4 Adapt the regulatory and policy framework for firms to new digital challenges

Kazakhstan has started to adapt the legal and policy framework for firms to the digital age, in particular regarding personal data and trust standards. However, the slow pace of change combined with frequent and partial amendments to laws, creates additional complexity for firms. In addition, most firms are poorly equipped to manage digital and cyber-security threats. The government has therefore a role to play to support the digital transformation of firms by easing the regulatory environment for firms in relation to digital topics and by developing public tools to raise both the awareness and capacity of firms to manage their digital security risks.

Challenge 5: The pace of adaptation of the regulatory framework to digital issues creates new barriers for firms

Kazakhstan has worked to adapt the legal and policy framework for firms to new challenges brought by the digital era

The digital transformation of governments, businesses and society relies as much on technological innovations, which enables new practices to emerge, as on the trust in the digital economy, which incentivises actors actually to go digital. The regulatory framework has a central role to play in ensuring the quality and adaptability of laws and regulations to the needs and challenges created by emerging digital technologies and uses, such as misappropriation of data or infringement of property and privacy rights. This is of particular importance to support the digital transformation of SMEs, as they are disproportionately affected by inefficiencies in institutions and regulatory frameworks (OECD, n.d.[1]).

In recent years, Kazakhstan has made noteworthy efforts to adapt the legal and policy framework for firms to new digital challenges, in line with its efforts to advance the digital transformation. On the data front in particular, Kazakhstan has been regularly amending its legal framework to gradually move toward the privacy and security standards set by the European Union's General Data Protection Regulation (GDPR) (Government of Kazakhstan, 2013[2]; Government of Kazakhstan, 2017[3]). As part of these efforts, the government created the Information Security Committee under the MDDIAI, mandated with the implementation and monitoring of compliance with the Law on Data Protection (Government of Kazkahstan, 2022[4]). Though the objective was to create a Data Protection Agency following the GDPR model, the Committees' mandate so far focuses mostly on technological solutions to data issues, rather than on legislative and implementation aspects for data protection issues (CAISS, 2020[5]). The new legislative framework also imposes obligations on companies to appoint a data protection officer to ensure internal compliance with the Law, notify the Committee about data breaches, and carry out data protection impact assessments before engaging in any activity requiring the collection and handling of data (Dentons, 2021[6]).

In addition, the government has recognised the need to involve the private sector to adapt regulations in line with new needs created by the digital transformation of businesses and commercial practices. For instance, the process of amending the laws on data and consumer protection, the civil and the copyright code, and the patent law on issues of "cybersquatting" issues for intellectual property rights (IPR) protection all involved both inter-ministerial discussions and consultations with private sector representatives, chiefly represented by Atameken and business associations.

However, the pace of change and simplification of the regulatory environment remains slow and raises new barriers for firms

Despite these reforms, OECD interviews indicate that the regulatory environment is not yet conducive to the digital uptake of firms, as it fails to anticipate and answer the needs of firms, leaves out important aspects of the digital operation of businesses, including e-commerce, and remains difficult for firms to navigate and authorities to implement. Data protection offers a relevant illustration. OECD interviews indicate that successive amendments to the Law on Data Protection have resulted in additional technical requirements that can prove cumbersome for firms, especially for smaller ones, reducing their incentive to operate digitally, without increasing trust from businesses or consumers, because the amendment process has been perceived as opaque and poorly advertised.

More generally, OECD interviews indicated that the pace of change of the regulatory environment remains too slow to adapt efficiently to emerging technologies and the challenges they create for businesses, and too fragmented for firms and public authorities to implement, therefore raising new barriers. For instance, since 2016, the Law on Data Protection has been amended at least five times, while at the time of writing

a new set of amendments relating to data management and data ownership are being drafted and discussed. Business representatives told the OECD team that despite formal involvement of Atameken and other representative associations, they remain poorly aware of the objective and content of the successive amendments. In the cases when they are aware, they indicated that only a small number of provided recommendations were taken into account in the final versions of the law. This has also been echoed by international organisations specialised on the topic (CAISS, 2020[5]; Portulans Institute, 2021[7]). In addition, Kazakhstan remains below the adequacy level of personal data protection as defined by the EU GDPR (CNIL, 2022[8]).

In a similar vein, the regulatory framework governing IPR has not yet been adapted to digital-specific challenges, such as cybersquatting or liability for the sale of counterfeits products on online platforms. While OECD interviews indicate that the Ministry of Justice is aware of this issue, it is unclear whether actual discussions on adapting the IPR protection framework to the digital era have started.

Finally, Kazakhstan is missing a dedicated law on e-commerce and online platforms, which is among the fastest expanding sectors in Kazakhstan and in which a vast majority of SMEs are active. Indeed, general aspects on these matters continue to be regulated by the 2004 law on trading activities (Government of Kazakhstan, 2004[9]), in combination with the laws on consumer rights, digitalisation, and protection of personal data for targeted issues. As a result, many firms are not aware of changes in requirements or opportunities related to their digital operations, which further complicates their operating environment and acts as a disincentive to turn their operations digital. OECD interviews suggest that part of this complexity arises from the regulatory and institutional frameworks themselves, where the responsibilities for e-commerce, data, consumer and IPR protection, and other legal issue are scattered among various ministries and public agencies, each responsible for sub-elements of a law and its implementation.

Recommendation 5: Adapt and streamline the regulatory framework for firms to accompany their digital transformation

The scale of change and scope of Kazakhstan's digitalisation ambitions point toward several challenges for businesses. First, ensuring that the adaptation of the regulatory framework to new needs created by the digital operation of firms does not create a fragmented, incoherent and contradictory operational environment. Second, ensuring that data is regulated in such a way that it allows firms to develop new business models without creating digital security vulnerabilities. The government therefore has a central role to play in maintaining the legal and judicial frameworks within which public administration and markets operate, refraining from the misappropriation of data and infringement of property and privacy rights.

In particular, Kazakhstan could undertake a regulatory review in consultation with the private sector to update all laws relevant to the digital transformation of firms, starting with consumer and data protection, IPR, and e-commerce (Box 4.1). For each topic, the government should aim to consult first with the private sector to gather firm input on the current challenges and gaps in the regulatory framework that prevent them from going fully digital. Formal PPD mechanisms, involving representatives of the private sector such as Atameken and sectoral business associations can be used to that effect, paying close attention to ensure that SMEs are included in such dialogues. Atameken and smaller business associations could support SME participation upfront through dedicated outreach, training and coaching to make their case effectively, as well as offsetting some of the costs for attendance (e.g. *per diems* or fuel allowances).

Once these inputs are gathered, the government should translate them into changes to the concerned laws, taking care to consolidate all changes into one single and coherent piece of legislation. The use of "one-in, X-out" or regulatory guillotine approaches, such as those adopted in several OECD countries, could facilitate the removal of obsolete regulation and contribute to regulatory offsetting (OECD, 2017[10]). However, the use of such approaches, focusing on the quantity of regulations, should not prevent focusing

on the impact and quality of regulations that can only be achieved through regular discussions with the private sector and monitoring (Trnka and Thuerer, 2019[11]).

From a broader perspective, on the data protection front, Kazakhstan could also strengthen its regulatory and institutional framework, moving closer to the European Union's GDPR standards. In particular, establishing a genuine data protection agency could help raise awareness and improve data protection practices for businesses and individuals alike. This would require separating the Information Security Committee from the MDDIAI, to become an independent public authority mandated with supervising the application of the data protection law (European Commission, 2022[12]). The new DPA should be granted investigative and corrective powers to handle complaints, and should provide expert advice on data protection compliance to businesses. On that matter, Kazakhstan could enhance its co-operation with the EU within the framework of the Enhanced Partnership Agreement and the EU Central Asia Strategy.

Box 4.1. Adapting the regulatory framework for businesses to new digital needs

The example of the EU e-Commerce Directive and the Digital Services Act

The e-Commerce Directive, adopted in 2000, provides the basis for digital regulation of trade in the EU single market. Besides basic requirements on mandatory consumer information, steps to follow in online contracting and rules on commercial communications, it also covers more complex matters, including competition.

In 2015, the European Commission has recognised that the digital landscape had undergone profound changes since the early 2000s and raised new challenges for firms, for instance in relation to online intermediaries. The Commission therefore launched a regulatory review to update the digital regulatory framework, ensuring that the fundamental rights of users are protected and that businesses benefit from a level playing field.

- Two public consultations were launched, involving consumers, public authorities, non-governmental organisations, SMEs and other relevant stakeholders for digital matters. Discussions aimed at assessing whether EU rules on e-commerce were still up to date and identifying new challenges faced by European citizens and businesses when buying online.
- Expert groups have then been set-up to discuss issues in the application of the Directive, as well as emerging issues in the area of e-commerce.
- On that basis, in December 2020, the Commission published the proposals for the Digital Services Act, complemented by the Digital Markets Act, a single new set of rules applicable to the digital space across the EU.

Source: (European Commission, 2022[13]; European Commission, 2022[14]).

Challenge 6: A lack of digital culture among firms leaves them vulnerable to digital security risks

Digital security has become a policy priority in recent years

Since 2017, as the digitalisation of the economy has progressed rapidly, Kazakhstan has also started developing digital security policies to reduce the country's vulnerability to cyber threats (Government of Kazakhstan, 2017[15]). In particular, the government launched the Cybersecurity Concept until 2022 ("Cyber Shield of Kazakhstan"), aimed at developing a cybersecurity sector in the country, which was practically non-existent in 2016 (Government of Kazakhstan, 2017[16]). The initiative covered the building blocks of such a strategy, starting with (i) the creation of a national register of trusted digital software and IT products to reduce reliance on foreign solutions; (ii) enhanced international co-operation with internationally recognised private digital security providers and international organisations active in the domain to build local capacity; and (iii) the development of a digital culture for the general population and the training of cybersecurity specialists. Some of the targets of the initiative have been further included in the objectives of the Digital Kazakhstan programme. This year, the government announced the launch of the Cybershield 2.0 programme, incorporating new challenges and aspects of the digital transformation in Kazakhstan, especially on the liberalisation and inclusion of the private sector, law enforcement, security, and defence sectors.

The strategy has been successful so far in creating a cyber-security landscape in the country. On the institutional front, the National Security Council, the Council for Cybersecurity, the Information Security Committee under the MDDIAI and an industry information security centre covering the country's financial sector were created (ITU, 2021[17]). However, OECD interviews indicate that the current institutional architecture can lead to co-ordination issues, while businesses remain poorly aware of the initiatives implemented. Kazakhstan has been actively seeking to expand international co-operation, in particular with the International Telecommunication Union (ITU), and through its involvement in the fourth industrial revolution working group of the World Economic Forum (WEF).

On the private-sector front, several companies are now dealing with cybersecurity issues, and are co-operating with the government to protect critical digital infrastructure, especially on e-government websites. In particular, the Centre for analysis and investigation of cyber-attacks (TSARKA) is operating the "BugBounty" platform, allowing the detection of digital vulnerabilities and cyber threats (TSARKA, 2022[18]). However, OECD interviews indicated that so far only e-government services and large businesses have used this service, as the fee remains prohibitive for SMEs who are also less aware about the existence of the initiative even if SMEs operating in the IT and e-commerce sector might benefit most from such services. The Computer Emergency Response Team (KZ-CERT) has also been created in recent years with a broader mandate, to collect and analyse security incidents reports, and provide consultative and technical assistance to all types of users, including SMEs, in prevention of cyber threats (Computer Emergency Response Team, 2022[19]). In addition, the Information Security Committee under the MDDIAI has been active in providing annual grants and retraining programmes for the unemployed to develop cyber security competencies. According to the Ministry's data, so far 3 000 people have received annual grants to study cyber security, while more than 36 000 people have been retrained in the last six years (Box 4.2).

Box 4.2. Developing cyber security competencies: the example of Kazakhstan's "Cyber Shield"

In 2017, Kazakhstan has adopted the "Cyber Shield" programme to support the development of a digital economy in the country through the development of a legal basis for and a culture of cybersecurity. Public-private working groups have identified several challenges in this regard, in particular insufficient awareness among citizens about cybersecurity threats; a shortage of information security professionals; inadequate information protection infrastructure; risks associated with the provision of electronic public services; and neglect information security requirements by most public and private organizations.

The Committee on Information Security has been implementing the state policy on cybersecurity, with a specific focus on the above-mentioned challenges. Since 2016, the Committee has been most successful in developing a pool of cybersecurity experts across the country, notably by providing grants to study cybersecurity, and free of charge retraining for unemployed to develop cyber-security competencies:

- About 3000 5-year stipends are granted every year for studies related to information and cybersecurity. For instance, in 2021, 2632 scholarships have been granted.
- Retraining for unemployed at the Presidential Academy of the Republic of Kazakhstan. In 2021, the programme accounted for 5921 graduates.

Source: (Government of Kazakhstan, 2022[20]).

However, businesses remain ill-equipped to manage digital security risks

The digital culture of the private sector and its ability to manage digital risks appears to be a central missing link in Kazakhstan's recent digital efforts, following from the rapid development and digitalisation across the country over the past decade, and an absence of policy attention on the matter (CAISS, 2020[5]). The focus of recent efforts on digital security has indeed been directed mainly at state and related entities, such as SOEs in so-called "strategically important" industries. For instance, none of the five dimensions of the Digital Kazakhstan programme addresses issues of data protection or the promotion of digital culture among the general population and firms. Programmes that are aimed at building digital awareness and skills to deal with security risks under the Cyber Shield programme have mostly focused on public servants (Government of Kazakhstan, 2017[21]). As a result, the level of awareness of and the ability to deal with cyber threats of the population and business remains very low, leaving them vulnerable to rising threats (CABAR, 2022[22]). For instance, a recent report of Kazakhstan's banking sector revealed a high level of ignorance of basic digital security recommendations across all levels of staff (Deloitte, 2021[23]).

Businesses and SMEs in particular are vulnerable to these threats, constraining their growth and competitiveness perspectives. For instance, phishing attacks have been rising over recent years, especially in relation to popular services and mailings on behalf of second-tier banks, postal organisations, trading platforms, and online stores. Given that most small enterprises in Kazakhstan only use basic digital tools, such as email services and online sale platforms, they are at the forefront of these attacks. The use of malicious software is also on the rise, about 2500 incidents related to this threat were reported to, and processed by, the National Computer Incident Response Service KZ-CERT in 2020, a 6% increase compared to 2019 (Government of Kazakhstan, 2021[24]). Beyond these, and despite the lack of precise and recent data, OECD interviews confirm that targeted attacks remain a big threat to Kazakh businesses. This problem was already flagged in 2016 by Kaspersky Lab, which found that 39% of Kazakh companies had lost access to business information as a result of cyber-attacks and that each corporate computer in the country had been subjected to an average of 13 malware attacks during the first half of 2016 (Kazakhstan Today, 2017[25]). By 2019, improvements remained limited, as Kaspersky Lab found that 92%

of organisations in Kazakhstan had been exposed to an external cyber-attack at least once, while 66% of companies faced internal threats to information security (Kaspersky Lab, 2021[26]). Interviews conducted by the OECD also indicated that the trend seems to have been on the rise since the pandemic, as many more businesses have turned parts of their operations online.

OECD interviews indicate that, as in many OECD and partner countries, a majority of business in Kazakhstan do not have digital security risk management practices, even at the most basic level, and are not necessarily aware of the benefits of integrating them into their business processes. For instance, many businesses do not have a dedicated person in-house, do not seek information from external sources, and do not tend to have formal procedures in place to detect intrusions. Only a few businesses, mainly large ones, are using the services of security consultancies, as the price of these initiatives remains high for smaller businesses to be able and willing to use them. In particular, if the mandate of KZ-CERT covers the provision of consultative and technical assistance to users in prevention of cyber threats, and their website indicates specific measures for SMEs (Computer Emergency Response Team, 2022[19]), OECD interviews suggest that few SMEs are aware of this service and have actually used it.

Recommendation 6: Build firms' awareness of, and capacity to manage, digital security risks

Enabling SMEs to be more aware of and effectively manage digital risk is crucial for them to make the most of the opportunities offered by the digital transformation (OECD, 2015[27]; OECD, n.d.[1]). For Kazakhstan's digital strategy to reach its targets of a secure and digital society, building a digital culture and equipping firms with the tools to manage their digital security risks will be essential. Doing so would require encouraging the adoption of better digital security practices among SMEs through dedicated public utilities, supporting the supply and use of business solutions to and by SMEs, and integrating SME policy considerations in the Cyber Shield strategy.

Many governments across OECD and partner countries have increasingly developed certification schemes, security standards and enforced personal data protection regulation to support businesses at large on the digital security front. However, SMEs are the most vulnerable firms in these respects, and specifically designed initiatives to raise their awareness and build their competences in digital security remains essential. Kazakhstan could expand the advisory and training offer for firms on digital security risk management offered by KZ-CERT. This could involve dedicated agencies (e.g. DAMU or Atameken), thereby following the practices of many OECD countries where SME agencies have taken a leading role to initiate a change in culture and practices of small businesses and equip them with the tools to manage their digital security risks (Box 4.3). The offer of advisory services could be developed either within agencies to provide SMEs with information about digital security risks and training tools (online and offline) to integrate such practices in their business processes, or by creating a register of certified external consultants SMEs could reach out to. All available support should be made easily accessible on the website of the implementing agency and publicised to ensure actual use by SMEs. Alternatively, or in complement, all advisory services and tools could also be made available on the "Government for Business" website.

On the demand side, the government should support preferential access to these services, to ensure wide uptake by small firms, and it could consider cost-sharing options via either DAMU or a dedicated budget line under the new phase of the Cyber Shield. For instance, training and advisory services could initially be provided either free of charge or at a subsidised rate, as SMEs often find it difficult to obtain the funding needed. Since trust in the quality of the services provided might also be limited in the beginning, vouchers or tax breaks for SMEs can also support the creation of a private market for advisory services. The government could leverage the experience of SMEs that are already actively using digital risk management practices in order to create networks of good practices and expertise. On the supply-side, Kazakhstan

could also design similar incentives for developing business solutions that could help SMEs improve digital security risk management, as well as adapting regulations to support the production of more secure digital products.

Finally, Kazakhstan could integrate SME digital security considerations either in the new phase of the Cyber Shield initiative, or directly as part of the next iteration of the NDS. In line with the 2015 OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity, doing so is essential to integrate SME-specific needs in strategy design and implementation, and minimise especially governance failures between digital security agencies and SME policy instances (OECD, n.d.[1]).

Box 4.3. Governments can support the digital culture of the private sector

Governments can support the improvement of the overall level of digital security in markets by acting on (i) the supply-side to encourage businesses to offer existing/novel digital security solutions, (ii) the demand-side to encourage businesses adopt better digital security risk management practices, (iii) the digital culture and cybersecurity skills of the population and businesses at large.

- On the supply-side, digital security solutions have mostly been encouraged by the development of regulations to enhance "security by design" or "privacy by design" features in IT products, and financial incentives as well as cluster ecosystems to develop new digital security technologies.
- On the demand-side, policies aim at setting rules and guidelines for data management, reducing information asymmetry for adopters of digital security products, and enhancing business capacity to manage their digital risks. In the first two instances, changes to regulation and legislations as well as the setting of security standards and procedures are the most widely used policy instruments. For the last, most OECD countries have entrusted their SME agencies to develop business advisory services and informational resources.
- Building digital culture and skills for cybersecurity has been mainly achieved through the provision of educational material and trainings, awareness campaigns on digital security risks and good practices, and the building of a knowledge base on digital security risks through Computer Emergency Response Teams (CERT).

Selected examples of SME-specific tools

- As a part of its 2020 Cyber Security Strategy, the Australian Cyber Security Centre has been mandated to offer both guidance on *what* SMEs should be doing, and on *how* they should implement a digital security strategy, with tailored toolkits (e.g. digital maturity assessments), matchmaking between digital security providers and SMEs, and grants available at each step of the process.
- The Belgian Federal Public Service for the Economy, SMEs, Middle Classes and Energy also offers an online set of resources to inform and assist SMEs in digital security matters, including documents on undertaking risk assessments, key principles for ensuring digital security, what to do in the event of an incident and a glossary of key technical terms.
- In Germany, the SME Go-Digital initiative launched in 2017 by the Federal Ministry for Economic Affairs developed a digital one-stop-shop where SMEs can receive diagnostic and targeted training programmes on digital security, with a reimbursement of 50% of the costs of the training.
- Chile's National Cybersecurity Policy includes the design of a large-scale cybersecurity campaign to promote the implementation of awareness and dissemination programmes in partnership with the private sector.

Source: Adapted from (OECD, n.d.[1]; Belgian Federal Public Service for the Economy, SMEs, Middle Classes and Energy, 2018[28]; Government of Chile, 2018[29]).

References

Belgian Federal Public Service for the Economy, SMEs, Middle Classes and Energy (2018), *Cybersecurity – is your enterprise ready?*, https://economie.fgov.be/fr/publications/cybersecurite-votre-entreprise. [28]

CABAR (2022), *How Digitalisation Became a Cyber Security Threat in Kazakhstan*, https://cabar.asia/en/how-digitalisation-became-a-cyber-security-threat-in-kazakhstan (accessed on 2 June 2022). [22]

CAISS (2020), *Protection of personal data in Kazakhstan: status, risks and opportunities (Защита персональных данных в Казахстане: статус, риски и возможности)*, https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf. [5]

CNIL (2022), *Map of data protection around the world*, https://www.cnil.fr/en/data-protection-around-the-world (accessed on 15 July 2022). [8]

Computer Emergency Response Team (2022), *Computer Emergency Response Team*, https://www.cert.gov.kz/about/kz_cert (accessed on 20 July 2022). [19]

Deloitte (2021), *Assessment of cyber risks in banks of Kazakhstan*, https://www2.deloitte.com/kz/ru/pages/risk/articles/cyber_risk_assessment_kazakhstan_banks.html. [23]

Dentons (2021), *The impact of the GDPR in Kazakhstan*, https://www.dentons.com/en/insights/alerts/2021/may/5/the-impact-of-the-gdpr-in-kazakhstan. [6]

European Commission (2022), *Shaping Europe's digital future - e-Commerce Directive*, https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive (accessed on 31 May 2022). [13]

European Commission (2022), *Shaping Europe's Digital Future - The Digital Services Act package*, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed on 31 May 2022). [14]

European Commission (2022), *What are Data Protection Authorities (DPAs)?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (accessed on 18 July 2022). [12]

Government of Chile (2018), *National Cybersecurity Policy*, https://www.ciberseguridad.gob.cl/media/2017/05/NCSP-ENG.pdf. [29]

Government of Kazakhstan (2022), *В 2022 году будет принята новая редакция концепции «Киберщит Казахстана»*. [20]

Government of Kazakhstan (2021), *Phishing websites, spear-phishing, whaling — Cyber Shield of Kazakhstan improves security systems*, https://www.primeminister.kz/en/news/reviews/phishing-websites-spear-phishing-whaling-cyber-shield-of-kazakhstan-improves-security-systems7698 (accessed on 21 July 2022). [24]

Government of Kazakhstan (2017), *Approval of the Cybersecurity Concept ("Cyber Shield of Kazakhstan"), Resolution by the Government of the Republic of Kazakhstan No. 407*, https://adilet.zan.kz/rus/docs/P1700000407 (accessed on 31 May 2022). [16]

Government of Kazakhstan (2017), *Law "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Regulation of Digital Technologies", 25 June 2020*, https://adilet.zan.kz/eng/docs/Z1700000051 (accessed on 6 July 2022). [3]

Government of Kazakhstan (2017), *State of the Nation Address*, https://www.akorda.kz/en/addresses/addresses_of_president/the-president-of-kazakhstan-nursultan-nazarbayevs-address-to-the-nation-of-kazakhstan-january-31-2017 (accessed on 13 July 2022). [15]

Government of Kazakhstan (2017), *State programme "Digital Kazakhstan:*, https://digitalkz.kz/wp-content/uploads/2020/03/%D0%93%D0%9F%20%D0%A6%D0%9A%20%D0%BD%D0%B0%20%D0%B0%D0%BD%D0%B3%D0%BB%2003,06,2020.pdf. [21]

Government of Kazakhstan (2013), *Law of the Republic of Kazakhstan dated 21 May 2013 On personal data and their protection*, https://adilet.zan.kz/eng/docs/Z1300000094#:~:text=The%20Law%20of%20the%20Republic,94%2DV.&text=This%20Law%20regulates%20the%20public,and%20protection%20of%20personal%20data. (accessed on 7 July 2022). [2]

Government of Kazakhstan (2004), *Law "On the regulation of trading activities" dated April 12, 2004 No. 544-II*, https://adilet.zan.kz/eng/docs/Z040000544_ (accessed on 1 June 2022). [9]

Government of Kazkahstan (2022), *Information Security Committee under the Ministry of Digital Development, Innovation and Aerospace Industry*, https://www.gov.kz/memleket/entities/infsecurity/activities/directions?lang=en (accessed on 12 July 2022). [4]

ITU (2021), *How Kazakhstan Efficiently Implements Its National Cybersecurity Strategy*, https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/News/20210810.aspx (accessed on 1 June 2022). [17]

Kaspersky Lab (2021), *Kaspersky Security Bulletin 2021 Statistics*, https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf. [26]

Kazakhstan Today (2017), *One in three companies in Kazakhstan loses critical data to cyber-attacks (Каждая третья компания в Казахстане теряет важные данные из-за кибератак)*, https://www.kt.kz/rus/reviews/kazhdaja_tretjja_kompanija_v_kazahstane_terjaet_vazhnie_dannie_izza_kiberatak_1153624177.html (accessed on 11 July 2022). [25]

OECD (2017), *Regulatory Policy in Korea: Towards Better Regulation*, OECD Reviews of Regulatory Reform, OECD Publishing, Paris, https://doi.org/10.1787/9789264274600-en. [10]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://doi.org/10.1787/9789264245471-en. [27]

OECD (n.d.), *OECD Studies on SMEs and Entrepreneurship*, OECD Publishing, Paris, https://doi.org/10.1787/20780990. [1]

Portulans Institute (2021), *Network Readiness Index - Kazakhstan Country Profile*, https://networkreadinessindex.org/country/kazakhstan/. [7]

Trnka, D. and Y. Thuerer (2019), "One-In, X-Out: Regulatory offsetting in selected OECD countries", *OECD Regulatory Policy Working Papers*, No. 11, OECD Publishing, Paris, https://doi.org/10.1787/67d71764-en. [11]

TSARKA (2022), *Center for analysis and investigation of cyber attacks*, https://cybersec.kz/en (accessed on 19 July 2022). [18]