REFORMS FOR ECONOMIC GROWTH AND BUSINESS RESILIENCE 2022

DIGITAL ECONOMY COMMITTEE

AMCHAM SERBIA

A LEADER IN CHANGE

DIGITAL ECONOMY COMMITTEE

OBJECTIVE 1: DEVELOP AN EFFICIENT AND SERVICE-ORIENTED E-GOVERNMENT AND REMOVE OBSTACLES TO ELECTRONIC TRANSACTIONS

…BY FACILITATING USE OF THE REGULATORY FRAMEWORK FOR ELECTRONIC DOCUMENTS, ELECTRONIC IDENTIFICATION, AND TRUST SERVICES

CHALLENGE: The **Law on Electronic Documents**, Electronic Identification and Trust Services in Electronic Transactions has been the first step in improving the regulatory environment for e-commerce and electronic communications between the public administration, members of the public, and businesses. Although it took effect in October 2017, this piece of legislation is **yet to be fully implemented by all authorities, across sectoral regulations, and in all industries.**

RECOMMENDATIONS:

- Create conditions for full and unchallenged implementation of the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions in the public sector by aligning sector-specific rules with this piece of legislation and its implementing statutory instruments. This is especially important for employment regulations (where annual leave approvals in electronic form ought to be recognised, as should all general and specific employment-related instruments), customers' ability to sign telecommunications and insurance contracts remotely, use of electronic delivery notes and similar documents that accompany goods shipments, and the like.
- These changes can be made by amending sectoral regulations, and until the revisions are complete it may be beneficial to consider having line ministries issue official opinions suggesting the Law on Electronic Documents be applied in these areas as appropriate, which would allow electronic documents to be used instead of physical ones before the rules are formally changed.

CHALLENGE: According to the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions and the Government Order on requirements for assurance levels of electronic identification schemes, the only option for members of the public to obtain **qualified electronic signature certificates (and certificates for other medium assurance trust services) is to attend in person so that positive identification can be made**.

RECOMMENDATION:

- To expedite access to qualified trust services, popularise and facilitate their use, and broaden the range of areas in which these services are available, amend the Government Order on requirements for provision of qualified trust services to permit qualified certificates to be issued remotely, using video conferencing or other up-to-date identification methods. Video identification could be used for remote signing of contracts in areas such as telecommunications and insurance, whereas currently it is recognised only by National Bank of Serbia (NBS) rules and so can only be employed by financial institutions overseen by the NBS.

CHALLENGE: Last year's amendments to the Government Order on case and document management by public authorities pushed back the entry into force of this regulation and the associated time limits to 1 February 2022. Although the initial plan was to have 30 authorities use the centralised electronic document management solution and to integrate 50 individual pieces of software with it, the document management

system remains absent, making it necessary to retain traditional document management practices. Many authorities use case management systems but a large number of these are rudimentary and involve nothing more than case registries, with documents not being digitised or stored electronically. Moreover, a variety of systems are used, which hinders interoperability.

> **RECOMMENDATION:** Ensure all public authorities and local governments switch to the centralised electronic document management system as quickly as possible. This arrangement would allow service users to file submissions and track their cases online. The authorities ought to receive training in this respect and a contact centre should be set up to support the deployment of the new software.

…BY INTRODUCING UP-TO-DATE REGULATIONS AND INFRASTRUCTURE TO SUPPORT DEVELOPMENT OF ELECTRONIC COMMUNICATIONS

CHALLENGE: Even though the Electronic Communications Bill was adopted by the Serbian Government in late 2017, it has subsequently undergone multiple revisions and is yet to enter parliamentary procedure. In the meantime, the EU has adopted the European Electronic Communications Code. Since the Bill as it currently stands is aligned with European regulations dating back to 2003, Serbia is significantly behind in adopting the Union *acquis* in this area. Delays with enacting this law are also hindering adoption of separate broadband internet legislation. Lastly, the current regulatory framework is out of step with the pace of sectoral development, especially with 5G rollout.

RECOMMENDATIONS:

- Adopt the Electronic Communications Law in consultation with stakeholders to ensure the new legislation is aligned with EU rules (and address issues with the current legislation identified to date, which will also accelerate amendment of secondary legislation that governs options already supported in the electronic communications market).
- Adopt legislation/regulations to comprehensively govern the development of broadband networks based on the principles of objectivity, transparency, non-discrimination, and technological neutrality.

CHALLENGE: Before a 5G spectrum auction is held, regulatory obstacles to siting cell towers must be overcome, as these limitations already hinder the extension of network capacity using existing technologies (2G, 3G, and 4G) in most urban areas. If this issue is not addressed, 5G, which requires much denser cell tower network coverage, will not be possible.

Regulations in this area, especially environmental protection rules, are not aligned with EU standards, and the issue is compounded by the fact that local authorities are responsible for their implementation, which results in sharply differing practices by the various towns and municipalities. Ignorance, fear, and misinformation have led to the imposition of a wide range of restrictions over the years, including in urban planning documents (such as the Belgrade General Zoning Plan) not specifically designed as safeguards against non-ionising radiation. Contrary to their intended purpose, these limitations have not reduced exposure to non-ionising radiation (and have actually heightened the risks, since fewer cell towers means mobile phones have to output more power to connect) and have also threatened the operation of mobile telephony networks and restricted broadband coverage.

Members of the public have baseless concerns as to the alleged adverse impact of cell towers on human health, and this issue should be addressed through outreach and presentation of scientifically proven facts.

RECOMMENDATIONS:

- Revise and enhance the regulatory framework governing cell tower construction to make the requirements more transparent and promote public trust in oversight and electromagnetic radiation measurements, as well as to ensure cell towers can be built and commissioned

more quickly and easily according to standardised and pre-defined procedures. Instead of the current arrangement where permits are valid for extended periods after complicated administrative procedures and with reference to results of simulations, theoretical modelling, and computer-aided projections of expected electromagnetic fields, emphasis ought to be placed on actual measurements of non-ionising radiation done in the field by licensed laboratories, with periodic controls after commissioning and public availability of actual measurements.

- Specific measures could include:
  - Amending the relevant government order to exempt telecommunications facilities from requirements of Schedule 2 of the Environmental Impact Assessment Law, in accordance with EU models.
  - Removing metric restrictions for cell tower siting from zoning plans and other local authority enactments.
  - Revising the definition of 'sources of non-ionising radiation of particular importance' in the Law on Protection from Non-Ionising Radiation and its implementing regulations.
  - Re-assessing reference values for electromagnetic fields set out in the Regulation on limits for exposure to non-ionising radiation as these are 2.5 times more restrictive than those applicable in most EU Member States.
- On 9 December 2021, the Government of Serbia established an Expert Group to address administrative barriers for cell tower siting. We hope the incoming government will continue efforts in this regard and begin removing barriers to the commercial launch of 5G as soon as possible.

CHALLENGE: Although discussions have been held and officials have announced preparations for allowing 5G rollout in Serbia, it remains unclear when this opportunity will become available. The delay has been stalling market development and hindering the digital transformation, which requires infrastructure based on next-generation technology. In addition, obstacles affecting access to and development of fixed infrastructure have made it difficult to provide broadband internet and mobile telephony coverage in areas where the public, businesses, and institutions need it the most.

RECOMMENDATIONS:

- Hold an efficient and simple 5G spectrum auction as quickly as possible according to an optimum model that will best suit the Serbian market, promote competition and new infrastructure investment, and follow EU best auction practices. It is important to ensure the auction is used to allocate the spectrum rather than as a source of short-term revenue for the national budget so that most of the funds raised are invested in network and infrastructure development. We feel that the main purpose of introducing 5G is to allow fast and efficient network development and provision of access to new technologies for as many users as possible, and as such we believe the auction method and licence prices ought to be chosen so that operators are incentivised to make rapid new investments in infrastructure to deliver services to as many users in as short a time as possible.
- Allow transparent and predictable access on a commercial basis to **existing fixed infrastructure** controlled by both telecommunications operators and other public and private entities, including state-owned enterprises (such as Serbian Railways) as well as to other infrastructure that permits straightforward and efficient fibre optic cabling (such as underground telecommunications routing canals, electrical lines, distance heating pipelines, and the like), including by enhancing the regulatory framework requiring large operators to ensure access.
- Ensure the drafting of regulations, both those on 5G and those designed to ensure unrestricted access to existing infrastructure, is transparent and inclusive.

…BY INTRODUCING AND ENHANCING ELECTRONIC SERVICES AND PROCEDURES

CHALLENGE: The ***e-Sud*** ('e-Court') web application, intended to allow online case management, is currently not available to parties in any proceedings other than those before the Administrative Court.

> **RECOMMENDATION:** Allow use of *e-Sud* in all civil and enforcement cases, including for online access to case files and online submission filing. The benefits of online case management ought to be promoted more widely, and amendments to procedural legislation should be made to permit online service of process and allow parties to represent themselves or be represented by holders of powers of attorney remotely in hearings. Broaden the use of *e-Sud* so parties can use it to communicate not only with courts but also with enforcement officers, who exercise devolved public authority in enforcement cases, and allow one-click access to case files.

CHALLENGE: In developing the Digital Health Strategy, Serbia has made great strides in mapping the road to a patient-oriented **digital health service**. To ensure this strategic document delivers tangible benefits, the Action Plan for a digital health service needs to be fully implemented, in particular insofar as it calls for the introduction of electronic patient records and the creation of an online platform for marketing authorisations and approvals of medicines.

Currently, electronic patient records do not include all medical information (such as specialist referrals, findings, and the like) or private healthcare data, including findings of tests conducted by private laboratories. This makes the records incomplete and poses challenges to tracking patients' medical histories.

The medical regulator ALIMS has failed to observe statutory time limits for granting marketing authorisations for medicines, with delays running into months and in some cases reaching 20 times the prescribed timeframes. These bottlenecks mean patients having to wait for extended periods before accessing novel treatments, interruptions to supply of medicines, and additional costs due to failed procurements.

> **RECOMMENDATIONS:**
>
> - Fully implement electronic patient records by allowing access to and integration of data from both public and private healthcare facilities. This can be done by clearly specifying the information these records must include, standards, unambiguous data entry and access procedures, and data access permissions.
> - Address delays with marketing authorisations by streamlining procedures mandated by the Medicines Law, to be accompanied by the development of an electronic platform the ALIMS can use to manage the process.

CHALLENGE: There is currently no single information system for businesses to share all cross-border trade data with public authorities and for these bodies to process the data, and no efficient risk assessment arrangements shared across all inspection services that control goods shipments. A unified solution for this purpose would reduce barriers to trade and facilitate goods imports and exports. The information systems currently used by the authorities vary widely in their sophistication and automation, and risk assessment as a concept is not recognised in all cross-border trade procedures.

> **RECOMMENDATION:**
>
> - Implement a **National Single Point of Contact** system that ought to entail complete digitalisation of procedures and risk assessment modules for all border inspections, including the sanitary, phytosanitary, and veterinary inspection services. The key objective here is to provide businesses with a single point of contact with inspections and other relevant authorities and improve the quality of data collected and facilitate their analysis. This goal can be achieved through a range of services used by both businesses and the government, including initial business registration, filing of customs declarations, risk management, collection of fees, taxes, and other dues, customs clearance, information sharing between government agencies, and the like.

CHALLENGE: The production of spatial and urban plans, which designate intended land uses and prescribe building requirements, is a major bottleneck for property development in Serbia. If all procedures are followed to the letter, it takes at least six months to enact a detailed zoning plan, with general zoning plans requiring at least one year. However, due to inefficient communication and co-ordination between the relevant authorities, adopting these plans often takes years.

Serbia currently boasts good planning document coverage, but these are in many cases incomplete and require further elaboration by means of plans at greater levels of detail, which property developers quite frequently have to finance before being able to build yet lack any certainty as to how long their projects will take to complete. The absence of a single comprehensive and up-to-date register of all plans makes it difficult even for professionals to know exactly what building requirements apply to which zone.

> **RECOMMENDATION:** Establish an online platform (tentatively named ***eProstor***, 'e-Space') to facilitate the development of spatial and urban plans, documents which determine land use and set out building requirements. This platform would permit institutions to exchange information electronically, make comments, issue building requirements and approvals, and use the online service simultaneously to develop plans instead of having to wait for each to complete its own part of the work in isolation, as is the case now. Linkages between eProstor and the National Land Survey Authority (RGZ), which administers the cadastre, would allow easy access to cadastral information required for construction whilst also allowing regular updates to data in the cadastre.

OBJECTIVE 2: PROMOTE INNOVATION

…BY REGULATING ARTIFICIAL INTELLIGENCE

CHALLENGE: Artificial intelligence (AI) is currently not regulated by law in Serbia, except in part by personal data privacy legislation. The development and use of AI by both the public and the private sector creates extensive opportunities, but also raises many legal, ethical, and security-related questions. The key challenges with using AI for decision-making are ensuring legal certainty, protecting personal data, and ensuring cybersecurity.

> **RECOMMENDATION:** Adopt a systemwide law to regulate the use of AI by the public and private sectors, taking into account the EU's Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), recent amendments to certain EU rules, the EU Data Governance Act, the Council of Europe's guidelines on artificial intelligence and data protection, and regulatory arrangements of European countries and US states. This law should integrate the standards of the Republic of Serbia on ethics and principles of artificial intelligence. This document would be crucial to ensure proper/quality use of data, minimize bias and define in which areas AI can be applied and where not.

OBJECTIVE 3: ACHIEVE THE HIGHEST LEVEL OF RELIABILITY AND SECURITY FOR USERS

…BY REGULATING SPECIFIC PERSONAL DATA PROCESSING ARRANGEMENTS

CHALLENGE: Even though the 2019 Personal Data Protection Law is largely aligned with European regulations and standards, the opportunity was missed to use this piece of legislation to regulate personal data processing in special situations or specific areas (such as CCTV recordings, biometric data, employment data, and the like).

RECOMMENDATION: The Personal Data Protection Law, which is the umbrella piece of legislation in this field, should at a minimum regulate fundamental principles for a variety of personal data processing types as required in practice, whereas other specific rules, where appropriate, would regulate the purposes of these specific types of data processing.

…BY STRENGTHENING CYBERSECURITY CAPACITIES

CHALLENGE: Cybersecurity is a major consideration given the importance of data stored in the government's information systems. Successful and sustainable digital transformation of public administration and the private sector that consistently enhances trust and communication with the public and businesses requires robust cybersecurity arrangements.

From a regulatory perspective, progress has been made with adopting expert recommendations for providing better security to public authorities' ICT systems, including the introduction of disaster recovery and business continuity standards for government bodies. Nevertheless, these standards do not seem to be fully implemented, and expert support and training for civil servants about cybersecurity risks seems to be lacking.

RECOMMENDATIONS: Continue implementing these standards and keep assessing the extent of compliance with them by organising cybersecurity drills in public administration. Furthermore, given that any public servant can potentially cause a data breach, it is critical that the Government establishes a **training program on the cybersecurity basics for its employees**. The training program may also include simulated phishing attacks to reduce the number of clicks by government officials on infected links.

It is also necessary to form special teams in individual state bodies responsible for monitoring, prevention, detection, investigation and response to cyber threats - the so-called SOC teams (Security Operation Center), as well as the strengthening of the national CERT (Computer Emergency Response Team). It is recommended that the Government appoint a Chief Information Security Officer (CISO), who would be responsible for the consistent implementation of the information security policy, defining standards/controls to be implemented within state ICT systems based on data sensitivity, as well as establishing a mechanism for information exchange between private and public sector in relation to emerging or current threats.

Finally, the development of new state administration services must be accompanied by analysis and testing regarding the application of appropriate information security standards.

…BY USING CLOUD TECHNOLOGIES

CHALLENGE: Cloud technologies are underutilised in the Serbian public sector, but could be leveraged to improve resilience and ensure business continuity and disaster recovery. International examples reveal migrating government data to the cloud allows greater agility in delivering services, which significantly reduces costs and investment needed to procure, deploy, configure, and maintain systems in the field, such as at data centres and server facilities.

RECOMMENDATIONS: Although government cloud data storage policies vary widely (from complete data localisation, as is the case in Serbia, to hosting most government data and services on commercial cloud platforms, such as in the US, Australia, and Singapore), countering emerging cybersecurity threats, having reliable backups, and accessing additional data storage capacity all require leveraging technology and changing policy to emphasise cloud solutions. **The best examples of these policy shifts include gradually migrating government data to the cloud, based on a risk assessment to categorise data and services and prioritise services with the greatest impact (such as public-oriented services) and non-critical data (including website hosting and publicly available information).** Many of these approaches involve **storing data in the cloud beyond national borders,** focusing on *how* the data are stored, not *where* they are located. Also, in response to users' need for decentralization, privacy and security of

stored data, models of cloud technologies based on blockchain technologies have been developed, which enable the storage of encrypted data in the cloud.

For Serbia, these regulatory changes should include considering more responsive public policies that are reliant on risk-based data classification, whilst phasing out current data localisation policies to ensure less sensitive information is stored on cloud solutions compliant with stringent global data protection and security standards.