

Digital economy and communications

64. Estonia's goal is to become the EU leader in the development and use of artificial intelligence (AI). We participate in the European AI funding projects to **strengthen the AI development capacity of Estonia** and ensure access to strategic technologies.

65. To ensure that small and medium-sized enterprises have access to the **EU's high-performance computing (HPC)**, the service must be kept accessible and affordable. It is essential for the promotion and implementation of Estonia's digital economy that entrepreneurs gain access to or participate in AI factories and that our SMEs can participate in the EU's AI procurement. If demand arises, we will apply for the establishment of a **local branch of an AI factory in Estonia**.

66. The **development of new data-driven services must be supported and funded by EU funds**. Under the leadership of the European Commission, EU-wide technological solutions must be developed for the data marketplace and for concluding and enforcing data reuse and repurposing agreements.

67. **The list of valuable data sets established at the EU level** (e.g. spatial data and services, energy sector, public water supply and sewerage) for which common disclosure restrictions should be imposed due to existing risks or threat assessments must be reviewed.

68. The digital identity of an EU natural person eID **must be interoperable across borders** and enable reliable identification of the individual. To achieve that, there is an urgent need to develop a certification scheme for the digital wallet.

69. **Legal clarity and certainty must be increased in the EU data area**. To this end, the Commission needs to ensure the **creation of test environments or sandboxes** for the implementation of EU data legislation to give businesses and public authorities certainty that their product or service complies with EU requirements.

70. In the EU, the uptake of **privacy technologies and secure data processing environments** must be encouraged to ensure that data is used and valorised in a privacy-preserving way. The European Commission needs to provide guidance and clarity on which privacy technologies are compliant and sufficient to protect fundamental rights in the EU.

71. It is important to initiate and implement the **Nordic-Baltic Cyber Consortium** and other similar EU regional projects to strengthen Member States' cooperation and joint capabilities in cyber incident prevention and response.

72. The number of cyberattacks against Member States in the coming years is not going to decrease. Based on the Cyber Crisis Management Framework, the Commission should develop an **operational plan for responding to a high-impact cross-border cyber incident** and practice its implementation in exercises.

73. It must be easy for the provider of a critical or essential service to **report cyber incidents**, including that only a single notification should be required for the same incident. The **risk analyses required** from a producer or service provider under cybersecurity and cyber resilience acts need to be structured in a similar way (e.g. structure of analysis, taxonomy, frequency, etc.) in order to reduce the administrative burden, in particular for SMEs.

74. **The primary task of the EU Agency for Cybersecurity (ENISA)** is to assist Member States in cybersecurity capacity building projects and to support them in the event of a cyberattack. ENISA's mandate should be reviewed accordingly, and it should be relieved of tasks that are not directly related to assisting and supporting Member States or that overlap with the European Cybersecurity Competence Centre.

75. There is a need for focused development of **language technologies** in the official languages of the European Union, including Estonian and other small EU languages. The EU should define language data as valuable data sets, realise the language data space, and support the development of the infrastructure needed to build a large EU language model. **To preserve the EU's linguistic diversity and avoid falling behind, it is necessary to support the creation of the needed infrastructure for AI development in small Member States.** We consider it important to integrate a sufficient quantity and quality of small language corpora into training AI in a way that ensures copyright protection.

76. With the extremely rapid development of AI solutions, it is important that **the authors** whose works have been used in the process of developing and training AI models **do not suffer as a consequence**. At the EU level, there is a need to create an efficient **licensing market for AI training data** (in the context of language data, this could be part of the language data space created by the European Commission) and legal clarity on the ownership of AI output. The AI sectoral codes of conduct must provide **authors, performers, and other right-holders with the tools to exercise and enforce their rights**.

77. The establishment of data centres must be accelerated to ensure a **physical cloud infrastructure in the EU** and to promote the **emergence and development of cloud service providers** physically located on EU territory under EU jurisdiction. The establishment of data centres and support for cloud service providers must be based on a geographic balance within the EU, as well as ensuring equal opportunities for companies in small Member States. To revitalise the EU's cloud services market, we support creating opportunities to favour EU cloud service providers in procurement processes.

78. The **resilience and attack-resistance capacity of priority international data communication cables** must be increased. Adequate resources from the EU budget must be provided to achieve this.

79. In the transformation of the **telecoms landscape**, it is important to avoid solutions that lead to forced **consolidation** of companies operating in the sector, as this will reduce competition, innovation, and quality of services.