Value-Driven Digitalisation Work Agenda

Table of Contents

Reason for the *Work Agenda*

Coalition Agreement

‘ The current digital revolution offers great opportunities for our society and economy and we will take advantage of them. At the same time, this will require solid rules, supervision and strategic autonomy. We have a duty to protect fundamental rights and public values (safety, democracy, self-determination, non-discrimination, participation, privacy and inclusivity), and must create a level economic playing field with fair competition, consumer protection and broad social cooperation. People also need to feel safe online. For that reason, the government, jointly with local or regional authorities and European partners, has committed itself to ensuring our public values in the digital domain. We will build a safe and inclusive digital society, rich with opportunities, for all Dutch and European citizens.

Source: Coalition Agreement 2021–2025, Digitalisation

Letter setting out the main features of the digitalisation policy

‘ It is up to us, as a nation and government, to set the digital transition on the right track and ensure proper social embedding. We must foster and embrace opportunities in a way that secures our public values. In the process, in partnership with the EU, we will make our own choices about the developments we should boost and those we should slow down, and the direction in which those developments should be steered. The aim is to safeguard public values during the digital transition, facilitate the debate on value-driven digitalisation and develop the building blocks for a values-drive digital government.’

Bron: Kamerbrief hoofdlijnen beleid voor digitalisering

Digitalisation policy themes

In this work agenda:
- **Digital Foundation:** cybersecurity, online identity, control of own data, privacy, equal treatment, democracy, strong rule of law, well-functioning digital government service provision, inclusivity and digital skills
- **Digital Government:** value-driven and open

To follow in more detail in the first half of 2023
- **Digital Society:** opportunities to increase the quality of our society and make it more inclusive, innovative and efficient in areas such as education, public health, climate, agriculture, food, the natural environment and mobility

To follow this year
- **Digital Economy:** an open, honest and secure digital economy that contributes to sustainable economic growth

Work Agenda *Five programme lines*

Foundation

1
Everyone will be able to *participate* in the digital age

2
Everyone will be able to *trust* the digital world

3
Everyone will have *control* of their digital lives

Digital Government

4
A digital government that works on a *value-driven* and *open* basis for all

5
Strengthen the digital society in the *Caribbean part of the Kingdom*

The Caribbean part of the Kingdom

1

Everyone will be able to *participate* in the digital age

We won't abandon anyone during the digital transformation. We will be making substantial investments in digital skills for all citizens and providing support through information points in libraries or tools such as Machtigen [Authorisation]. We will make things as easy as possible for those with digital skills by providing supporting and convenient services and a portal to suit everyone. We will set up innovative and proactive services to assist citizens when needed. We will help authorities, businesses and social organisations keep up with the digital age, e.g. by supporting the implementation of new European legislation. Lastly, we will seize the opportunities digitalisation offers to work towards a modern, inclusive democracy and reduce the impact of online disinformation in the process.

2

Everyone will be able to *trust* the digital world

As in the physical world, security and trust in the digital world are essential prerequisites if citizens and businesses are to flourish and public values are to take centre stage. However, online security is by no means a given, with the ever-present risk of threats such as phishing, botnets, cybercrime and disinformation. We will combat those risks and the damage they cause. We are committed to ensuring privacy, anticipating emerging technologies and creating a reliable and secure digital environment so that everyone can enter the online world with confidence.

3

Everyone will have *control* of their digital lives

Every citizen must be able to view and retrieve their own data held by the government and have it corrected where necessary. You must also be able to decide with whom you share your data. This will put an end to public and private parties collecting, trading and sometimes losing all kinds of personal data. This change will require regulations and policy on wallets and other basic services. We will connect the developments taking place within various ministries in this area. Algorithms can also give you the feeling of losing control of your life. With legislation, the creation of frameworks, and supervision, we will make algorithms and their applications fair and transparent so that you can rely on data being treated properly.

4

A digital government that works on a *value-driven* and *open* basis for all

The government must be fully digitised for the first three lines to succeed and for the government itself to function effectively, both internally and externally. To that end, the government must be open and driven by public values in its actions (including professionalism, integrity and transparency). We are committed to ensuring adequate information management that will give citizens, organisations and parliament insight into the government's actions and decisions. We also intend to guarantee careful data management (data handling). This will give citizens confidence that their personal data are being handled properly. We are also working on our internal ICT organisation and systems so that we, the government, can direct this process. For example, we are building a secure and scalable infrastructure with strong generic features. We are also working to improve digital professionalism and flexible, experimental and open approaches. We will not do this alone but through cooperation with regional authorities and the scientific and business communities.

5

Strengthen the digital society in the Caribbean part of the Kingdom

Citizens and businesses in the Caribbean Netherlands must be able to participate in the digital society at an equivalent level. This is often not yet the case. We are working towards providing high-quality and accessible physical and digital services. We will also be increasing the digital skills of citizens and businesses in the Caribbean Netherlands and addressing internet stability, speed and affordability. We will improve privacy safeguards and invest in the digital society. There are similar issues in the Caribbean countries within the Kingdom, with regard to which we will provide assistance and support.

Note: The ambition is "everyone". It is about reaching as many people as possible, limited by legal or justified exceptions

VALUE-DRIVEN DIGITALISATION WORK AGENDA

Priorities are described along five dimensions

Social challenge

- Clear description of the social problem we want to solve and/or opportunity we want to exploit
- Focus on the urgency and importance of the problem

Results achieved

- Main results of actions already taken
- Focused on recently achieved results

Goals

- Overview of the main goals, described in terms of the impact on citizens and businesses as much as possible
- Goals are long-term and describe the desired outcome

Target indicators

- Indicators to measure the extent to which the ambition has been realised[1]
- A target value is included where possible
- 'Yet to be determined' means that appropriate benchmarks, indicators and target values will be formulated in the first half of 2023

Actions

- Key actions and their intended outcomes. Actions without particularly visible results are not included
- Short-term results (by the end of 2023) and longer-term results (by the end of 2025)
- The initiator and the party or parties carrying out the action are identified

1. *Example of an indicator: '80% of people aged 16–75 will have basic digital skills by 2025'*

Ministries, supervisory authorities, inter-administrative partners, implementing and knowledge organisations, communities, the EU, international partners and Parliament will be jointly responsible for achieving results.

1 Everyone will be able to *participate* in the digital age

1.1 Improve digital skills and knowledge | Overview

👥 Social challenge

Too many people lack the digital skills needed to participate in society and take advantage of the opportunities digitalisation has to offer. Those skills include media literacy, information literacy and basic ICT skills. Digital skills are probably among the most important skills citizens must have to cope with everyday life. According to the Netherlands Court of Audit (Algemene Rekenkamer), an estimated 2.5 million Dutch people lack the basic skills, including digital skills, to use messaging services and computers at a basic level. Around three million Dutch people have insufficient digital and administrative skills, such as those needed to apply for benefits (digitally or otherwise) and to do business with the authorities and the private sector. Participating in the digital world is not without risks, such as cybercrime and disinformation. In the Netherlands, more than five million Dutch adults (including employees, young people and the elderly) struggle to consciously, critically and actively engage with digital social media. Local or regional authority officials and company executives also frequently lack the necessary skills.

📈 Results achieved

- Basic infrastructure (collaboration between the government, municipal authorities, course providers and social organisations) to improve the basic skills of the 2.5 million semi-literate people in the Netherlands (Tel mee met Taal (Count on Skills) programme) is in place
- 554 Digital Government Information Points to help people with digital public services
- Public-private partnership to provide people with digital devices (#allemaaldigitaal). More than 12,000 have received a device.
- A Digital Helpline (Digihulplijn) is up and running, with between 500 and 1000 people calling every month for answers to questions about digitalisation
- A Basic Skills Master Plan (Masterplan Basisvaardigheden) under which the government will invest EUR 1 billion each year in reading and writing skills, mathematics, citizenship education and digital literacy for primary and secondary education
- A Civil Service Professionalism Programme (Ambtelijke Professionaliteit Programma) in which RADIO trains senior civil servants to ensure they have an adequate level of digital literacy and are capable of leading the digital transition

🎯 Goals

			🕐 Target indicators
1	Everyone will have the digital skills to participate in the digital society as independently as possible. We will do this by proactively reaching out to people lacking in digital skills and providing an adequate range of training courses that reflects people's needs and technological developments. We will focus on target groups and cover various areas, including healthcare, agriculture, food, the natural environment and finances	➔	Percentage of people aged 16–75 with basic digital skills by 2025 (according to Eurostat) (target value: 80%; the value in 2021 was 79%)
2	Children and school-leavers are digitally proficient	➔	Yet to be determined
3	Public administrators, employers and employees are digitally proficient and able to take advantage of the opportunities technology and digitalisation can bring in a safe and resilient way	➔	• By 2025, an up-to-date and appropriate range of courses focused on digitalisation will be available for government administrators and senior managers on a long-term basis • By 2025, there will be an accessible range of courses in every labour market to teach advanced digital skills (e.g. AI) to school leavers and people who are retraining
4	Citizens will understand the opportunities and risks presented by the top five emerging technologies	➔	Yet to be determined
5	People will be able to turn to their neighbourhoods (public, private and social) for support with digital challenges in everyday life	➔	Percentage of people requiring digital support who succeed in finding assistance in their neighbourhood by 2025 (target value: 90%)

1.1 Improve digital skills and knowledge | Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1 Continue the development of platforms - adopt a national and local-level approach (collaboration between libraries, municipalities, welfare organisations and private parties) to enhance digital skills such as media literacy, information skills and basic ICT skills, approaching people proactively. This will involve the further development of things such as Tel mee met Taal, Digital Society Alliance (Alliantie Digitaal Samenleven), the Dutch Media Literacy Network (Netwerk Mediawijsheid) and the help network for Digital Government Information Points (IDO)	• Wide range to enhance digital skills for everyone • Information Point as advice centre for safe internet use • Information Point as an advice centre to teach digital skills needed in dealings with the healthcare sector (e.g. booking a hospital appointment online) • Between 25% and 50% of municipal authorities are actively engaged in reaching out to and helping people with acquiring digital skills and improving inclusivity • Expansion to 600 IDOs, including static and mobile facilities at locations outside libraries	• All 35 contact municipalities are actively engaged in digital inclusion, reaching out to and helping people acquire digital skills. They have prepared a plan for this to guide regional municipal authorities and have set up a platform • Screening instrument that people can use to test whether they are sufficiently proficient and obtain an overview of the range of appropriate courses	**Ministry of the Interior and Kingdom Relations (BZK)**, Ministry of Education, Culture and Science (OCW), Ministry of Health, Welfare and Sport (VWS), Ministry of Social Affairs and Employment (SZW), Association of Netherlands Municipalities (VNG), municipal authorities and libraries
2 Public/social/private collaboration to establish **framework conditions for digital skills**, such as computers and internet access	• The government will make 50,000 devices available for vulnerable groups (150,000 every three years)	• Digital Society Alliance (ADS) multi-year plan • Public-private support network	**BZK**, other ministries, ADS, NL Digital
3 Set up an **annual digital skills monitoring repor**t (including basic ICT skills, media literacy, information literacy and computational thinking)	• Annual monitoring report combined with existing Eurostat reports • Statistics Netherlands (CBS) *Tel mee met Taal* monitoring report • Digital skills study by the University of Amsterdam (UvA) completed • Conduct five-year measurement study based on the EU-level indicator for the digital skills of secondary school pupils (ICILS 2023)	• Annual monitoring reports containing clear recommendations for improvement drawn up or put out to tender	**BZK**, OCW, Digital Society Alliance

1.1 Improve digital skills and knowledge | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
4	As a nation, commit ourselves to improving digital skills **for marginalised groups internationally** (including young people, women and minorities) because an inclusive digital society does not stop at the border		• Women, young people and minorities have better access to digital education • The digital skills of women, young people and minorities have improved • Women and minorities have access to opportunities in the digital economy	**Ministry of Foreign Affairs (BZ)**
5	Add digital literacy to the **curriculum for primary and secondary education**	• Schools providing primary and secondary education receive more support in teaching digital literacy (Basic Skills Master Plan)	• Development of new curriculum attainment targets	**OCW**, Netherlands Institute for Curriculum Development (SLO) and the education world
6	We encourage **the provision of courses for employers and employees**, and approach them proactively	• Promotion and improvement of courses provided for employees to improve digital skills, e.g. through the Social and Economic Council's Lifelong Development (LLO) action agenda and Tel mee met Taal (National Growth Fund *'LLO Collectief Laagopgeleiden en Laaggeletterden'* (Semi-literate and Low-skilled people)) project • The Groenpact Digitalisation and Technology Acceleration programme for green education. Farmers can request advice or take courses using the Agricultural management consulting and education grant module (SABE) • Accessible range of training and retraining courses on topics such as web development, information security, programming and AI for jobseekers and school-leavers	• If the results are positive, the *LLO Collectief Laagopgeleiden en Laaggeletterden* project will continue to run until 2027 • Accessible range of training courses on new technology, etc., available in every labour market region in collaboration with public-private parties (Digital Society Alliance)	**Government-wide**, local or regional authorities, Digital Society Alliance

1.2 **Accessible**, high-quality and proactive service provision | Overview

Social challenge

The government works for everyone. Nevertheless, the current digital services are not fully geared towards citizens' needs and everyday lives. This is because we are not being sufficiently proactive in offering those services; they need to be more user-friendly and accessible.

- At the moment, the initiative to use a particular service lies fully with citizens and businesses. For instance, a study conducted in 2018 revealed that 230,000 senior citizen households might have missed out on their healthcare or housing benefits
- A study by the National Ombudsman shows that citizens struggle to complete digital forms because of complicated language, excessive or superfluous information, or because they can only be completed using an app
- It is sometimes difficult for people to find their way to a government agency, and they receive inadequate help when they have a problem or matters they need to sort out involving multiple government agencies

It is also not currently possible for everyone to do business digitally with a government agency on their own or through someone else. The parents of adult disabled children can find this a challenge, for example.

Results achieved

- The DigiToegankelijk centre of expertise stimulates authorities and agencies to make their websites and apps accessible. It provides advice and insight regarding compliance with the statutory obligation (not all websites and apps satisfy all requirements yet)
- The Generic Digital Infrastructure (GDI) management has been restructured as of 2022. The GDI is funded centrally by the Ministry of the Interior and Kingdom Relations
- There has been a noticeable improvement in services relating to life events such as 'death' (Verification of the National Register of Deceased Persons, Overview and Insight by means of letters for surviving relatives sent by 150 municipal authorities) and 'studying' (financial statements for students)

Goals

1	Citizens and businesses will receive public services that fit their needs and everyday lives. Dutch people living abroad will receive good digital public services. All public service provision will be: • Proactive and organised from the perspective of citizens and businesses, based on life events, among other things • User-friendly, understandable, transparent and accessible to all • Digital where possible and always accompanied by an alternative for those who are unable or unwilling to use the digital option • Customised where necessary, if people are unable to keep up, temporarily or otherwise • Performed as one united government, supported by widely applicable GDI1[1] building blocks
2	Citizens who are unable to keep up with the digital world or are not allowed to act on their own behalf, digitally or otherwise, will be able to have someone represent them for all digital services

Target indicators

→
- By 2024, online public sector information, including the rights and obligations of citizens, must cover all information areas[2] provided for in the EU Single Digital Gateway (SDG) Regulation must be designed in a way such that it satisfies the requirements of that Regulation/the SDG
- Others, yet to be determined

→ Yet to be determined

1. *Generic Digital Infrastructure is a collective term for the digital facilities used government-wide to provide citizens and businesses with services, including an access service (DigiD) and a key register system*

2. *Information areas aimed at citizens and businesses, such as 'citizens' and family rights' and 'taxes'*

1.2 Accessible, high-quality and proactive service provision | Actions

	Description of the action	Result — By the end of 2023	Result — By the end of 2025	Carried out by — By whom, with whom
1	Set up public services in a way that ensures that citizens and businesses can always choose **how they wish to use that service** (click, call, face-to-face)	• A view on the point of contact service (based on the single point of contact concept) with government-wide support • Scaled-up practical initiatives involving various forms of the point of contact service to determine the impact on the organisations involved • Expansion to 600 Digital Government Information Points (including information points outside libraries) and development to private service providers • Framework for accessible and high-quality services (duty of care provided for in the General Administrative Law Act (Algemene Wet Bestuursrecht)) • Implementation of the Electronic Administrative Communications (Modernisation) Act (Wet Modernisering Elektronisch Bestuurlijk Verkeer) to give citizens the right to send digital messages to administrative authorities	• Launch of a digital space to provide government-wide information about public products and services • National roll-out of effective and feasible forms of the point of contact service • Fully digital procedures based on life events (birth, study, work, moving house, retirement, and starting, operating and closing a business) • Creation of a feedback tool to enable implementing organisations to improve service provision • Implementation of the Electronic Administrative Communications (Modernisation) Act (Wmebv) and Single Digital Gateway (SDG) by Water Authorities	**BZK**, government-wide, Association of Netherlands Municipalities (VNG), Digital Society Alliance and fully or semi-private parties with a public function
2	Develop **proactive and transparent service provision** with a focus on one area at a time	• The arrangements for proactive service provision in one area will be worked out in more detail (yet to be determined) • Implementation of the first phase of the MijnZaken Omnichannel project (track & trace) in frontrunner municipalities for information on the delivery status of products and services	• Expansion of proactive service provision to other areas (one a year) • Expansion to include more authorities and agencies	**BZK, Central Judicial Collection Agency (CJIB)**, government-wide, VNG, private parties
3	Improve **user-friendliness, comprehensibility and compliance with the statutory obligation regarding digital accessibility**	• Development of an assessment framework for inclusive service provision • Delivery of a database of models containing easy-to-understand texts • Digital Accessibility Support Scheme (DTO) set up • The 16 most essential government apps made more accessible digitally (implementation of Ceder TK-26643-869 motion)	• Clear Language in Communications Monitor (Monitor begrijpelijke teksten) active • Digital Accessibility supervisory function set up	**BZK**, government-wide, inter-administrative

1.2 Accessible, high-quality and proactive service provision | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
4	Noticeable improvements to services related to **life events**	• Improvements regarding ongoing life events, including 'Turning 18', 'Studying' and 'Starting a business' • Initiate study and improvement actions in one area (to be decided on later)	• Improvements regarding the life events 'having a child', 'employee with debts' and 'sustainable business practice'	**BZK**, government-wide, inter-administrative
5	Modernise the present **Generic Digital Infrastructure (GDI)**: transition from a GDI based on mainly central facilities to a GDI mainly comprising standards and smaller, reusable, open source-based components that all government organisations can use	• Digital Architect appointed for GDI • First GDI programme plan submitted to the Lower House, containing specific agreements, standards and facilities that will be worked on in the coming year, including the accompanying budget. This is part of the Long-Term Programme for Digital Government Infrastructure (MIDO)	• Annual programme plan containing a coherent overview of the GDI building blocks and their development in four areas: access to government services, interaction with the government by citizens and businesses, data exchange between government organisations and infrastructure	**BZK (MIDO)**, other ministries, local or regional authorities, implementing organisations
6	Implement the **Single Digital Gateway (SDG)** to give citizens and businesses easy access to digital public services in the EU	• Information about cross-border government products and services is made available through YourEurope.eu (Annexe I to the SDG) • EU citizens and businesses have access to online procedures (Annexe II to the SDG)	• Assistance services are available online for users requiring assistance with the information and procedures disclosed (Annexe III to the SDG)	**BZK**, government-wide, implementing organisations
7	Increase options for people to have someone **represent them in digital matters**	• Administrators, insolvency practitioners and people with parental authority may conduct business digitally on behalf of someone else • The process enabling people to authorise someone else voluntarily will be continuously improved	• All kinds of legal representatives will be able to conduct business digitally on behalf of those who need them to • All public service providers will be able to link up with the GDI facilities	**BZK**, Ministry of Justice and Security (JenV), Ministry of Health, Welfare and Sport (VWS), VNG, implementing organisations

1.3 Reduce the impact of online disinformation | Overview

Social challenge

Disinformation can deliberately set people on the wrong track and influence their thinking.[1] Disinformation undermines public debate and damages the open economy, public health, national security, mutual trust and trust in public bodies and institutions. More than half of the Dutch population consumes news through major online platforms. Those platforms have revenue models based on personalisation of the services (including information) they provide to citizens. This increases the chance of disinformation being disseminated. For example, sensational content is sometimes given a more prominent place on a platform. The platforms still fail to take sufficient responsibility for reducing the amount of disinformation. It is important to the government that actions of platforms and national and European legislative proposals do not affect fundamental rights, including freedom of expression, but safeguard them instead.

Results achieved

- The Digital Services Act has been developed within the context of the EU and clarifies the responsibilities platforms have in combating criminal and unlawful material among their services
- The EU Code of Practice on Disinformation has been signed by the major platforms and is mandatory. The Code aims to reduce the negative impact of deep fakes, increase collaboration between fact-checkers, increase transparency in political advertising, detect bot networks and provide the scientific community with better access to data
- The 'isdatechzo.nl' website was developed at the behest of the BZK as a means of informing visitors about the impact of fake news and how to identify it

Goals

1	The government stimulates healthy online debate • Review of government-wide disinformation policy • Citizens are familiar with and actively contribute to the creation of disinformation standards • The government ensures that online platforms make active efforts to put their assurances into practice in the implementation of the EU Code of Practice on Disinformation
2	The government supports public media and institutions in developing their own infrastructure and social media environments that satisfy public values to create a more multi-form digital media landscape. Citizens can use those and other alternative platforms • The government stimulates and employs public alternatives to online platforms and services for public institutions that satisfy public values (see goal 3 regarding 'digital commons' within 2.1 'Safeguard public values')

Target indicators

- Government-wide disinformation policy with specific goals shared with the Lower House

- Launch of five new applications for platforms (e.g. PubHubs, a social media platform for public broadcasters, schools, libraries and museums) with at least 10,000 users (see 2.1 'Safeguard public values')

1. *Disinformation is untrue, inaccurate or misleading information intentionally created and disseminated to make money or harm a person, social group, organisation or country. Deep fakes are an example of disinformation*

1.3 Reduce the impact of online disinformation | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	Coordinate Government-wide and inter-administrative **disinformation policy**	• Revise government-wide disinformation policy with specific targets for the end of 2022	• First goals of the disinformation policy have been achieved	**BZK**, JenV, central-government wide, VNG, Association of Provincial Authorities (IPO), Association of Regional Water Authorities (UvW)
2	Organise a broad **social debate** about online standards and behaviour	• Internet users are more aware and resilient with regard to posting and reading online material • Initial debates conducted on an alternative platform that supports public values		**BZK**, JenV
3	Arrange the proper implementation of the **European Digital Services Act (DSA)**	• The government has contributed to the effective monitoring of the DSA, including at the EU level • Central reporting point or knowledge centre established where citizens can easily report unlawful online material and have it assessed (Online Content enforcement) • The government has made agreements with the internet sector on compliance with removal orders with a legal basis • The government has identified the impact of online platforms on democracy and human rights • The implementing legislation required for the DSA for monitoring and enforcement purposes has been created • Structural financing for the monitoring/enforcement of the DSA will have been arranged		**Ministry of Economic Affairs and Climate Policy** (**EZK**) **JenV**, **BZK**, government-wide

1.3 Reduce the impact of online disinformation | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
4	Support the **EU Code of Practice on Disinformation** goals by collaborating with non-governmental parties	• A pilot study on responsible data sharing with scientists has been set up to gain insight into the dissemination and scale of disinformation, e.g. dark patterns and the level of protection for children • Initiatives to make more reliable content more visible and guarantee authenticity (proof of provenance), e.g. through the use of digital signatures for tweets[1] are being encouraged • Researchers have access to platforms' online data • Monitoring of implementation by EU Commission • Reduction of the impact of negative deep fakes, collaboration among fact-checkers (e.g. through BENEDMO[2]), transparent political advertising and detection of bot networks through the EU Code of Practice on Disinformation	• Pilot study on responsible data sharing has been completed • Continuation of the reduction of the impact of negative deep fakes, collaboration among fact-checkers, transparent political advertising and detection of bot networks through the EU Code of Practice on Disinformation	**BZK**, government-wide, scientific community
5	Encourage and utilise **secure public or private alternatives** to online platforms and services provided by public institutions that satisfy public values	• Result of the government study on encouraging open public algorithms to identify disinformation • See 2.1 'Safeguard public values'	• See 2.1 'Safeguard public values'	**BZK**, government-wide, VNG, IPO, UvW

1. *The Twid project is working on a proof-of-concept for a browser plug-in which can add information to Twitter to demonstrate the authenticity of a message and an account*
2. *Benelux European Digital Media Observatory, Flemish-Dutch cooperation against disinformation*

1.4 Support EU and national regulations and implementation cohesively | Overview

Social challenge

Developments within our society and economy have accelerated the digital transition. In many cases, the issues involved transcend national borders. This has prompted a host of new legislation from the EU, including the Accessibility Act, Digital Services Act, Digital Markets Act, Data Act, eIDAS Regulation and AI Act. However, that new legislation does not always fit in with the Dutch situation and makes heavy demands on authorities and agencies, businesses and supervisory authorities:

- EU legislation does not always align with Dutch practice. Where that is the case, we must make sure that Dutch practice aligns with European rules so that the objectives behind those rules are achieved
- Complying with all new legislation is a tall order. The assistance provided for authorities and agencies, businesses and entrepreneurs with the implementation of legislation remains inadequate
- The supervision of EU legislation and regulations on digitalisation varies widely, and responsibility for that supervision has not yet been clearly assigned

Results achieved

- EU Directive on digital accessibility has been implemented in authorities and agencies, and a support network has been established for it (Expertise Centre for Digital Accessibility)
- Cooperation between BZK, JenV and EZAK on the EU legislation agenda is ongoing
- Document providing insight into/an overview of EU legislation prepared with the Netherlands Enterprise Agency (RVO)
- Europa Decentraal with funding guide
- Start of co-financing fund, including funding from CLAIRE (Confederation of Laboratories for Artificial Intelligence Research in Europe), funding of the Dutch share in Blockchain infrastructure and formation of the Dutch Societal Innovation Hub in cooperation with the Ministry of Economic Affairs and Climate Policy
- Supervisory authorities are consulting digitally

Goals

			Target indicators
1	The Netherlands contributes public values, fundamental rights and implementability during the creation of new EU legislation and regulations	→	• Public values, fundamental rights and implementability are included in all regulations
2	Authorities and agencies, businesses and entrepreneurs receive support to understand and implement EU legislation on digitalisation	→	• There is an implementation framework for every piece of EU legislation on digitalisation
3	Supervision of EU legislation and regulations is organised in an understandable and targeted fashion and supports the implementation	→	• Supervision is arranged for EU legislation and regulations

1.4 Support EU and national regulations and implementation cohesively | Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1 **Implementability** for private and public parties, including monitoring and enforcement, and making public values a structural part of **European contribution**. In doing so, we focus on clarity and consistency for users by proactively participating in preliminary European processes in which implementing organisations are involved	• We have identified which processes the Netherlands is committed to that will run until the end of 2025 under the EU's Digitalisation and AI Strategy. The parties concerned have been identified • Digitalisation advisory group for value tensions when new national or EU legislation is introduced (see 2.1 'Safeguard public values')	• The Netherlands will align EU legislation effectively with Dutch practice • The Netherlands will seek alignment with the EU Cybersecurity Strategy, the Council Conclusions on the EU's cyber posture, the Strategic Compass, and the Council Conclusions on EU digital diplomacy.	**BZK, EZK, JenV, Ministry of Foreign Affairs (BZ)** and other ministries
2 Set up additional support **tools for the implementation of EU legislation**, in coordination with supervisory authorities and the private sector	• To be fleshed out later		**BZK**, **EZK**, **JenV**, other ministries, authorities and agencies, including local or regional authorities, VNG, IPO, implementing organisations, supervisory authorities and private parties
3 Expand the 'Digital Europe Hub' knowledge centre to encourage **knowledge exchange among sectors** and assist with implementation	• Information platform set up and staffed jointly with the RVO, ICTU and Europa Decentraal • Co-financing arranged for the Dutch Societal Innovation Hub (DSIH), GovTech Incubator and AI Testing and Experimental facilities		**BZK**, EZK, local or regional authorities, Europa Decentraal, RVO and ICTU
4 Arrange effective **supervision** of EU legislation and regulations on digitalisation		• Responsibility for the supervision of EU legislation is clearly assigned	**BZK**, **EZK**, **JenV**, other ministries, authorities and agencies, including local or regional authorities

2 Everyone will be able to *trust* the digital world

2.1 Safeguard public values | Overview

Social challenge

Public values are the foundation of a responsible digital transition. Digitalisation can lead to the online violation of public values, including human dignity, autonomy and non-discrimination. The concentration of market power is a present danger. It is unclear what values and standards apply online or how they are protected. There is no shared conceptual framework of important public values that should be considered in the digital transition. The standards in place for children's rights online, gaming and gambling remain inadequate. Citizens and public organisations are over-reliant on private platforms for public activities such as education, research, healthcare, art and culture, while those platforms do not always behave in a publicly responsible way.

Results achieved

- The IAMA (human rights test) has been developed for discussion and decision-making concerning the use of algorithms by government agencies
- New rules on ensuring public values online (DSA, DMA, DGA, DA, AI Act and the GDPR) are being negotiated at the European level
- It is estimated that the interoperability of messaging services will be mandatory through the Digital Markets Act (DMA) from 2024
- Online marketing aimed at children is prohibited on the major platforms
- At the European level, the BIK+ (Better Internet for Kids) has been developed. It contains actions that Member States can take to protect children online
- Inter-administrative procurement conditions have been developed that enable us to put ethics and public values into practice in government procurement and tendering
- €20 million from the Human Rights Fund will be set aside annually until 2027 to increase the online and offline safety of human rights defenders throughout the world

Goals

1	There is an awareness and shared understanding of the public values ensured during the digital transition and the standards that must be applied in the process. We work with public institutions on a shared conceptual framework, quality mark or statutory obligation for public values and technology. We are organising the debate on value tensions and 'the kind of digital world in which we want to live', including citizens, businesses and social organisations in the process
2	Citizens and businesses see that the government is setting and enforcing clear limits when protecting public values and human rights online, both in the Netherlands and internationally. We will protect particularly vulnerable groups such as children and socio-economically vulnerable people, including in online gaming and gambling
3	The public core of the internet will be strengthened and expanded. Citizens, businesses and public employees will be able to use secure public or private alternatives to online platforms and services provided by public institutions. Those services will be interoperable with others and developed open-source as 'digital commons'[1]. The Netherlands will support the use of the DMA to oblige companies with a gatekeeper function to ensure interoperability because this will combat market power and make public alternatives more viable

Target indicators

- We will have an inter-administratively shared system of standards and conceptual framework for public values for digitalisation

- Yet to be determined

- Identify and support five 'digital commons', such as an algorithm that can be used to identify problem behaviour online, age verification for children or the further development of open encryption

1. *Information and knowledge sources that are created jointly and owned or shared between a community and are usually freely available to third parties*

2.1 Safeguard public values | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	Develop a **mandatory quality mark** for public values and technology for public institutions that is to be used over five years in all public digital invitations to tender and made available to private parties	• The quality mark should be developed by public institutions • Integrated Assessment Framework (IAK) modified after implementation test • Procurement conditions have been drawn up to safeguard public values and ethics in government procurement and tendering in cooperation with the Association of Netherlands Municipalities (VNG)	• The quality mark will be used by public institutions • Exploratory study on legal embodiment through obligation • The quality mark will be used by private parties	**Ministry of the Interior and Kingdom Relations** (**BZK**), all other ministries, at the inter-administrative level, implementing organisations, the business community
2	Conduct continuous **human rights impact assessments** on digital services with a substantial impact on citizens	• Publication by the government of human rights impact assessment on digital services with a substantial impact on citizens • Development of a public cloud or fixed supply agreements with parties that satisfy public values	• Publication by the government of human rights impact assessment on digital services with a substantial impact on citizens	**BZK**, authorities and government agencies
3	Organise the **debate on value tensions** on a continuous basis on a fixed platform with authority, such as the advisory group on digitalisation	• Exploratory study on a possible role involving the Social and Economic Council (SER) in the public debate on public values and the assessment of public values in situations where tension may arise • See 1.3 'Reduce the impact of online disinformation'	• See 1.3 'Reduce the impact of online disinformation'	**BZK, SER,** all other ministries, at inter-administrative level
4	Set clearer **standards and limits** for online gaming and gambling	• Guide for gamers showing how to identify seduction techniques in games, public information on the effects of spending a long time online, and a tech-etiquette guide including online dos and don'ts have been drawn up		**BZK**, Ministry of Education, Culture and Science (OCW), Ministry of Economic Affairs and Climate Policy (EZK) and Ministry of Justice and Security (JenV)

2.1 Safeguard public values | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
5	Protect **children's rights online** and protect children from and empower them to deal with harmful content[1]	• Plan and schedule drawn up for the implementation of BIK+ activities (awareness-raising, knowledge sharing and code of conduct for age-appropriate design) • Further development of the Children's Rights Online Code and exploration of a statutory obligation • The usability of the Children's Rights Online Code will have increased • Children's rights impact assessment (KIA) carried out and decision on exploration of statutory obligation • Assistance with the use and application of age verification tools • Improvement methods identified for enforcement and supervision in the area of children's rights • Awareness-raising campaigns conducted aimed at protecting children from harmful content • User-friendly parental control tools, advert filters and blocking tools are built into all electronic devices and installed in devices in public spaces (including schools, libraries and youth clubs)		**BZK, OCW, Ministry of Health, Welfare and Sport (VWS), EZK and JenV**
6	Strengthen **civil-society organisations**, in particular in Africa and the MENO region countries, to hold governments and regulatory bodies accountable for ensuring people-oriented online values and rights	• Strengthen civil-society organisations that defend the rights and interests of citizens, including diaspora organisations, religious actors, faith-based organisations, cultural institutions and trade unions		**Ministry of Foreign Affairs (BZ)**

1. *This partially answers the motion by members Cedar and Bontenbal to discuss the Parliamentary Assembly's recommendations to improve the level of protection of children. You will receive a parliamentary letter on children's rights online in which we explain the level of protection of children from extreme content*

2.1 Safeguard public values | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
7	Strengthen **'digital commons'**	• Five 'digital commons' will be identified and supported for open-source development		**BZK, VNG**
8	Develop a **digital public social medium** (PubHubs) for all public institutions and citizens that meets the highest standards for public values	• The first PubHubs put into use and public organisations assisted in the development of alternatives • Pol.is network democracy applied to three cases for the government and for new developments covered by this work agenda	• Alternative algorithms have been offered to social media organisations	**BZK to provide encouragement**, Public Spaces/public parties
9	Make **interoperability** mandatory for companies with a gatekeeper function using the DMA (Digital Market Act); this is part of the Digital Economy strategy	• Stimulation of interoperability solutions by BZK	• The DMA will enter into effect in early 2023 and will probably be mandatory from 2024. Under the DMA, gatekeepers must make number-independent interpersonal electronic communication services (including messaging apps) interoperable with other providers if they so request	**EZK**, BZK

2.2 Safeguard privacy, responsible data use and increase transparency regarding data processing and exchange | Overview

Social challenge

Privacy plays a key role in citizens' trust in a digital government and society. Lawful data processing ensures trust. Various pieces of EU legislation, including the GDPR, lay a solid foundation for protecting privacy online, but the implementation of that and upcoming new legislation is complex.

The government still too often collects data unnecessarily and remains insufficiently transparent about data processing and exchange by public sector organisations. This has the effect of reducing citizens' trust in the government.

Results achieved

- The Responsible Data Use Advisory Function (part of the inter-administrative data strategy) has been set up and has provided advice on six cases as regards what is technically possible, permitted by law and ethically desirable when it comes to data use
- Broader obligation under the GDPR for organisations to carry out Data Protection Impact Assessments (DPIAs) to reduce the privacy risks of data processing
- Tightening of regulations on the processing of special personal data and micro-targeting through the Digital Services Act

Goals

			Target indicators
1	Citizens can rely on all[1] authorities and government agencies acting in accordance with the GDPR • We will be better able to gather information about government data exchanges (open data sharing) • The legitimacy of existing digital systems in terms of legal and other principles that are safeguarded (open policy) can be explained • Authorities apply privacy-by-design[2] • We do not use facial recognition without a legal framework and checks	→	• Yet to be determined
2	Authorities and government agencies have adequate levels of knowledge and capacity in the area of privacy • Civil servants feel that they receive sufficient assistance to enable them to handle data responsibly and apply privacy standards correctly in the process • Public sector organisations receive assistance in responsible data use and privacy	→	• Yet to be determined
3	The government clarifies the privacy frameworks for citizens and businesses and increases oversight • The government is transparent about responsible data use (open processing registers) • Strengthening of online privacy, e.g. through the e-Privacy Directive and the implementation of the various European frameworks • Invest in strengthening the position of the Dutch Data Protection Authority (AP) and the relationship between digital supervisory authorities	→	• Coverage of the GDPR processing register • Other - yet to be determined

1. *If applicable, with statutory exceptions*
2. *Such as a design resulting from purpose limitation, data minimisation and data masking*

2.2 Safeguard privacy, responsible data use and increase transparency regarding data processing and exchange | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	**Investigate the extent to which the GDPR could be improved** by public sector organisations. Public sector organisations receive assistance in the area of responsible data use and privacy	• Insight into the extent to which public sector organisations fail to adhere to the GDPR • Policy response to the Research and Documentation Centre (WODC) study • Exploratory study on the possibility of strengthening the position and competencies of DPOs and setting up a DPO register and quality requirements for the government • Exploratory study on the possibility of introducing Chief Privacy Officers at ministries • Development of a training course within the Senior Civil Service for managers in the area of privacy		**JenV, BZK**
2	Create **clarity within authorities and government agencies** about what is technically possible, permitted by law and ethically desirable when it comes to data use	• The Advisory function for responsible data use will continue to advise on cases • Increased certainty of action (through CPO positioning and Dutch Data Protection Authority (AP) cooperation) • Exploratory study on the usefulness of and need for a privacy helpdesk • Guide on the use of online material for municipal authorities	• The Advisory function for responsible data use will continue to advise on cases	**BZK, implementing organisations, JenV,** all other ministries, VNG, the Association of Provincial Authorities (IPO), the Association of Regional Water Authorities (UvW)
3	Develop and continually gather information about the government architecture for a **federated data system** with a central anonymisation function	• National Innovation Centre for Privacy Enhancing Technologies (NICPET) has been launched • A roadmap for the development of data architecture has been prepared • See 4.1 'Improve information management for open government'	• See 4.1 'Improve information management for open government'	**BZK** (for NICPET), **all other ministries**, the VNG, IPO, UvW and implementing organisations
4	Reinforce data processing **supervisory authorities** and strengthen cooperation between supervisory authorities	• Additional investments in digital supervisory authorities and cooperation on digital supervision • Promote privacy innovations	• Standardised disclosure of the AP's decisions • See 3.3 'Regulate algorithms'	**BZK** (for algorithms), **JenV** (for the GDPR), **EZK**
5	Investigate the future-proofness of the **basic privacy and information rights** under the Constitution	• See 4.1 'Improve information management for open government'	• List of necessary legislative changes by the Department for Constitutional Matters and Legislation (CZW) • See 4.1 'Improve information management for open government'	**BZK** (Legislation and Legal Affairs Department (DWJZ)), JenV

2.3 Prepare for new digital technology | Overview

Social challenge

New digital technologies present opportunities and risks for society. Digitalisation can contribute to improving sustainability, better healthcare and better choices in spatial design. At the same time, 43 per cent of people in the Netherlands indicate that the introduction of new digital technology and innovations can make them feel uneasy or anxious.[1] Furthermore, not everyone will be equally capable of understanding and making the most of new advanced services, such as autonomous systems.[2] At present, we are over-reliant on digital technology developed by businesses in countries that do not necessarily share our public values. The government cannot intervene effectively and on time when new digital technologies have a significant and, in particular, negative impact on public values. This means that the government does not always strike the right balance between boosting or regulating the development and impact of new digital technology.

Results achieved

- The Ethically Responsible Innovation Toolbox has been developed and provides points of reference for citizens and businesses developing or using new digital technologies, and assists authorities and government agencies in ethically responsible innovation through models, methodologies, guidelines and practical examples
- The second Public Spaces conference was organised in 2022
- The Agriculture, Water and Food Knowledge and Innovation programme was developed, in which Agriculture & Food and Horticulture & Propagating Materials departments collaborate with the Water & Maritime department. In collaboration with farmers, suppliers and knowledge institutions, farmyard innovations have been and are being developed in the National Experimental Garden for Precision Farming project

Goals

			Target indicators
1	The Netherlands is a frontrunner in the development and use of responsible digital technology. We must be able to develop new digital technologies in accordance with the values of democracy and the rule of law in Europe and beyond. Digitalisation and measures taken to improve sustainability must be mutually reinforcing	➜	• Yet to be determined, in the elaboration of the Digital Economy strategy
2	Citizens and businesses see the government draw up standards and framework conditions in time to steer new technology in the right direction. The government is capable of regulating or boosting new digital technologies when they affect public values	➜	• By 2025, technology-neutral conditions[3] and an impact assessment will have been developed for public values that authorities and government agencies can apply to new digital technologies relevant in the public domain • Several 'ethical leaflets' developed in the Ethically Responsible Innovation Toolbox and applied at the inter-administrative level when new digital technologies are used (target value: all authorities and government agencies and local or regional authorities)
3	Knowledge institutions, businesses and authorities and government agencies are involved at the right time in developing, using and scaling new digital technologies. This will enable us to formulate and mitigate future opportunities and risks	➜	• Number of labs where the government and social actors cooperate on the development of new digital technology to solve social problems (target value: 3)

1. *VMWare 2022*
2. *Digitalisation in 2030 Foresight Study*
3. *Technology-neutral conditions in line with the quality mark and/or a statutory obligation for public values and technology*

2.3 Prepare for new digital technology | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	Draw up a **policy agenda** for public values and new digital technology (with clear frameworks for the impact of new digital technologies on public values)	• The first policy agenda has been drawn up and coordinated with parties such as the National Innovation Community or the CIO consultation group • The annual international congress on public values and preparing for new digital technology has been organised and cohesion between the various congresses created (i-government, cybersecurity congress, etc.) • Exploratory study on the possibility of forming a 'digitalisation advisory group' (see also 2.1 'Safeguard public values') • Government-wide legislative agenda for digitalisation (and therefore also for the development and use of digital technology), as recommended by The Netherlands Scientific Council for Government Policy (WRR), has been prepared	• Initial goals from the policy agenda for public values and technology have been achieved • Further development of the policy agenda	**BZK**, **JenV**, **EZK**, other ministries and at inter-administrative level (VNG, IPO and UvW)
2	Use new digital technology for **public service provision**	• First self-created or promoted public or non-public secure alternatives to online platforms and services provided by public institutions have been developed (see also 1.2 'Accessible, high-quality and proactive service provision' and 2.1 'Safeguard public values')	• Secure public or private alternatives to online platforms and services provided by public institutions developed further	**BZK**, EZK, OCW, scientific community and public-private partnership

2.3 Prepare for new digital technology | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
3	The Netherlands is boosting the sustainability and **digitalisation transition** abroad, focusing on strengthening SMEs	• The first steps have been taken towards supporting fair digital platforms and services for farmers and male and female entrepreneurs to increase opportunities in fintech and e-commerce • Increase the Netherlands' commitment to improving online access to reliable data, information and media sources internationally, including in developing countries	• Support developed further	**BZ, Foreign Trade and Development Cooperation (BHOS), Netherlands Enterprise Agency (RVO)**

2.4 **Strengthen cybersecurity** | Overview

Social challenge

The absence of basic measures means that the government is lagging as far as digital resilience is concerned (Cybersecurity Picture 2022), making it a promising target for malicious persons (state and criminal).

It is our social responsibility to capitalise safely on the economic and social opportunities provided by digitalisation and protect our security and public values at the same time. Cybersecurity is an essential prerequisite for successful digitalisation.

As part of this wide-ranging social responsibility, it is the government's job to set a good example and handle citizens' data securely.

Results achieved

- For essential providers and major providers, the Revision of the European Network and Information Security Directive (NIS2) means
- a statutory obligation for information security, reporting of high-impact incidents and a supervisory regime. JenV is responsible for the EU process and implementation in Dutch legislation. BZK is responsible for the public sector and legislation directed at local or regional authorities
- Work is already taking place with local or regional authorities on the preparation of legislation and regulations, appropriate supervision and reducing the cybersecurity audit burden imposed by the government on local or regional authorities
- The secure procurement of ICT products and
- services is encouraged through the use of government-wide sets of standards
- The government continues to assist and facilitate the Government-wide Cybersecurity Exercise and the Information Security & Privacy service persistently
- Strengthening digital resilience is one of the road maps to be implemented in the Government I-Strategy 2022 – 2025 (I-strategie Rijk 2022 – 2025)
- Publication of the proposed Cyber Resilience Act, containing security requirements for the entire life cycle and ICT supply chain

Goals[1]

1	The Netherlands is able to capitalise safely on the economic and social opportunities provided by digitalisation and protect our security and public values at the same time
2	Authorities and government agencies meet the prescribed security requirements applicable to them
3	Authorities and government agencies only use and purchase secure ICT products and services from the market
4	Authorities and government agencies will use a uniform domain name extension so that citizens can tell whether they are really dealing with an authority or government agency online. Citizens have a point of contact for questions about the authenticity of a government site/email/app
5	All authorities or government agencies are practised in preventing cyber incidents and assisted by government professionals through the 'Information Security & Privacy' help function

Target indicators

- Yet to be determined

- Yet to be determined

- Percentage of public sector organisations that have introduced sets of standards for information security, such as the Government information security baseline (BIO) (target value: 100%)
- Percentage of tendering procedures and procurement of ICT products and services that meet the government's cybersecurity procurement requirements (target value: 100%)

- Yet to be determined

- Percentage of public sector organisations that regularly (at least annually) carry out drills using simulated hack attacks (target value: 100%)

1. The government is committed to strengthening cybersecurity through the Netherlands Cybersecurity Strategy (NLCS), coordinated by the Minister of Justice and Security. The government's commitment is elaborated in the NLCS action plan and reported on periodically. The main actions and specific rules relating to public values are included in the actions for this priority

2.4 Strengthen cybersecurity | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	Introduce a **statutory duty of care** for information security, **a duty to report** and **a supervisory regime** for the entire government The aim is to reduce the audit burden (created by the multitude of rules set by the government for local or regional authorities as regards cybersecurity) by harmonising legislation	• The implementation of the BIO support programme has been updated for the entire government by the Centre for Information Security and Privacy (CIP) • The accountability system ENSIA (Single Information Audit Unified Norm) has been developed further. Steps have been taken to organise horizontal and vertical supervision using the BIO as a basis, helping municipal authorities work on improving information security and facilitating democratic accountability for information security • A revised BIO is in place • Pilots have been conducted to establish the added value of IT reports and IT audit statements within the government, similar to standard financial annual reports. The exploratory study connects with pilots conducted in the business community • Exploration of the possibility of making open-source tools available to local or regional authorities to support information security implementation	• The Government information security baseline (BIO) has been laid down in statute • An additional set of requirements has been developed for key digital processes and systems used by the government • Implementation of the revised European Network and Information Security Directive (NIS2) in Dutch legislation • Reduced cybersecurity audit burden for local or regional authorities through harmonisation of legislation • Supervision has been organised • Indicators that measure ambition regarding the security of public sector organisations are monitored and displayed on the basisbeveiliging.nl site, developed and managed by the Centre for Information Security and Privacy (CIP). The entire government can take them as a model and see how the government is developing as regards the indicators concerned	**BZK**, JenV, various ministries, local or regional authorities, CIP
2	Coordinating the government-wide strategy for **international cyber policy** is part of the International Cyber Strategy (not yet brought into operation)	• Coordination of activities in line with the international Cyber strategy on international security, human rights and the rule of law online and linking digitalisation and security		**BZ, EZK**, JenV, BZK, DEF, local or regional authorities and government services (General Intelligence and Security Service (AIVD), Military Intelligence and Security Service (MIVD), National Cybersecurity Centre (NCSC), National Coordinator for Security and Counterterrorism (NCTV), Public Prosecution Service (OM) and the National Police)

2.4 Strengthen cybersecurity | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
3	The government only purchases **secure ICT products and services**	• The Government Cybersecurity Procurement Requirements (ICO) tool has been developed further, broadened and implemented (including further development of government-wide sets of requirements) • Indirect positive influencing of the market to supply secure products and services	• Legislation ensures that authorities are required to use the sets of standards for secure procurement • European schemes have been included in the national Government Cybersecurity Procurement Requirements (ICO) in accordance with the EU Cybersecurity Act (CSA) certification schemes	**BZK**, EZK, local or regional authorities, CIP
4	Provide **own domain**s (e.g. overheid.nl; the precise extension to be used is being explored with the Ministry of General Affairs (AZ)) to make it easier for citizens to identify reliable websites	• Transition plan for government domain extensions • Provision of government-wide extension for public authorities • Extension used for the first time	• Extension used government-wide	**BZK**, AZ
5	Set up **point of contact** where citizens and businesses can ask questions about the security of government websites	• Point of contact established where citizens and businesses can ask questions about the security of government websites from 2023		**BZK**, AZ/DPC, Netherlands Publication Office (KOOP)
6	Facilitate **annual government-wide** drills using simulated hack attacks and prepare a government-wide annual test calendar for red teaming (from the I-Strategie Rijk)	• Annual government-wide cyber drill using simulated hack attacks • An option has been developed enabling drills to be conducted simultaneously • Delivery of Red Teaming Toolkit • Start of the implementation of red team tests by ministries • Inter-ministerial knowledge-sharing organised	• Authorities and government agencies participate actively and conduct drills with their own crisis organisations on a structural basis • Experiences with hacking attacks will be shared widely within the government to ensure continuous learning • Annual test calendar for red teaming • The knowledge gained from the government process has been made available to local or regional authorities	**BZK, JenV**
7	Provide a **help function** concerning information security and privacy for authorities and government agencies	• The CIP has taken steps to extend and update the expansion and further development of the Information Security & Privacy service. The first authorities or government agencies receive customised recommendations from professionals within the government about digital security and privacy. This ensures readily accessible assistance from organisations with specific expertise for organisations with inadequate knowledge in the area of information security	• Authorities and government agencies know how to find the Information Security & Privacy service, and it has been developed into a platform by and for government professionals who can support each other	**BZK**

3   Everyone will have *control* of their digital lives

3.1 Control of your own data | Overview

👥 Social challenge

Digitalisation has increased the importance of personal data, yet citizens have hardly any control over it. Their information position has weakened as a result. Having autonomy and being able to control our data and identities is a crucial part of the foundation of our digital world.
Every citizen must be able to view, correct and reuse their data held by the government and businesses wherever possible[1]. You must also be able to decide with whom you share your data without having someone looking over your shoulder. The government must set the frameworks to allow control of data and must set a good example.

📊 Results achieved

- A platform has been established to enable lessons learned and ways of controlling data to be shared within the public and private sectors (rog.pleio.nl)
- Using MijnOverheid, citizens can see which of their data are stored by a number of public sector organisations
- Using MijnOverheid.nl, citizens can see which organisations can view data in the Personal Records Database (BRP) and which organisations are notified when changes are made to it
- The first version of agreements on the Control of Data (Regie op Gegevens) system and reference architecture is available
- The national roll-out of a system for inspection of personal data processing for 600 government decisions of relevance to citizens has begun

🎯 Goals

1	Citizens and businesses are given the right and ability to use their data digitally, including the ability to inspect their data and share it digitally, e.g. using an ID wallet (see 3.2 'High-quality identity system including login tools and a wallet')
2	Citizens and businesses have the right to inspect all1 data that have been used for a government decision that specifically affects them
3	As of 2025, it will be easy for citizens and businesses to correct data held by the government

⏱ Target indicators

➜
- Number of authorities and government agencies using a standard API allowing data to be retrieved at a local level and displayed to citizens in various environments (target value: wherever possible[1])
- Citizens can view the provision of data from the 15 most important government sources
- Citizens can decide to share data from the Personal Records Database (BRP) with the "*Stichting Interkerkelijke Ledenadministratie (SILA)*", the Inter-Church Membership Records Foundation

➜
- Number of government decisions for which people can see in a single location what type of data the government used for various government decisions by 2024 (target value: 600 government decisions)
- Number of personalised government decisions for which citizens can see which of their specific personal data were used (target value: for the 20-25 most important decisions)

➜
- Annual report by the Reporting Centre for Errors in Government Records to the Lower House

1. *Limited by statutory or justified exceptions that apply when weighing interests in the context of investigations, law enforcement, Ministry of Defence, intelligence gathering, etc.*

3.1 Control of your own data | Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1 Provide insight into **which data the government uses to reach a decision**	• Impact analysis of the proposal to provide an overview of the type of data used for 600 types of decisions	• Overview of the type of data used for 600 types of decisions • Citizens can see which of their specific personal data were used for the 20-25 most important personalised government decisions • Authorities and government agencies use a standard API	**Ministry of the Interior and Kingdom Relations (BZK)**, local or regional authorities and all implementing organisations that draw up decisions
2 Collaborate with housing associations **to share income data** through MijnOverheid.nl, with the permission of the citizen concerned	• Thirty housing associations have joined	• All housing associations have joined	**BZK**, housing associations, BZK Wonen, Aedes
3 Develop **Personal Health Environments** (PGOs)	• PGOs allow data to be retrieved	• PGOs widely used in society	**Ministry of Health, Welfare and Sport (VWS)**, BZK, healthcare sector
4 **Inform** people about the **retrieval and use of their data** from **key registers** of relevance to citizens and businesses by the government and non-government data consumers	• In addition to alerts from the BRP, a further two government sources will have made data provision transparent	• Unambiguous and easy inspection of all data provided from key registers	**BZK**, local or regional authorities, Logius, source holders
5 Embed **frameworks and rules for the digital sharing of data with organisations** with a statutory task	• Proposal for amendment of the Digital Government Act (Wet Digital Overheid)	• A statutory basis for the frameworks and rules for the digital sharing of data	**BZK** and local or regional authorities
6 Collaborate with Zorgeloos Vastgoed and Digicampus to **simplify house buying**	• First government sources available to make buying a house a more user-friendly experience • Initial experiences and solutions copied to other sectors (open information)	• All government sources available to make buying a house a more user-friendly experience • Initial experiences and solutions widely adopted in other sectors (open information)	T**o be determined later**, local or regional authorities, BZK Wonen, Royal Dutch Association of Civil-law Notaries (KNB), Land Registry Office, Tax and Customs Administration

3.1 Control of your own data | Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
7 Develop an **overview that makes debts (claims) to the government clear** to citizens and businesses and provide citizens easy access to their debt data	• First version of a digital overview of liabilities and debts to the government is available	• Expansion of the overview to include more authorities and government agencies that show claims and debts in a single location	**Ministry of Social Affairs and Employment (SZW), Ministry of Justice and Security (JenV), Central Judicial Collection Agency (CJIB)**, local or regional authorities, Tax and Customs Administration, Employee Insurance Agency (UWV), Education Implementation Service (DUO), Social Insurance Bank (SVB), Netherlands Enterprise Agency (RVO)

Note: All activities aimed at gaining control of your data using an ID wallet fall under action track 3.2

3.2 High-quality identity system including login tools and a wallet | Overview

Social challenge

The social challenges surrounding the digital identity system involve making it easier, more reliable and more privacy-friendly to do business digitally.

- Service provision entails unnecessarily high administrative burdens for citizens and businesses. In addition, countless organisations store citizens' data that citizens cannot later obtain to use elsewhere. Examples include taking out a mortgage, which requires the retrieval of data from various agencies to provide proof
- The assurance level when logging in or sharing data is often inadequate when citizens do business. For instance, a high assurance level is not always requested for medical data

Results achieved

- Digital Government Act bill (expected to take effect in 2023). The Digital Government Act (Wdo) stipulates that Dutch citizens and businesses must be able to log in to public or semi-public sector organisations securely and reliably. Under the Wdo, people have a choice of login method
- DigiD is widely used and enjoys a high level of user satisfaction
- The Netherlands' efforts in negotiations on the European Digital Identity Framework (eIDAS revision) appear to be successful. The aspects involved include the unique identifier, assurance level and attention to risks
- The Netherlands is a leading country when it comes to public, private and scientific developments in digital identity (IRMA, MedMij, Datakeeper, Mobiel Rijbewijs (Mobile Driving Licence), Vastgoed wallets (Property wallets), vID, MijnGegevens, QTSP adoption)

Goals

1	The system for access to digital government services will be expanded to enable private parties to provide identification services while maintaining citizen privacy. This enables people to use login tools in the public and private sectors. The government will also provide a public login tool for businesses
2	Citizens can rely on service providers requesting login tools publicly and privately with an appropriate assurance level to do business securely and reliably
3	The Dutch population has the option to use an ID wallet safely and in a privacy-friendly, accessible and reliable way, making it easier to do business digitally (e.g. logging in, data sharing, signatures and local authorisation management)

Target indicators

- Number of DigiD alternatives approved for the access system and made usable for citizens as a login tool (target value: multiple alternatives)
- Implementation of the Digital Government Act

- Number of service providers in the public sector using the login assurance level required for the specific service provided (EU eIDAS Regulation) (target value: all services providers use the correct assurance level)

- A reliable, open-source, public example wallet (ID wallet) that citizens can use for as many services as possible (public and private)

3.2 High-quality identity system including login tools and a wallet | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	Draw up a **European Digital Identity Framework** (revision of the eIDAS Regulation)	• European Digital Identity Framework prepared and legislation laid down (revision of the EU eIDAS Regulation)	• Date set for implementation of Dutch legislation	**BZK**, **Ministry of Economic Affairs and Climate Policy (EZK), EC**
2	Develop **Dutch public open source wallet** with the highest requirements for data protection, information security and accessibility	• First example available • Participation of all authorities and government agencies organised	• Every Dutch person can use a high-quality wallet containing, among other things, diplomas, driving licences, ID documents, identity cards for visitors to State institutions, certificates of succession and healthcare data starting with the European Health Insurance Card (EHIC). Such wallets can be used publicly and privately	**BZK**, VWS, OCW, Ministry of Infrastructure and Water Management (IenW), KNB, Logius, National Office for Identity Data (RvIG), ICTU foundation, Netherlands Vehicle Authority (RDW), DUO, AT, local or regional authorities
3	Forms of **digital access system** (eID means of access)	• Digital access system in force and the first >1 of private means of access approved by the regulator • Development of public login tools for businesses	• Every Dutch citizen can use a variety of approved login tools in a user-friendly, secure and reliable way	**BZK**, Logius, RviG, various implementers + local or regional authorities
4	Introduce technical and legal innovations to enable people to retrieve **data from the government** and **share them** with others	• Legislative procedure started to enable data sharing through wallets		**BZK**
5	Participate as a country in **large-scale European pilots involving ID wallets**	• The Netherlands participates in three large-scale European pilots that enable business to be conducted across borders using ID wallets	• Three large-scale pilots successfully completed, resulting in an improved EU infrastructure within which business can be done using ID wallets and a better understanding of the opportunities and risks among the public	**BZK, IenW, OCW,** RDW, RviG, ICTU, DUO, Radiocommunications Agency Netherlands (AT)
6	Set a standard for **login tools** with the **correct assurance level (eIDAS)** in the public sector	• Baseline measurement: number of public services with the correct assurance level	• Open overview and supervision: no more public services available with insufficient assurance levels	**BZK**, all implementing organisations and local or regional authorities that draw up decisions
7	Set up a **Dutch approval system for ID wallets** that satisfy the public values that are important in the Netherlands	• First system architecture prepared • First set of requirements for approval drawn up	• Uniform assessment framework prepared for wallets for accreditation as recognised ID wallets	**BZK, AT**, parties providing wallets and service providers

3.3 Regulate algorithms | Overview

Social challenge

Having control over your digital life means being able to rely on digital systems, including algorithms, satisfying public values and understanding how they work. This is not yet a given for businesses and the government.

- It is not sufficiently clear to society which standards, based on public values, should be guaranteed for algorithms. For instance, the Tax and Customs Administration used a self-learning algorithm for benefit fraud detection that makes selections based on income, giving a higher risk score for low incomes
- The algorithms used by the government are not always transparent, meaning that citizens sometimes see the digital world as a 'black box'. Examples include the algorithm that determines whether the occupancy of an address should be investigated. It must be possible to explain an algorithm's output

Results achieved

- Digital (AI) awareness tools: AI Parade (available at Dutch libraries)
- The Dutch contribution to the EU's AI Act has resulted in human rights featuring more prominently in risk assessments for high-risk AI systems and supplementary measures that strengthen transparency and the rights of natural persons
- ELSA labs (ethical, legal, societal aspects) for people-oriented AI have been launched, in which participants collaborate to produce algorithms that satisfy human rights and public values

Goals

|			Target indicators
1	As the government, we perform human rights assessments on algorithms. We set clear requirements for public sector organisations in an implementation framework for the use of algorithms	→	• A regulator that actively ensures that algorithms used by the government are checked for transparency, discrimination and arbitrariness • Generally applicable procurement conditions for algorithms purchased by the government from third parties in place
2	Businesses providing high-risk AI systems in the Netherlands have a CE mark on their products and demonstrate that they satisfy public values, including human rights	→	• Yet to be determined
3	High-risk algorithms used by the government are CE marked and transparent unless there is a legal basis to do otherwise	→	• A transparent and easily found algorithm register • An algorithm watchdog (as referred to in the Coalition Agreement) • Supervision in the context of the Artificial Intelligence Act
4	A statutory basis for the above is created through active contributions to the EU, Council of Europe and the UN to safeguard public values around AI and algorithms	→	• Visible input from the Netherlands

Note: The social challenge and goals are in line with the parliamentary letter on public control of algorithms dated 7 October 2022

3.3 Regulate algorithms | Actions

	Description of the action	**Result** **By the end of 2023**	**Result** **By the end of 2025**	**Carried out by** **By whom,** with whom
1	Set up a **public algorithm register**	• First version of algorithm register live	• All[1] algorithms of relevance to citizens are included and visible in the algorithm register	**BZK**, ICTU, local or regional authorities and implementing organisations
2	**Be transparent** about which algorithms and **underlying 'rules' are used** within the government	• The example set by SVB and www.open-regels.nl is followed. Interpretable implementation rules from at least five implementing organisations are added	• Standing rule: 'transparent unless …' • All implementation rules are publicly accessible at all implementing organisations unless there is a legal basis for this not to be done (e.g. in the judicial domain)	**BZK**, JenV local or regional authorities
3	Draw up generally applicable **procurement conditions for algorithms** purchased by the government from third parties	• First set of procurement conditions drawn up (at least for high-risk algorithms)	• Generally applicable procurement conditions implemented	**Government-wide**, local or regional authorities
4	Develop an **implementation framework for government use of algorithms**	• First supported version of the implementation framework	• Implementation framework is in use	**Government-wide**, local or regional authorities
5	Based on the EU's AI Act: Ban certain algorithms and make it mandatory for algorithms posing a high risk for people to be **CE marked** and registered in a European database	• First CE marking • First algorithm registered in an EU database by the Netherlands	• 50+ CE marks • 50+ algorithms registered in EU databases	**BZK, JenV, EZK**
6	Set up an **algorithm regulator**	• Regulator role selected and regulations prepared accordingly • Regulator budget allocated • Regulator function active	• Regulator organised	**BZK, EZK, JenV,** local or regional authorities, Dutch Data Protection Authority (AP), AT
7	Draw up **guidelines** for the **use of algorithms** in sectors such as healthcare and government to be introduced into the EU	• Guidelines for the use of algorithms, e.g. for healthcare and government sectors		**BZK, VWS, JenV,** local or regional authorities

1. *Limited by statutory or justified exceptions that apply when weighing interests in the context of investigations, law enforcement, Ministry of Defence, intelligence gathering, etc.*

4 A digital government that works on a *value-driven* and *open* basis for all
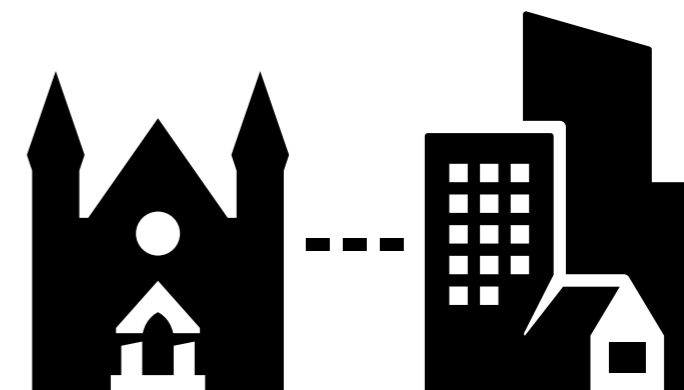
4.1 Improve information management for open government | Overview

Social challenge

Dutch authorities and public sector organisations are required to be open: actions and decisions must be transparent and capable of reconstruction by the government and local or regional authorities. To that end, it must be possible to find information without doubts about its accuracy or genuineness. Information must also be provided within legal frameworks and deadlines. That is not yet fully possible with today's information management. This damages confidence in the government's capabilities and goodwill and restricts the 'new political culture'. In other words, information management needs to improve: we must give citizens, organisations (including the media) and parliament insight into the government's actions and decisions (and the reasons behind them) upon request and proactively. Putting citizens and organisations in a better information position helps them hold the government accountable and represent their interests. Adequate information management also contributes to efficient and effective work within the government.

Results achieved

- The Open Government Act (Woo) has been in force since May 2022. The Woo requires public sector organisations to disclose certain information actively. For instance, from 20 September 2022 (state opening of Parliament), all documents sent to Parliament will also be accompanied by the supporting 'decision memorandums'
- Action plans, including the *Open op Orde* project (government-wide), ministerial action plans, Woo Long-Term Plan (Association of Netherlands Municipalities (VNG)/municipalities) and the Inter-province Digital Agenda (IDA) – Woo project (Association of Provincial Authorities (IPO)/provinces) have already been drawn up and are now being implemented
- The entire civil service has insight into the state of its information management
- A government commissioner for Information Management has been appointed and started encouraging the government as a whole to implement the changes required as regards information management
- An Advisory Board on Openness and Information Management has been set up that monitors, mediates and provides solicited and unsolicited advice

Goals

			Target indicators
1	Public sector information is permanently available for disclosure through uniform and open standards because systems and work processes will be properly organised and a cultural shift has taken place (including an organisation-specific approach[1])	➜	• Coverage rate of use of the metadata standard (MDTO) (target value: all ministries, provinces and municipalities)
2	Citizens' and organisations' requests for the disclosure of public sector information are dealt with on time and in full (information upon request) through adequate guidance, work processes and easy-to-find information (see also goal 1)	➜	• Percentage of Woo requests handled within the statutory and/or agreed period within government (target value: 100%)
3	Active disclosure of public sector information[2] is technically possible and set up to enable the government to start acting on the basis of openness; systems, work processes and culture are geared towards that, and it is clear what is due to be published, and when	➜	• Percentage of administrative bodies disclosing Woo information categories on PLOOI (Open Public Sector Information Platform)

Additional comments for this page

- *The Minister of the Interior is responsible for the disclosure policy.*
- *The Minister for Digitalisation and Kingdom Relations is responsible for improving information management.*
- *The Government Commissioner for Information Management drives this priority.*

1. *The information management of a ministry responsible for policy requires a different structure from that of an implementing organisation or inspectorate, for example*

2. *This initially concerns the 17 information categories under the Woo*

4.1 Improve information management for open government | Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1 Implement the *Open op Orde* **generic action plan aimed at (1) improving professionalism through better HR policy, (2) actively organising information management within the organisation, (3) harmonising and standardising IT information systems and (4) setting up control, scheduling and dashboards**	• Review of the generic action plan in Q4 2022 (assurance given to TK) and inclusion of an overview of the results already achieved • Inclusion of the generic action plan in the Long-Term Plan for Government Information Management (mandatory under the Woo)	• To include, among other things, (1) greater capacity, Leerhuis (learning establishment) offering courses/training sessions, (2) publication of supporting memoranda to Parliamentary papers, (3) continuously developed IT system, (4) government-wide dashboards with targets/showing progress	**BZK/Ministry of Education, Culture and Science (OCW) for government** (*Open op Orde*/Government programme for sustainable digital information management (RDDI)), all ministries
2 Draw up **specific action plans for ministries and local authorities** to improve disclosure within all public sector organisations	• Execute action plans for own organisation and achievement • of the objectives formulated throughout government • Follow-up measurement and comparison between the • baseline and follow-up measurements	• Objectives in the ministerial action plans achieved • Annual measurements of, reports on and assessments of the effects of the objectives achieved performed	**All ministries,** BZK (Government Chief Information Officer (CIO Rijk)) **Association of Netherlands Municipalities for municipalities** (Woo Long-Term Plan) **Association of Provincial Authorities (IPO) for provinces** (IDA Woo project) **Association of Regional Water Authorities (UvW) for water authorities**
3 Implement and administer the **Open Government Act (Woo)** which provides for access to information (upon request and actively); include technical framework conditions such as the **Open Public Sector Information Platform (PLOOI)** and notifications for new publications based on the Electronic Publications Act (*Wet Elektronische Publicaties*)	• Financial and human resources reserved for the implementation and administration of the Woo • Improved percentage of requests handled within the statutory/agreed period • Publication of the first information categories on PLOOI	• Increased number of mandatory information categories published using PLOOI • Increased percentage of requests handled within the statutory • and/or agreed period	**BZK** (for PLOOI: Netherlands Publication Office (KOOP)), Government-wide **Local or regional authorities Implementing organisations**

Improve information management for open government | Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
4 Update and implement **new Public Records Act** (*Archiefwet*), including the Public Records Decree and the Public Records Regulation that ties in better with the requirements for the management/ retention of digital information (lifecycle management) and contributes to the earlier disclosure of information to be retained	• Bill established • Metadata standard (MDTO) established for • the entire government • Further preparations for entry into force (including the draft Public Records Regulation and Decree)	• Implementation of the updated Public Records Act (including decree/regulation) • Further roll-out of the MDTO	**OCW**, government-wide **Local or regional authorities** **Implementing organisations**
5 Set up more robust **supervision and coordination** of information management through Government Commissioner, the Public Sector Information & Heritage Inspectorate and **CIO Rijk**, among others	• Follow-up actions have been established		**Government Commissioner** **Public Sector Information Advisory Board**
6 Explore and develop a **'General Information Act'** bill that creates coherence between information legislation and regulations and provides guidance on how to organise information management and information provision	Depending on the outcome of the exploratory study, aim for: • Inter-administrative agreement on the General Information Act bill	Depending on the outcome of the exploratory study: • Complete the legislative procedure (submission to the cabinet, mandatory advice, consideration by Parliament)	**BZK/Government Commissioner,** *Open op Orde* programme

4.2 Improve data management for citizens and organisations | Overview

Social challenge

The use of data by the government can offer many opportunities but can also create distrust, such as in the case of the childcare benefits scandal. As such, it is essential that data are always collected, stored and processed on the basis of clear legal and moral values (e.g. respect for the GDPR, privacy, non-discrimination, control by citizens, etc.).[1] With such safeguards, the targeted use of data, including citizens' data, can create a lot of social value because it helps the government and municipalities understand who needs what help and when. This requires sound agreements and partnerships between authorities and government agencies in line with citizens' interests and the law. Non-personal, open government data can also be useful for the activities of citizens, businesses and other organisations, including research activities. Here, too, data quality is essential (including timeliness and representativeness); that basis is currently not up to scratch.

Results achieved

- Several central and local or regional public sector organisations are actively publishing open data, and other innovative initiatives are being taken in relation to data (see www.digitaleoverheid.nl/initiatief for an overview of initiatives)
- Using the Common Ground initiative, municipalities such as Utrecht, Haarlem and Den Bosch have improved their handling of data (more efficient and in line with current legislation) by storing it uniformly, separating storage from specific work processes and applications, and consulting data at the source using APIs (instead of copying and storing it in multiple locations)
- Rules for a single set of data ethics have been introduced in the public sector
- An inter-administrative data strategy has been established

Goals

	Goals		Target indicators
1	Secure, legal and value-driven storage and handling of data (e.g. structurally safeguarding the GDPR, privacy and control), creating trust among citizens, including by setting clear requirements for access and use of data	➔	• Number of ministries and large implementing organisations that publish transparent information about their data management set-up and compliance with legislation, including the GDPR (target values: all ministries and major implementing organisations)
2	High-quality data resulting from adequate data architecture, systems and guidelines, enabling the government to create more value for specific citizens and organisations and make better overall policy choices	➔	• Yet to be determined
3	Where useful, necessary, permitted and in line with citizens' interests and wishes, citizen data are used and shared as one government, to which end the correct agreements/governances, standards and facilities are in place to achieve that percentage of administrative bodies publishing Woo information categories on PLOOI	➔	• Yet to be determined
4	Non-personal data of authorities and government agencies and public organisations are available as open data, where possible, to allow citizens, businesses and other organisations to use them for their activities	➔	• Yet to be determined

---

1. See, with regard to the values: 2.1 'Safeguard public values'; 2.2 'Safeguard privacy, responsible data use and increase transparency regarding data processing and exchange'; 3.1 'Control of own data' and 3.3 'Regulate algorithms'

4.2 Improve data management for citizens and organisations │ Actions

Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1 Appoint **Chief Data Officer** for each ministry to reinforce control and supervision of data management and use	• CDO appointed for each ministry (coordinator's role)	• CDO role formalised for each department, including explicit role specification	**BZK** (**CIO Rijk**), all ministries
2 **Influence European data legislation** in line with Dutch public values with active lobbying and cooperation at EU level			**BZ/EZK/BZK**
3 **Implement legislation and regulations** (new and existing), such as the GDPR and new EU Acts, actively comply with guidelines relating to data by raising awareness among employees and being transparent	• Discriminatory risk profiles identified (execution of motion 21)	• New European data legislation (Data Governance Act, Data Act) implemented	**BZK (CIO Rijk/Digital Government Directorate)**, mainly ministries with implementing organisations (also being data source holders) **Local or regional authorities**
4 Set up a **proper data management** system ('bookkeeping') that gives insight into the data available, its significance in relation to policy and law (including the legal basis), data classifications, the parties with whom the data are shared and the persons in charge	• Data quality framework created for the government (first version)	• Data catalogue standard developed • Data dictionaries standard developed	**BZK**, government-wide, including implementing organisations (also being data source holders) **Local or regional authorities**
5 Improve the **sharing of data between authorities and public/semi-public organisations** by, among other things, ensuring that there is a legal basis, setting up chains, including data chains, and the required governance for each chain (e.g. using the **Common Ground initiative and a federated data system**, and learning from initiatives in other countries, such as Solid in Belgium, in the process)	• Reuse of Government Information Act (*Wet Hergebruik overheidsinformatie*) revised • Picture of the future for the Key Registers System/federated data system set out in more detail • Develop domain-specific solutions (e.g. in healthcare)	• Develop legislation and regulations further where necessary (e.g. legal bases) • Develop agreements/governances, standards and facilities further where necessary (e.g. for practical aspects of data sharing)	**BZK (through IBDS)**, ministries within their own domains (e.g. Ministry of Health, Welfare and Sport (VWS) for healthcare), implementing organisations **Local or regional authorities**

4.2 Improve data management for citizens and organisations | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
6	Increase the **supply of open data** from government, local or regional authorities and public organisations (by way of illustration: the KNMI Data Platform or RIONED regarding urban water management)	• Act implementing the Open Data Directive (*Wet implementatie open data richtlijn*) (revision of the Reuse of Government Information Act)		**BZK**, ministries within their own domains (e.g. VWS for healthcare), other public sector organisations holding data relevant to the public
7	Exploit the **opportunities provided by data**, e.g. innovation through cooperation between authorities and government agencies, the market and the scientific community in: sharing best practices, applications, data ecosystems/labs, and encouraging the use of open data (following the example of the Ministry of Agriculture, Nature and Food Quality (LNV) with Geonovum in relation to geodata and the Royal Netherlands Meteorological Institute (KNMI) with ARISTOTLE), eliminating bottlenecks (legal, technical and/or organisational) where possible	• Two supra-ministerial data cooperation initiatives (data courses) launched • Action programme within leading ministries (e.g. LNV) • Create a more detailed overview of domain-specific bottlenecks and identify solutions (e.g. in healthcare)	• Start implementation of supra-ministerial data cooperation initiatives • Gradual implementation of solutions for domain-specific bottlenecks (possibly accompanied by amendment of legislation and regulations, if legal)	**BZK (CIO Rijk & through IBDS)**, ministries for specific themes, implementing organisations

4.3 Improve the government's ICT organisation and systems | Overview

Social challenge

ICT is essential to a modern government's ability to act; demands are made of technology, but also of people and organisations. This is because ICT has human aspects: working digitally must be at the heart of policy and implementation. The plans made by the government must be substantiated and embedded financially and digitally, with transparent costs and benefits. This requires a professional ICT organisation that attracts digital talent with an attractive working and learning environment. The technical foundation must be in order first: this means 'cleaning up' old systems (improving, integrating or phasing out) to make space for an innovative ICT landscape and generic facilities, using open source and standards where possible. The government would also like to occupy a central position in society: we must work for citizens and learn from science and the market.

Results achieved

- CIO Rijk is currently responsible for government-wide coordination to improve the government's information provision and ICT in cooperation with the CIO consultation group, the CISO board and the CTO board
- Work is being carried out within the I-Strategy theme 'Digital resilience', including on cybersecurity and privacy; frameworks for societal requirements such as digital identities and data control are being discussed as part of the theme 'Data and algorithms'. We are also working on agreements to provide better insight into the composition and use of algorithms
- However, other prerequisites such as digital skills and solid digital infrastructure are being worked out in more detail in the themes 'I-professionalism' and 'ICT landscape', respectively

Goals

			Target indicators
1	Improved IT/information provision systems and infrastructure, with a modern ICT landscape and the right agreements, standards and facilities, as a basis for the effective functioning of the government internally and in its dealings with citizens [I-Strategy – 3 & 4]	➡	• Number of departments and major implementing organisations that have designed their IT/information provision landscapes in accordance with the principles of the Civil Service Enterprise Architecture (Enterprise Architecture Rijksdienst) (target value: 12 ministries and all major implementing organisations)
2	A professional IT/information provision organisation at the heart of policy, implementation, supervision and enforcement, with robust professionalism and effective governance, capable of exploiting the opportunities offered by digitalisation and developing the IT/information provision systems required for this [I-strategy – themes 1, 7 & 9]	➡	• Number of ministries to have fully implemented the CIO system 2021 Decree (Besluit CIO-stelstel 2021) according to measurements taken by the Government Audit Service (ADR) (target value: 12) • Percentage of proposals for new policy, implementation or enforcement with an information section (target value: 100%) • Percentage of implementation tests with a digital section (target value: 100%)
3	The costs, benefits, coherence and position of the government's IT/information provision activities are transparent and capable of being understood by Parliament and society [I-strategy – theme 8]	➡	• Yet to be determined
4	The government actively cooperates with local or regional authorities, businesses and the scientific community, enabling it to learn faster, innovate and purchase more effectively [I-strategy – theme 10]	➡	• Yet to be determined

4.3 Improve the government's ICT organisation and systems | Actions

📣 Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1 Set up a **Government Architecture Board (Architectuurboard Rijk)** led by the government architect who will bring the I-landscapes in order under architecture, including enterprise architecture (this does not concern the primary processes)	• Government architect appointed • Government Architecture Board set up	• Government Architecture (EAR) has been renewed	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
2 **Implement government-wide Life Cycle Agreement (Lifecycle Convenant) and associated standards** concerning government-wide collaboration on effective life cycle management of ICT systems for better insight into and handling of legacy architecture	• Baseline measurement of LCM maturity • Government-wide LCM community established for knowledge sharing and professionalisation	• Insight into current and desired I-landscapes, including a plan on how to achieve them and phase out legacy architecture • LCM manual ready for structural embedding	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
3 Modernise **Government-wide Digital Infrastructure (RDI)** using appropriate agreements, standards and facilities, guided by government-wide principles: standardisation, reuse and open source	• Portfolio board focuses on generic and government-wide facilities • Government Open Standards Monitoring Report available • 'Open source, unless' for frontrunners	• Multi-year budget for generic facilities available • The following applies to government: 'Open source, unless'	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
4 **The transition to the cloud** proceeds securely and responsibly in accordance with a government-wide cloud strategy (with attention to European digital sovereignty and security and clear agreements on aspects such as interoperability and data portability)	• Cloud strategy and frameworks available	• Cloud strategy and frameworks implemented	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
5 Aim for **sound commissioning practices** by the government for information provision/IT services and facilitate **innovative procurement policy** in which modern requirements and wishes are firmly embedded (e.g. with regard to European digital sovereignty, standards and harmonisation, openness/open source, etc.)	• Sound Commissioning Practices handbook available • Study concerning national and European public procurement legislation completed	• Tools and good practices for Sound Commissioning Practices available throughout government • Innovative procurement policy handbook available	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]

1. E.g. DUO, BD, UWV, Directorate-General for Public Works and Water Management (RWS), Custodial Institutions Agency (DJI), NP

4.3 Improve the government's ICT organisation and systems | Actions

|	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
6	Structural use of **technology scanning** for existing services to exploit the opportunities offered by new technology	• Several government organisations perform technology scans	• Each government organisation conducts regular technology scans	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
7	**Make** government **ICT chain more sustainable**, under coordination by the National Working Group for Sustainability in Civil Service ICT	• Improve return process for civil servants' unused devices	• Servers virtualised where possible • Liquid cooling in data centres • Data storage reduced where possible • Server CPU loads reduced • Sustainability data for ICT hardware added to the government's ICT dashboard	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
8	**Attract i-professionals and young talent** through the use of recruitment teams in collaboration with higher education and competitive employment conditions, among other things	• Uniform IT quality profiles (IT roles) implemented within government • IT learning paths developed	• Monthly labour market campaign • Cooperation between higher professional education and university education establishments and government: internships, field labs, minors, etc.	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
9	**Retain i-professionals and young talent**	• Exploratory study conducted to establish which 5–10 interventions are necessary to retain i-talent within government	• Gradual implementation of required interventions	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
10	Expand **range of mandatory and non-mandatory courses** offered by the National Academy for Government Digitalisation and Computerisation (RADIO) to improve I-knowledge among non-I staff	• Various courses, e-learning sessions, podcasts and webinars on different ICT themes developed	• Supplementary and mandatory courses, e-learning modules, podcasts and webinars on different ICT themes developed	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
11	Develop ministerial information plans into **fully-fledged digitalisation plans based on clear standards** from the CIO System Decree and elaborate them in quality framework (including standardisation)	• Information plans linked to government budgetary cycle	• Annual update	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]

1. *E.g. DUO, BD, UWV, Directorate-General for Public Works and Water Management (RWS), Custodial Institutions Agency (DJI), NP*

4.3 Improve the government's ICT organisation and systems | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
12	Improve **insight into the costs and social value (and the standards to be applied)** of IT/information provision with a revamped government ICT dashboard	• Dashboard management and maintenance	• A.o., CO_2 emissions of government-wide ICT activities added to the dashboard	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
13	Implement **standards and obligations provided for by CIO System Decree** regarding **digital leadership** (including the learning capacity of top management) and government-wide IT/information provision **governance** (including formalisation of the **CTO** and **CDO roles**), and elaborate Code for Good Digital Public Governance (CODIO)	• Civil Service CIO System Decree (2020) implemented • CIO System Decree expanded to include the CDO role • CTO role and system examined	• CIO System Decree expanded to include the CTO role • Every ministry has assigned the CIO, CTO, CISO and CDO roles • Practical tools provided under CODIO are in use	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]
14	Anticipate digital consequences by mandating an **information section for every new piece of policy**, implementation, supervision and enforcement, and expand the **implementation test to include a digital component**	• The information section handbook is available • Quick scan in place for information provision risks	• Information sections implemented throughout government • Implementation test expanded and in use	**BZK**, other ministries, implementing organisations, local or regional authorities (should central policy have an impact)
15	Promote **cooperation with the market** through network meetings and joint training courses	• CIO meetings between market operators and CIOs organised every other month	• Innovation platform established for government-wide collaboration and knowledge sharing	**BZK** (**CIO Rijk**), Government-wide, including major implementing bodies[1]

1. *E.g. DUO, BD, UWV, Directorate-General for Public Works and Water Management (RWS), Custodial Institutions Agency (DJI), NP*

5   *Strengthen* the digital society in the *Caribbean part of the Kingdom*
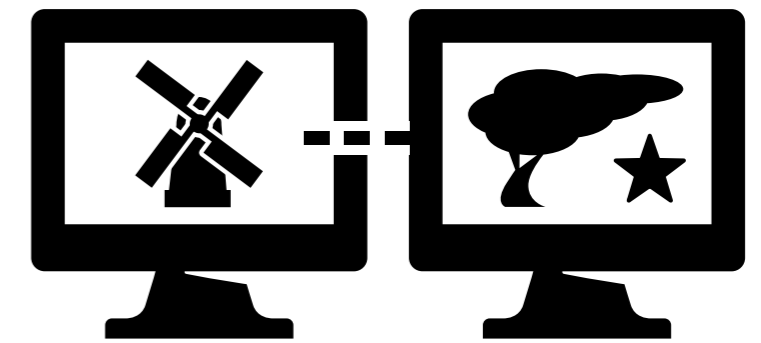
5.1 Strengthen the digital society in the Caribbean part of the Kingdom | Overview

Social challenge

Citizens and businesses in the Caribbean Netherlands must be able to participate in the digital society at an equivalent level. This is often not yet the case. Public sector and semi-public sector service provision is not yet optimal and digital government is still in its infancy. People often still need to visit offices and submit written documents. This is a time-consuming and error-prone process. Things that can be arranged digitally are not always done sufficiently securely. In addition, only about 85% of citizens have internet access at home; probably one in five citizens is not digitally literate; in Saba and Sint Eustatius, in particular, the internet is found to be expensive, slow and unstable. We need to make improvements in these areas. We will better ensure privacy and cybersecurity and invest in the digital society. There are similar issues in the Caribbean countries within the Kingdom, with regard to which we will provide assistance and support.

Results achieved

- Structural coverage in the government budget for subsidising internet subscriptions for citizens in the Caribbean Netherlands.
- A tax reference number (CRIB) enabling digital submission of tax returns in the Caribbean Netherlands using the 'Mijn CN' portal

Goals

			Target indicators
1	Public sector and semi-public sector service provision in the Caribbean Netherlands will be on the same level as in the European Netherlands, both digitally and physically. Public service provision will be accessible and high-quality for all citizens and businesses. This will be mandatory and, where possible, based on the same legal and other standards that apply to the European Netherlands. Statutory obstacles due to differences in legislation and regulations as compared with the European Netherlands will be eliminated where possible	→	• Yet to be determined
2	Internet access will be assured in the Caribbean Netherlands and everyone – citizens and businesses – will be able to participate in the digital world proficiently and safely: • Infrastructure: increase internet stability and coverage • Digital skills and inclusion: everyone can participate, improved digital skills, better access to internet tools and affordable internet access • Security: safeguard privacy and strengthen cybersecurity	→	• Yet to be determined
3	Kickstart the transition to a digital society in the Caribbean Netherlands through investments	→	• Yet to be determined
4	Facilitate and assist the constituent countries in their transition to a digital society	→	• Yet to be determined

5.1 Strengthen the digital society in the Caribbean part of the Kingdom | Actions

	Description of the action	Result By the end of 2023	Result By the end of 2025	Carried out by By whom, with whom
1	Further develop the **identity and access system**	• Students from the Caribbean Netherlands and the constituent countries will receive a citizen service number (BSN) faster, making it easier for them to request facilities	• Every citizen from the Caribbean Netherlands has a BSN • Improved quality of address registration	**Ministry of the Interior and Kingdom Relations** (**BZK**), **National Office for Identity Data** (**RViG**), Ministry of Education, Culture and Science (OCW)/Education Implementation Service (DUO), Caribbean public bodies, National Office for the Caribbean Netherlands
2	Execute action plan entitled '**Public Service Provision for the Caribbean Netherlands** to bring public service provision to an equivalent physical and digital level'	• Completion of analysis and goal definition phase • Quick wins and no-regret measures identified • Completion of planning and investment decision phase	• Quick wins and no-regret measures implemented • Policy and legal standards for accessible and high-quality public service provision and digital government introduced, based on the principle 'equal or equivalent' as compared to European Netherlands • New, yet to be determined digital facilities for digital government introduced	**BZK**, **Caribbean public bodies**, National Office for the Caribbean Netherlands, OCW, Ministry of Health, Welfare and Sport (VWS), Ministry of Finance (FIN), Ministry of Social Affairs and Employment (SZW)
3	Execute action plan to improve **internet affordability, availability and stability**	• Completion of analysis and goal definition phase • Completion of planning and investment decision phase	• Measures to be decided on later	**Ministry of Economic Affairs and Climate Policy** (**EZK**), **BZK**, Caribbean public bodies, telecom providers
4	Improve **digital skills**	• A digital government information point will have been established • Measures to be decided on later	• Measures to be decided on later	**BZK**, **OCW**, Caribbean public bodies, libraries
5	B**e safe and secure online** in the Caribbean Netherlands	• Measures to be decided on later	• Measures to be decided on later	**BZK**, National Cybersecurity Centre (NCSC)
6	Draw up fourth round of **growth fund proposition**	• Action plan ready • Proposition drawn up	• Plan submitted • Measures to be decided on later	**BZK**, Caribbean public bodies, **EZK**, OCW
7	Determine with the constituent countries how we can facilitate and support them during the **transition to a Digital Society** and decide on further action	• Action plan • Needs identified • Business cases and decision-making • Action plan drawn up	• Measures to be decided on later	**BZK**, **EZK**, OCW, Aruba, Curaçao, Sint Maarten

Working towards a *safe, inclusive and promising* digital society