The directions of the development of digital government are known throughout the public sector and work is carried out to follow them in a uniform manner across the country. The functioning of digital government is based on common principles, and interoperable and compatible solutions (technologies).

8. Targeted international cooperation

Current situation:

+ Estonia is expected and wanted in all international cooperation formats in the field of digital technology and an esteemed contributor to international policy-making. Due to limited resources we have to choose where, on which topic, to which extent and how actively we participate, both in the European Union and elsewhere in the world.

+ People and companies operate internationally but still have to endure paper-based procedures — in the EU and among the Nordic countries as well as at a bilateral level, cross-border exchange of data and services have remained limited to pilot projects and individual initiatives. First and foremost, cross-border interoperability, including common approaches and supporting platforms, should be developed for this purpose.

+ Estonia has learned from the successful and unsuccessful digitalisation experiences of other countries. It has allowed us to take over good ideas and solutions and improve policy-making but it also needs purposeful activities in conditions where resources are limited.

+ The entire world is highly interested in the experiences and solutions of the Estonian digital government, opening up opportunities of exporting knowledge and solutions for Estonian experts and entrepreneurs. It is often useful or necessary that the state contributes in the early stages of the sales process by introducing its achievements and the actors in the sector.

Results:

+ The trends and volumes of external cooperation are in accordance with the objectives and needs of the development of digital government.

+ Estonian digital solutions are interoperable with European trends. Estonian residents and entrepreneurs can carry out the main procedures digitally and at once when travelling or doing business in the European Union, including the Nordic countries and the Baltic region — there are more and more cross-border services.

+ Best global practices and new trends are always taken into account in digital government-related policy-making.

+ The export of Estonian digital government solutions and consultation services grows with the help of 'opening doors'.

Activities:

+ We participate in the forms of cooperation of OECD and Digital Nations for the purpose of knowledge exchange and launch joint initiatives with the countries at the forefront of the development of digital government.

+ We participate in the forms of cooperation, policy-making and law-making of the EU and Nordic countries according to the development needs of digital government. The focus is on promoting cross-border interoperability and ensuring the compatibility of common solutions and the architecture of digital government.

+ Where necessary and possible, we support the Estonian IT sector with the export of digital government solutions, and state authorities in the field of business diplomacy by sharing content knowledge to other countries and providing state experts.

II sub-objective. Connectivity

Target based on the general objective:

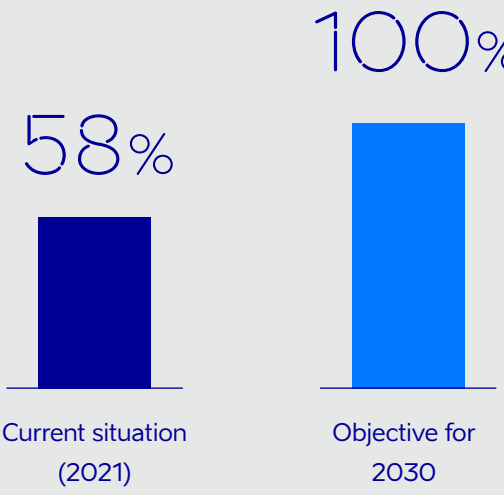
By 2030, ultrafast, reliable and affordable telecommunications connections are available in Estonia irrespective of your location, making it possible to create and use innovative services.

This sub-objective is directly related to the implementation of one of the axes of the vision of digital society: creating an impressive way of life. As has been stated above, the vision sets out that services should be convenient and available all over Estonia, which is why relevant (telecommunications) connections are needed.

The digital power of the economy, in turn, depends on the development of connectivity. The better the connections, the more digital solutions, products and services can serve as vehicles for development in various sectors and across Estonia. The quality and availability of connections also determines whether conditions are favourable for the creation of future solutions in Estonia and whether people from other countries come here with the same aspirations.

metric:

The proportion of Estonian households and companies who are able to access an Internet connection of at least 100 Mbit/s which can be increased up to 1 Gbit/s.



The Consumer Protection and Technical Regulatory Authority measures the results once a year.

Trends in connectivity

1. Up-to-date and forward-looking legal space

Current situation:

+ The single market communication regulation at the EU level sets a clear framework for the competition-based functioning of the Estonian communications market. Regulation must be consistent and legally certain: this turns Estonia into an attractive investment environment which, in turn, promotes the more rapid and efficient construction of communication infrastructure with a very high capacity[35]. The prices of mobile communications services are affordable. There are three major cable network operators and three mobile telephone operators and a number of smaller regional telecommunications companies on the Estonian communications market. A highly competitive retail services market proves that newcomers can easily enter the communication services market.

+ On the European and global scale, the Estonian communications market is small in terms of the number of consumers, which may lead to unexpected reorganisation or consolidation and in the end decrease efficient competition if unfavourable economic and regulatory circumstances coincide.

+ The experience of collectively developing a base network of high-speed Internet has provided favourable presumptions for the use of similar models in the future.

+ As a limited natural resource, the 3400-3800 MHz, 694-790 MHz and 24.25-27.5 GHz frequency bands (the so-called 5G frequencies) can be adopted in mobile communications as a next step. The possible use of the 40.5-43.5 GHz and 66-71 GHz frequency bands can be specified.

Results:

+ The interests of the state and market participants have been taken into account when shaping the legal space, so that the regulatory environment stays as stable as possible and the market develops in a balanced manner. Among others, cooperation in building core infrastructure is promoted, also in market failure areas.

+ Frequency resources required for the rapid development of the mobile network and the creation of new services have been allocated to the market quickly and efficiently.

+ The decisions adopted by the European Union and the International Telecommunications Union are in accordance with Estonia's interests.

+ **We shape and represent the positions of Estonia** in the discussions held in the European Union and the International Telecommunications Union

Activities:

+ **We promote innovative investment and cooperation models** for developing communication infrastructure

+ We carry out consistent and **efficient supervision of the functioning of the market**

+ We make the **frequency resources,** which have been agreed on internationally and are freed up domestically, available to market participants as quickly as possible **on the basis of competitions**

2. Development of access networks

Current situation:

+ In addition to networks established by telecommunications operators, a broadband backhaul network of 7000 km has been created with state support, evenly covering the entire country. It is available to all telecommunications companies and state authorities on an equal basis and at affordable prices in order to improve the availability of communication services and the affordability of joining networks in rural areas.

+ All three mobile networks offer adequate average and maximum speeds across Estonia which are sufficient for using modern services. The upload and download speeds of mobile Internet have increased by 70% on average within the last two years in Estonia.

+ Estonia is currently below the average of the EU with regard to the availability of fixed broadband subscriptions in rural areas and the adoption of ultra-fast broadband. The importance of a modern communications network has increased and will continue to increase in connection with remote working and learning due to the coronavirus pandemic.

+ As of 2021, there are an estimated 120,000 households and companies without a fast fixed connection in rural areas. More than 45,000 of them will get a fibre-optic access network by the end of 2023 which is in line with the 2025 Gigabit Society targets of the EU. Nevertheless, at least 75,000 addresses remain in market failure areas, i.e. the 'white area', which require investments made by the state in cooperation with telecommunications companies.

Results:

+ Opportunities to join access networks have been established for all companies and authorities as well as households that are inhabited throughout the year in rural areas.

+ Households, companies and authorities that have joined an access network can use and ultra-fast (at least 100 Mbit/s) broadband connection which can be increased up to 1 Gbit/s.

Activities:

+ **We support the development of very high capacity access networks** in rural areas where telecommunications companies do not invest under the conditions of competition.

3. Development of 5G and 6G core infrastructure

Current situation:

+ The existing core infrastructure including broadband backhaul networks and the towers connected to them provides a good basis for necessary investments in additional infrastructure and services in order to take a new leap in the development of mobile communications.

+ The widespread adoption of smart networks requires considerable investments from telecommunications companies, not only in connection with specific 5G/6G infrastructure, but also additions to the backhaul network and base stations. In order to make use of the potential of technology, it is important that services are not merely made available as pilot projects, but are also widely accessible in areas where business investments do not promise quick profits.

+ Balanced regional development and the availability of modern services may be hampered if there is no very high capacity broadband infrastructure and 5G coverage outside larger cities. At the same time, investing in new core infrastructure outside larger cities is not financially beneficial for telecommunications companies in the short term. 'White areas' can still be found along the primary movement corridors of people, i.e. the main and secondary roads.

+ At the moment there is no specific timeframe concerning the arrival of the next generation of mobile communications, i.e. 6G, but it can be assumed that it will begin at least before 2030.

Results:

+ The entire Estonia is covered by 5G. 5G core infrastructure has been built by the state in cooperation with telecommunications companies in market failure areas, allowing for the adoption of new technologies.

+ When 6G arrives on the market, Estonia is ready to adopt these networks.

Activities of the development plan:

+ We support the **establishment of core infrastructure in the main transport corridors** in Estonia, allowing for uninterrupted 5G coverage.

+ **We support the coverage of selected residential and business areas with 5G.**

+ We make the necessary **preparations for the adoption of 6G** when the relevant technology arrives on the market. We support reaching an agreement on the legal framework and support measures of the adoption of 6G at the EU level as soon as possible.

newest technologies are meant for the provision of services at a new level

4. Development of new content and business services

Current situation:

+ While 4G and early 5G services focused on consumer applications, newest technologies are meant for the provision of services at a new level (including communications and business services). The advances in the adoption of 5G and 6G are no longer viewed in terms of adding and counting connections. Instead, the success of their adoption is determined by the number and spread of content and business services (i.e. cases of use).

+ Solutions concerning the environment, energy, the industry of smart regions, connected mobility, communications security, social services and healthcare as well as free broadcasting may be of interest to Estonia. In other words, Estonia may gain economic and social advantages by developing use cases in these areas.

+ Estonia has the opportunity to be a pioneer by innovating content and business services based on new broadband technologies. Estonia would be able to take advantage of global 5G trends and support structural changes primarily in the areas of use of 5G business services.

+ The protection and upholding of the principles of Internet freedom continues to be important in Estonia in order to ensure the availability of modern content and business services.

Results:

+ Content and business services with significant public influence are in daily use, resolving important social and economic problems.

+ The level of Internet freedom remains high in Estonia.

Activities of the development plan:

+ We support the activities of the **development networks of innovative services.**

+ **We support** the planning, analysis and development of **services that attract widespread public interest.**

+ We participate in the work of international organisations with the purpose of **protecting Internet freedom.**

III sub-objective. Cyber security

Target based on the general objective:

The Estonian cyberspace is safe and reliable.

The cyber security sub-objective makes a direct contribution to the implementation of the vision of digital society 2030, since the aim is to guarantee the protection of our digital government, economy and digital way of life more broadly. In a safe environment, we can make bold advances in our digital development: the development of services, the digital transformation in the economy and the creation of future solutions. The cyber security sub-objective thus consistently supports the entire vision, also keeping in mind and promoting national security interests.

metric:

Estonia's cyberspace is resilient to cyberthreats and trusted.
For this purpose, we assess the state of two aspects or metrics:

1.

Service providers (within the meaning of the Estonian Cybersecurity Act) have met the requirements of cyber security at a level with no considerable potential damage.

Current situation: starting level unknown. The metric is being developed. The first result should be available in 2022 (we will add the metric to the calculation of the general objective once it has been developed and we have the first result).

2.

The use of digital services has not been avoided due to the existence of security risks.

Current situation: starting level (2019): 96.2%

Objective for 2030: above or equal to 96%

Metric: Internet users in the age of 16-74 who have refrained from communicating with public sector institutions or service providers via the Internet due to security risks in the last 12 months (Statistics Estonia, IT 44). The inverse response is used as the metric: the result is the number of people who have not refrained from communication. The result is measured by Statistics Estonia. Results have been measured at an interval of a couple of years so far. The Ministry of Economic Affairs and Communications will commission a measurement once a year from now on.

Trends in cyber security

1. Relevant national cyber security set-up

Current situation:

+ The responsibility for ensuring cyber security is largely decentralised in Estonia. All information system owners and electronic service providers must take care of the security of their systems and incident management on their own and have the abilities required for that. At the same time, the cyber security field is increasingly specialised and owners of systems find it very difficult to obtain all the competences required for the protection of their systems. It creates an excessive burden for them and reduces the level of cyber security.

+ Some tasks related to guaranteeing cyber security are centralised. For instance, these include cyberspace monitoring and safety warnings, the development of the standard of information security measures, supervision and policy-making, etc. In addition, certain state functions are centralised, such as the investigation of cybercrime, crisis management and cyber operations for the purposes of national defence.

+ In order to ensure that the cyber security field is coordinated, a system involving a leading ministry and a cyber security authority is implemented. The leading ministry in the field of national cyber security is the Ministry of Economic Affairs and Communications (MEAC) and the cyber security authority is the Information System Authority (RIA). The Ministry of the Interior and its subsidiary bodies are responsible for investigating cybercrime and ensuring internal security. The Ministry of Defence and the authorities in its area of government are assigned cyber security tasks related to national defence. The Ministry of Foreign Affairs deals with cyber diplomacy. This general management system has evolved over the years but the roles, responsibilities and allocation of work are unclear in a number of cases and insufficiently regulated by law.

+ The roles, responsibilities and tasks related to ensuring cyber security must be determined according to current needs and they must be comprehensive. Changes and growth in cyberthreats and additional tasks (certification, technology assessment, operational cooperation, etc.) have to be taken into consideration when updating the organisation of cyber security.

+ The current arrangements for resolving cyber incidents and crises must be supplemented. Various incidents and situations (including COVID-19) have highlighted shortcomings in the national crisis management system. For example, the tasks and responsibilities of various levels are unclear, ranging from the institutions and public authorities influenced by the incident to the responsible ministry of the field and the Government of the Republic.

Results:

+ A clear, comprehensive national cyber security administration model that meets the needs of Estonia (including risks and trends) is in place.

+ The responsibility and tasks of authorities and organisations have been appropriately laid down in existing legal acts.

Activities:

+ **We constantly analyse changes in digital trends and cyberthreats and their impact** on cyber security in Estonia and its organisation.

+ We prepare and update a **cyber security administration model** based on risk analyses, determining the roles, responsibilities and tasks of authorities and organisations with a national cyber security function.

+ Where necessary, we carry out an **organisational restructuring** based on the updated national cyber security administration model.

+ **We amend and specify** legal acts, contracts, crisis-response plans and other **regulatory documents**, which set out the roles, responsibility, tasks and cooperative relations of authorities and organisations.

2. Analysis capacity for trends, risks and impacts

Current situation:

+ In order to ensure the sustainable development of digital society and the safe implementation of innovation, we have to improve our understanding of global trends and the development of technology. This means that we must be able to understand the risks associated with technology and their impact, and develop risk management measures. Cyber security must support innovation and innovation must support cyber security. More attention must be paid to accomplishing it than has been done so far.

+ Information system owners are responsible for mitigating risks related to their information systems and services. A number of authorities and organisations support the compilation of risk assessments and the development of security measures with analyses and instructions: the Information System Authority, security authorities, educational and research institutions and national and international centres of competence. The capacity to constantly analyse the situation needs to be developed in order to update existing security requirements and prepare practical recommendations and instructions for information system owners. This also requires the development of a relevant basic competence, among others at academic institutions.

+ The analysis of the trends, risks and impacts of digital society is not carried out entirely proactively and systematically yet. Developments in the field of artificial intelligence, cloud technology, robotics, augmented reality, communication technology, the Internet of things and many other technological trends bring along with them changes which we need to prepare for. Our analysis capacity is still insufficient for an appropriate interpretation of the impacts of global developments in the Estonian context and the development of necessary security measures.

Results:

+ Decision-makers, policy-makers and the owners of networks and information systems have a good situational awareness of the trends and risks of global digital development and cyber security and their impact on Estonia.

+ Risks have been thought through and mitigated when planning and implementing digital innovation.

+ We can develop and implement cyber security measures that are suitable or the Estonian context quickly enough, among others by engaging the competences of various authorities, companies and experts.

cyber security must support innovation and innovation must support cyber security

Activities:

+ We increase the capacity of the public sector in assessing the cyber security situation and risks and developing security measures across the state and in various sectors. We also increase the relevant awareness and competence.

+ We establish a work process for security considerations in planning digital innovation.

+ In order to support policy-making related to cyber security, we establish a **network-based think tank** which takes technological, security policy, economic, foreign policy and other relevant aspects into account in its prospective assessments and recommendations.

+ We establish sustainable arrangements for defining and funding the research and development needs, programmes and projects of cyber security. We develop and implement a national plan concerning research and development activities related to cyber security.

+ We support **an increase in funding for research and development and joint actions related to cyber security at the EU level** and actively participate in them in order to collectively generate and share knowledge in the EU.

+ We increase the **capacity of academic institutions and development centres** in implementing cyber security-related research and development projects of national importance.

In the aforementioned activities, we pay more attention to and focus on:

+ ensuring the security of the basic services and platforms of the Estonian digital government, and artificial intelligence and cloud computing;

+ strategic risks related to the reliability of technology which may have an impact on society via the use of and dependence on technology.

3. Increased capacity for maintaining cyber security

Current situation:

+ The current cyber security capacity of the state is insufficient for preventing and reducing the risks that endanger networks and information systems. The consistent growth and development of cyberthreats creates the need of rapidly developing our preventative capacity, and improving the monitoring and supervision of its implementation.

+ The implementation of cyber security measures is costly in the case of a decentralised administration model. Authorities and organisations need similar resources (experts, tools) to exercise their cyber security functions, which makes it more expensive to guarantee cyber security. Not all authorities have sufficient capacity for procuring specific competences and taking measures at an adequate level due to limited resources.

+ Cyber incidents occur and we have to be ready for them. The Estonian digital ecosystem has an extremely complex infrastructure, rendering it financially impractical to implement all kinds of preventive security measures. The use of security measures must be optimised and residual risks must be taken into account. This means that it is not possible to prevent all incidents. Instead, if they occur, we have to quickly identify them, respond and resolve them.

+ The capacity for managing and resolving cyber incidents and crises is insufficient, considering the digital dependence of the Estonian state. The crisis management system faces greater demands due to the growth in the number of cyberthreats and incidents. This concerns both organisational capacity and the use of cyber security products and services. Cyber security tools supporting the monitoring of networks and information systems, the development of a situational picture and the management of incidents must be constantly updated and improved.

+ There is a shortage of competent cyber security experts. The field of digitalisation and cyber security is more and more specialised. The increasingly rapid development of various technologies, such as cloud computing, artificial intelligence, cryptosystems, the Internet of things, robotics, augmented reality, etc. creates a need for specialised experts. It is required for national policies, the development of security measures and profitable international cooperation.

+ It is challenging to be an internationally trailblazing and leading country in the ever-changing and specialising field of cyber security. Estonia's good reputation derives from the successful use of digital possibilities, accompanied by the skilful provision of cyber security. This reputation supports the export opportunities of companies and contributes to national security. A high degree of competence (i.e. experts and practical experience) is required in many fields in order to be able to direct international processes. Due to increasing complexity, it is not possible to be highly competent in all aspects; instead, clear areas of specialisation must be selected.

Results:

+ Measures guaranteeing cyber security have been taken at the required level which has been determined in updated legal acts, standards and instructions. Guaranteeing the continuity, integrity and confidentiality of important services is the priority.

+ The state is capable of promptly resolving crises of various dimensions and participating in international crisis management.

+ There are enough specialised experts and tools to implement modern cyber security measures.

+ Estonia is a trailblazing and leading country in specific prioritised fields of cyber security in the EU and at a broader international level.

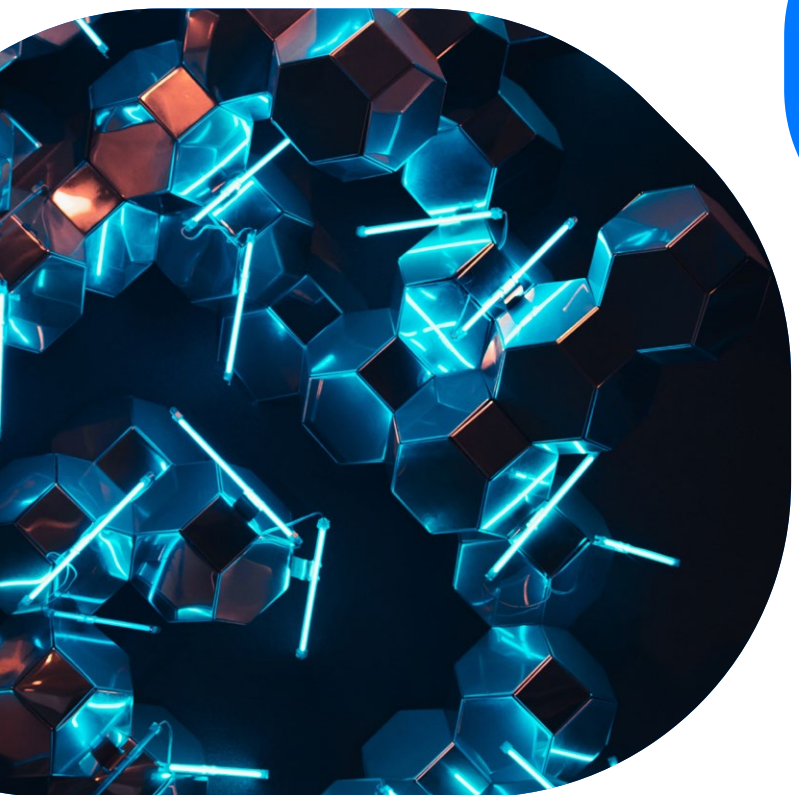
The current cyber security capacity of the state is insufficient for preventing risks.

Activities:

+ We **systematise** and consolidate to a practical extent **the functions of cyber security.**

+ We increase the **capacity** of government agencies that participate in the provision of national cyber security **in monitoring and supervising the cyber security situation.** We develop updated metrics and mechanisms for assessing the situation of national cyber security.

+ We organise **national and international exercises** to practice resolving incidents.



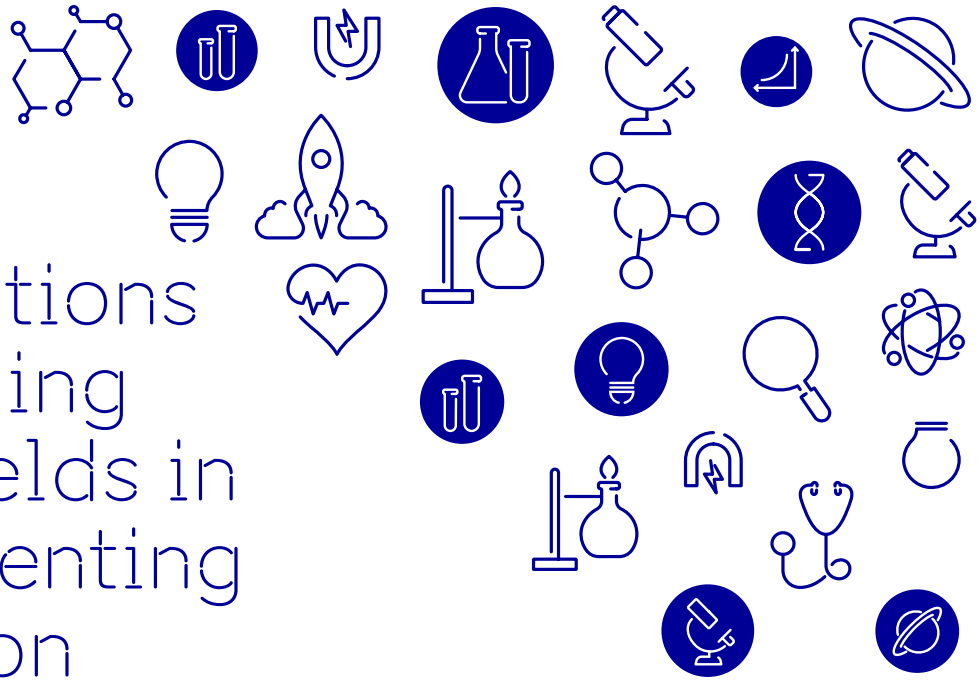
+ We increase the **capacity** of authorities and organisations performing public functions and providers of vital services **in taking preventive measures:** creating a safe architecture, implementing information security standards, certification, testing (including a considerable increase in the number of various tests), auditing, training, consultation and notification.

+ We increase the **capacity** of government agencies that participate in the provision of national cyber security **in resolving cyber incidents.**

+ We advocate the provision of **cyber security at a uniformly high level** in the EU and promote cyber security-related cooperation between Member States in order to manage risks and increase our joint capacity of responding to incidents.

+ We increase the **number of specialised experts in the public sector** with regard to issues that are required for the provision of a high level of cyber security, the functioning of basic digital government services, the implementation of artificial intelligence and cloud computing and digital innovation.

+ We determine and **develop as a priority the fields of cyber security where Estonia has the greatest international potential.** We take the initiative at an international level in fields that are based on national priorities and substantive strengths.



Expectations concerning other fields in implementing our vision

In order to implement the vision of digital society 2030, this development plan needs to be supplemented in other policy fields in a number of ways. According to the procedure for compiling development plans in Estonia, it is not an obligation automatically conferred on other fields, but rather a request and expectation in connection with the content and direction of other policy measures, based on the vision of digital society established in the framework of this development plan. These create the basis for submitting opinions and coordinating activities between authorities when implementing and updating development plans.

The following is required to achieve the targets of digital society by 2030:

+ The availability of a sufficient number of ICT specialists with an adequate level, including cyber specialists, is of critical importance.

The number of ICT specialists must at least double in the economy by 2030 and the proportion of cyber specialists must increase among them to achieve future targets to the extent necessary.

For this purpose, relevant learning opportunities must constantly be expanded and the quality of learning must be improved at all levels. Above all, this requires decisive steps with regard to increasing the volume and quality of teaching capacity, including ensuring a sufficient number of teachers.

As the domestic education system does not suffice for realising our potential, we must make it easy for talents to come to Estonia — it must be a convenient and attractive destination.

+ In order to take the wider digital transformation in the economy and public administration to the next level of digital maturity,

it is important to launch widespread reskilling and upskilling initiatives in connection with digital skills.

This enables specialists of various fields to acquire required specialised digital knowledge in order to launch and manage or support digital changes in their organisations. Furthermore, the development of (specialised) digital skills must be a natural part of every level of education. These steps also facilitate the adaptation of employees to changes in the economy.

+ The need to address the wider digital literacy of the population persists

The need to 'attract people to the Internet' is ever decreasing. Instead, it must be ensured that they have up-to-date skills to deal with digital solutions in a useful and safe manner. By 2030, all Estonian adults should be regular Internet users. This gives us the opportunity to guarantee their sufficient capabilities, including a basic level of awareness, so that they can make even better use of services following the leap in the development of digital government.

+ Within the field of research and development activities, investments have to be made in increasing the capacity of research and development (R&D) related to the development of digital society.

This way, we can find people to create smart solutions and detect knowledge and solutions that can be promptly tested and implemented in the state and economy. The key is to guarantee sufficient funding of ICT-related R&D.

+ The best possible services need to be based on good Estonian language technology,

so that domestic and global service providers can make their services as convenient as possible for the members of the Estonian digital society. This requires increasing investments in basic language technology solutions.

+ Enterprise policies must simultaneously focus on two targets:

1) supporting digital transformation in more traditional sectors (e.g. industry) by pulling the necessary levers

- from improving knowledge and skills to supporting investments (including ensuring a cyber-secure digital transformation)

2) constantly developing a technology-based business environment.

We must establish and guarantee excellent conditions in Estonia for developing smart products and services, founding and growing new companies creating such solutions and attracting relevant foreign talent.

Developing the business environment plays a significant role in

making Estonia the easiest place to conduct business in the entire world.

As the next leap in our development, it is important to develop the organisation of real-time economy and solutions.

+ In order to guarantee the development of the business environment and more broadly the creation and adoption of new solutions,

law-making must be flexible in the rapidly changing world and quickly respond to opportunities.

At the same time, legislation must continue to protect the fundamental rights of people and ensure the ethical use of data.

+ If public services become more and more invisible, i.e. proactive and automatic in the state, communication between people and the state and people's understanding of the functioning of the state may decrease. To avoid this,

the quality of information services and the openness of governance must be improved.

In other words, people must be more and more actively involved in making public decisions and holding discussions. Among others, digital solutions can be smartly used for this purpose, ranging from supporting the functioning of communities to increasing the opportunities of participation at national level.

+ Using the support activities of business diplomacy and export, we must continue our efforts to

provide Estonia with the reputation of an ambitious and smart digital society and state in the world.

This opens doors to companies, allowing them to take their IT solutions to the world, and turns them into stronger partners in the creation of future solutions for Estonia. On the other hand, Estonia's prominence also determines whether talents and global players consider Estonia as their next place of residence.

+ Social engagement, coherence and reduction of division highlighted in the vision

is only possible if health, welfare and other development plans aimed at the development of society focus on an extensive and substantial digital transformation strategy, the development of content areas is strongly integrated and implementation is managed effectively.

+ In addition, we

must continue the rapid digitalisation of our cultural legacy in the field of culture,

improve the quality of the creation, preservation and availability of digital culture and promote the reuse and cross-usage of digital content. This way, we can accomplish the vision of promoting Estonian culture in the digital era.

Organisation of management

The Ministry of Economic Affairs and Communications (led by the Minister of Entrepreneurship and Information Technology as of 2021) **as the main body leading the development of digital society is responsible** for implementing the development plan.

The development plan is **implemented by means of a digital society programme** (hereinafter referred to asthe programme) which includes the development of digital government, connectivity and cyber security. The programme sets out the specific objectives for certain years and the activities required for accomplishing them together with the responsible entities, funds and metrics. The programme is prepared **for four years** according to the duration of the state budget strategy and updated **once a year.**

There are plans to **review the development plan more thoroughly at least twice during this period and update it** in order to take into account the rapidly changing environment (e.g. the development of technology) and the success of the activities. The implementation of the development plan is previously assessed as one of the bases of the review. The updates are to be made in the first half of 2024 and by the end of 2027.

In terms of organising the management of the development plan, the main **task is to ensure synergy between the objectives and activities of various areas and authorities** because the development of digital society (above all the implementation of the vision for 2030) depends on the common efforts of many participants. In order to ensure the required compatibility, the coordination of cooperation and a single information field, **the management of the development plan and its various levels have been planned as follows.**

Name	Task/role	Frequency	Members
Steering group of the Digital Agenda **(within the meaning of the government regulation: steering committee)**	+ Discussing and approving the development plan and its amendments to forward them to the government + Monitoring and guiding the implementation of the development plan at the level of the vision and the fields, and directing the cooperation within a field, where necessary + Discussing the focal points of the programme every year, approving the programme, discussing and approving changes on an ongoing basis, where necessary + Initiating the assessment of the development plan	At least once a year (at the beginning of the year when the programme is updated), more frequently where necessary	**Head:** minister responsible for digital development **Members:** Deputy Secretary General for Digital Development of MEAC; the deputy secretary generals of fields contributing the most to the vision (MEAC, economic development and business environment; Ministry of Education and Research, digital skills; Ministry of Justice, public law); the Government Office as the coordinator of national strategic planning; representatives of the Association of Information Technology and Telecommunications and the Association of Estonian Cities and Municipalities; the directors general of the Information System Authority and the Consumer Protection and Technical Regulatory Authority; (a) non-governmental expert(s) in the field of digital society development The work of the steering group is organised by the Deputy Secretary General for Digital Development of MEAC

Name	Task/role	Frequency	Members
Cyber Security Council **(subgroup of the security committee of the government)**	Cyber security: + Discussing and approving the development plan and its amendments before the discussion of the government + Monitoring the implementation of the development plan and related development plans and directing cooperation in the field, where necessary + Discussing and approving the focal points of the programme every year	Development plans are discussed in the council at least once a year when updating the programme at the beginning of the year	Head: Secretary General of MEAC Members: secretaries general of relevant ministries, heads of authorities and other representatives of the field The work of the council is organised by the National Cyber Security Department of MEAC
Advisory committees of specific fields: advisory committees in the fields of digital government, cyber security and connectivity	+ Monitoring the implementation of the development plan and directing cooperation at working level in their own field where necessary + Discussing the programme and making proposals to the steering group + Discussing the assessment of the development plan and making proposals for amendment to the steering group	At least once or twice a year (before the end of the half-year)	Head: Head of the relevant department at MEAC Related public sector institutions (at the level of deputy secretary generals or heads of department); a representative of the Association of Estonian Cities and Municipalities; representatives of the private sector; experts of the field The work of the advisory committees is organised by the relevant department at MEAC under the Deputy Secretary General for Digital Development
Thematic working groups and networks: permanent (e.g. the IT steering group, architectural council) or temporary, including cross-sectoral and multi-agency groups	+ Planning the more specific content of activities and implementing them, relevant coordination and organisation + Making proposals to initiate new activities or adjust existing ones	When required	Depending on the activity and topic — related authorities, partners, target groups

Estimated cost

The estimated cost includes the total assessment of the costs (without VAT) that are required for ensuring sufficient funding for the achievement of the objectives of the Digital Agenda via the digital society programme:

Year	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	Total 2021–2030
Cost (million, €)	68	111	135	120	120	125	131	135	138	139	1224

Among others, the following has been included and taken into account in the prognosis:

+ the known funding that has already been decided for the period 2021-2030, including external funding and basic funding from the state budget for the implementation of the lines of action of the development plan (according to the latest budget strategy);

+ the total estimated cost of the implementation of the lines of action, i.e. the so-called additional needs which have to be met in the state budget process in the future.

References

[1] Estonia 2035: https://valitsus.ee/strateegia-eesti-2035-arengukavad-ja-planeering/strateegia

[2] Digital Economy and Society Index 2020, https://ec.europa.eu/digital-single-market/en/digital-economy-and- society-index-desi

[3] eGovernment Benchmark 2020, https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2020-egovernment-works-people

[4] 2020 United Nations E-Government Survey, https://www.un.org/development/desa/publications/ publication/2020-united-nations-e-government-survey

[5] Digital government means the use of digital technology for the provision of public services and the organisation of public administration and governance.

[6] A public digital service is a direct public service or support service which is provided via an electronic channel, such as an electronic self-service, the information gateway eesti.ee, a website/portal, application or e-mail.

[7] There are plans to also start measuring the satisfaction of public sector employees with e-services.

[8] https://www.riigiteenused.ee/et/user

[9] The common solutions of digital government are solutions which are used by several administrative fields or authorities (or the private sector) and which take into consideration broader state-wide needs.

[10] Event services are direct public services provided jointly by several authorities so that a person is able to perform all the obligations and exercise all the rights conferred on them due to an event or situation. An event service compiles several services (hereinafter referred to as component services) related to the same event into a single service for the user.

[11] Proactive services are direct public services provided by an authority on its own initiative in accordance with the presumed will of persons and based on the data in the databases belonging to the state information system.

[12v]The first development plan was approved by the Cabinet in December 2020: https://www.mkm.ee/et/ uudised/valitsus-kiitis-heaks-jargmised-sammud-sundmusteenuste-arendamisel

[13] In Estonian, the word 'kratt' refers to a system of artificial intelligence. It is based on a software algorithm which is autonomous and capable of learning and carries out activities traditionally carried out by people.

[14] Estonia's national artificial intelligence strategy for 2019-2021 https://www.mkm.ee/sites/default/files/eesti_kratikava_juuli2019.pdf

[15] The reliability of artificial intelligence is based on ethical guidelines for AI which have been set as a goal at the EU level.

[16] Bürokratt is an interoperable network of public and private sector AI applications which has been linked with state

information systems and functions as a single channel for direct and information services from the viewpoint of users. See the concept of Bürokratt at https://www.kratid.ee/burokratt

[17] A human-centred digital government is one where the use of digital solutions is not an end in itself but rather a tool for increasing the well-being of people. For people's trust in digital government to become stable and grow, digital solutions have to be reliable. Reliable digital solutions are dependable, ethical and lawful, guaranteeing the fundamental rights and freedoms of all people.

[18] The Personal Data Usage Monitor makes data processing transparent, improving people's awareness and helping institutions respond to personal data enquiries. The Personal Data Usage Monitor provides a person with an overview of what has been done with their data and what is displayed in the state portal eesti.ee. It is meant to be linked with public sector information systems which store and process personal data in their databases.

[19] A consent service is a digital service linked to the database of an authority, enabling people to give their consent, and view and withdraw it. Data users can view the consents given to them for the issue of data; database administrators can check whether a consent has been given when issuing personal data to the data users.

[20] The aim of the green IT initiative is to reduce the negative impact of technologies by designing, producing, using and later processing technologies in an environmentally friendly manner.

[21] Privacy technology is a technical measure for ensuring the privacy of a person in a proactive and preventive manner.

[22] The 'once-only' principle means that the same data are not repeatedly requested from users. The principle of reuse refers to an agreement allowing the reuse of data collected by someone else or for another purpose in the creation of new knowledge.

[2] The X-Road is a technological and organisational environment enabling a secure Internet-based data exchange between state authorities and the private sector, whereby evidential value is guaranteed. To exchange data, a member of the X-Road describes the shared data and other members can use that data based on an agreement. Thanks to the large number of systems that have joined the X-Road, all members can use the services and data of others to improve their own business processes.

[24] Nordic Institute of Interoperability Solutions: https://www.niis.org/

[25] A data embassy is a private cloud solution of the state, allowing for the storage and, where necessary, exploitation of data and services at a secure data centre outside the state's territorial borders. It makes it possible for the Estonian state to continue functioning if the operation of data centres within its territory is terminated or suspended.

[26] The marketplace is a common platform for the procurement of standard IT services in the public sector.

[27] English: disruptive innovation

[28] English: emerging technologies

[29] Mission-based initiatives are innovative (cooperation) initiatives directed at resolving a multi-faceted problem that has a state-wide or broad social impact.

[30] Open innovation means that innovative solutions are created and built openly together with and by various parties or even under their leadership, instead of the state or a single authority devising, commissioning and doing everything on its own.

[31] English: event-driven microservices and domain-driven design

[32] The so-called API-first principle

[33] English: code repository

[34] English: artifactory

[35] A very high capacity network either consists wholly of optical fibre elements at least up to the distribution point at the serving location or which is capable of delivering under usual peak-time conditions similar network performance in terms of available down- and uplink bandwidth, resilience, error-related parameters, latency and its variation.

[36] Shaping Europe's digital future: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

[37] A European strategy for data: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[38] Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0587

[39] EU Cybersecurity Strategy: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[40] An SME Strategy for a sustainable and digital Europe: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52020DC0103

[41] EU Digital Education Action Plan (2021-2027): https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_et

[42] European Skills Agenda: https://ec.europa.eu/social/main.jsp?catId=1223&langId=en

[43] Coordinated Plan on Artificial Intelligence: https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0009.01/DOC_1&format=DOC

[44] Tallinn Declaration: https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

[45] Berlin Declaration: https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

[46] Europe's Digital Decade: digital targets for 2030: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_et

Estonia's Digital Agenda 2030