Chapter 5

ENHANCING TRUST IN THE DIGITAL ECONOMY

Latvia's digital security policies

This section provides an overarching description and analysis of digital security policy in Latvia. The first *Cyber Security Strategy of Latvia*, covering the period 2014-18, took stock of the digital transformation, and marked a shift towards a more strategic and whole-of-government approach to digital security. The second *Cyber Security Strategy of Latvia*, covering 2019-22, continues this trajectory, with a greater emphasis on risk management, resilience, public awareness, and the need to balance digital security with openness, prosperity and human rights.

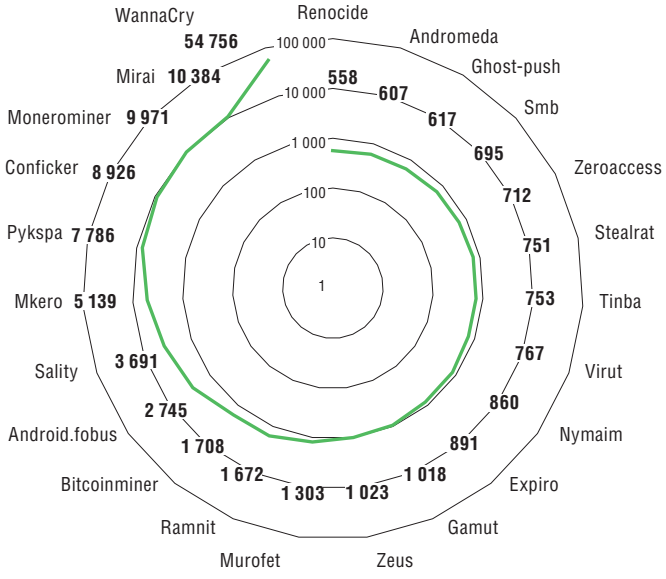
These strategies are representative of the advancement in the Latvian government's approach to digital security policy. However, the economic and social risks of digital security are not yet fully integrated into these documents or their processes for implementation. In fact, Latvia's geopolitical environment has led the government to rely mainly on a national security conceptual framework that focuses on critical infrastructures and state institutions. Multi-stakeholder engagement and market-oriented policies could be strengthened in order to fully realise the potential of the digital transformation. This would also help increase the ownership of digital security risk by senior leadership in organisations and businesses, especially SMEs.

Recent trends

Digital security attacks in Latvia

In 2018-19, media attention in Latvia focused on attacks by politically motivated entities from countries "having an opposite political ideology to that of NATO and the EU" (CERT.LV, 2018). Examples include operations targeting the electoral process in the Saeima, Latvia's Parliament. However, a thorough analysis suggests that, like many other countries, Latvia suffered from attacks which had a more global reach, such as WannaCry and Mirai[1] (Figure 5.1). However, the number of organisations affected by such attacks in Latvia was relatively low. The main victims of digital security incidents in Latvia were small and medium enterprises (SMEs) and municipalities (CERT.LV, 2018).

Figure 5.1. Most common malicious code attacks in Latvia, 2018

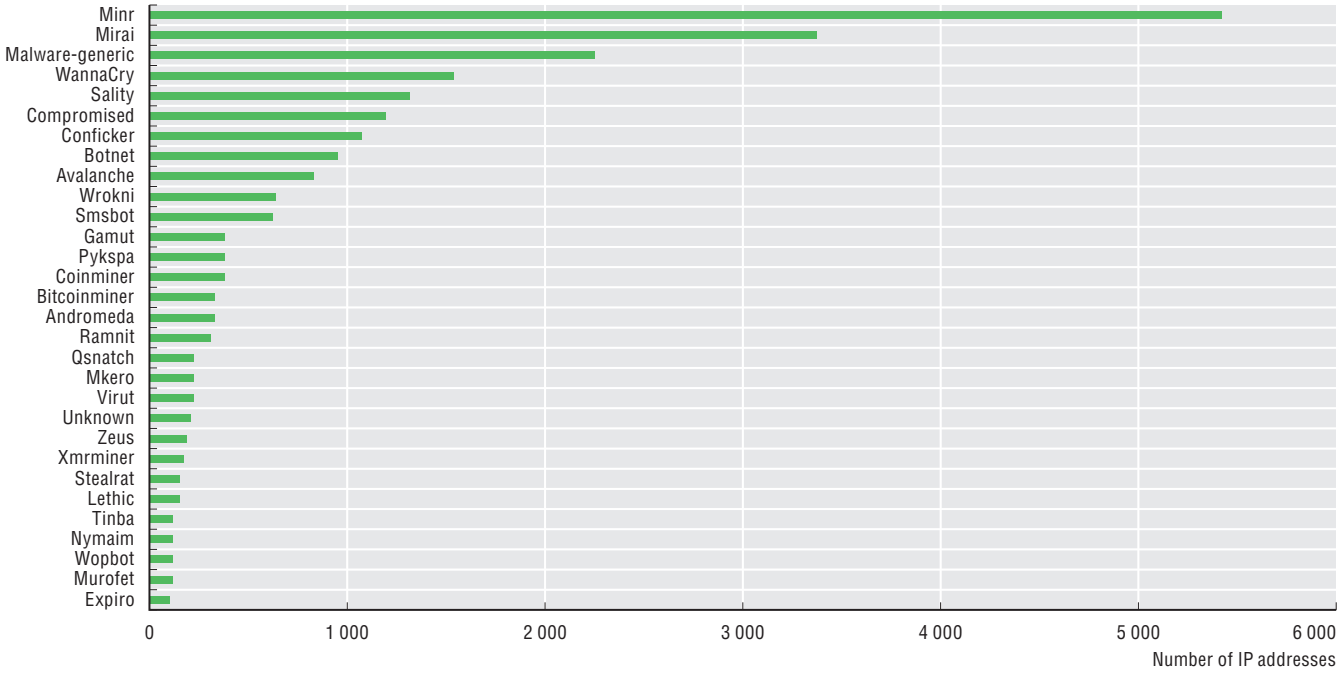


Source: CERT.LV (2018), *CERT.LV Public Performance Report*, *https://cert.lv/uploads/cert-gada-parskats-2019.pdf*.

More recent data (Figure 5.2) confirm that the main forms of malware targeting Latvian organisations match those in other countries, with Mirai and WannaCry being, respectively, the second and fourth most common malwares in the first quarter of 2020. The dominant position of Minr as the most common malicious code in Latvia during this period illustrates the global trend of cryptocurrency mining malware.

Figure 5.2. Most common malicious code attacks in Latvia, Q1 2020

Number of unique IP addresses threatened by malicious code



Source: CERT.LV (2020), *CERT.LV reģistrētie incidenti no 01.01.2020. līdz 31.03.2020*, *https://cert.lv/lv/2020/04/pieejama-statistika-par-2020-gada-1-ceturksni*.

Key dates for digital security policy in Latvi

Digital security is a not a new policy area in Latvia. Prior to 2012, the Latvian approach to digital security focused mainly on technical aspects and infrastructure. The Ministry of Transport (MoT) was the institution responsible for overall co-ordination of digital security policy.

In 2010, Latvia adopted the Law on the Security of Information Technology ("IT security law"), which entered into force in 2011 and serves as the main legal framework for digital security (see the section on the legal framework). It resulted, *inter alia*, in the establishment of:

- the Latvian Computer Emergency Response Team, CERT.LV,[2] which is hosted by the Institute of Mathematics and Computer Science of the University of Latvia and was placed under the authority of the Ministry of Defence
- the National Information Technology Security Council (NITSC), a body which meets at least once every four months and is mainly composed of high-level representatives of ministries and other public organisations involved in digital security policy.

In 2013, the Latvian Cabinet of Ministers approved the *Information Society Development Guidelines 2014-2020* (VARAM, 2014), which serve as a national digital strategy. The adoption of the guidelines represented in shift in perspective with the recognition that digitalisation affects all parts of society. Digital security risks became a strategic public policy issue requiring the involvement of many ministries through a whole-of-government approach.

This shift was confirmed in 2014 with the adoption of the *Cyber Security Strategy of Latvia (2014-2018)*, which states that "the idea that ICT is a matter of interest of just a small groups of professionals has been gradually substituted by the understanding that the entire society is, to a greater or lesser extent, linked with ICT" (MoD, 2014). Logically, the first objective of the strategy was to build a clear governance framework for digital security in Latvia. This new governance framework was structured around the NITSC, under the overarching supervision of the Ministry of Defence (MoD), which took over the co-ordinating role in the definition and implementation of the digital security policy in Latvia.

In 2016, the MoD, in co-operation with other ministries and the NITSC, undertook a mid-term review of the implementation of the strategy; then, in 2019, the Latvian Cabinet of Ministers approved a report on the strategy's implementation which considered that most of the objectives had been met or are in the process of being executed. However, the report also recognised obstacles to meeting certain objectives, in particular: 1) that digital security is not always a priority for decision makers; 2) a lack of digital security skills; and 3) a lack of funding for digital security.

Building on these elements, in 2019 the Latvian Cabinet of Ministers the second *Cyber Security Strategy of Latvia (2019-2022)*. Prepared by the MoD in co-operation with other ministries and the NITSC, this document sets out the national priorities for digital security policy in Latvia and identifies upcoming challenges. The new strategy's main objective is to strengthen and improve digital security capabilities by boosting resilience against attacks and enhancing public awareness of threats in cyberspace.

This reflects a positive evolution in Latvia's approach to digital security. The development of the two cyber security strategies and the leadership role played by the MoD since 2013 has made digital security a strategic priority in Latvia. However, national security has been foregrounded at the expense of other aspects, notably economic and social prosperity (Figure 5.3). This is confirmed by an analysis of the set of definitions related to digital security provided in Latvian policy documents (see next subsection).

Digital security and associated terms in Latvia's policies

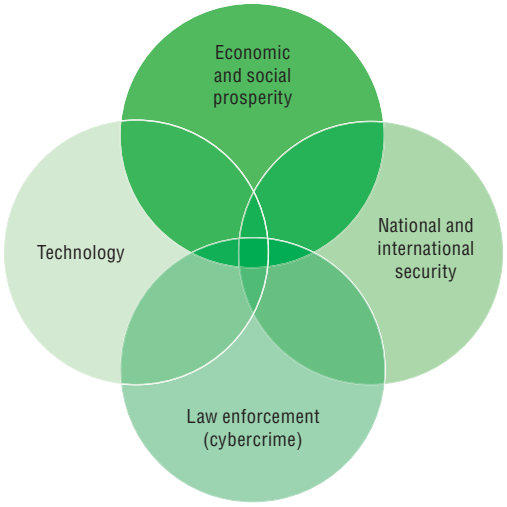
Latvian policy documents rely on the concepts of "cyber security", "security of information technologies" and "information security" (MoD, 2014; VARAM, 2014).

In its 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, thereafter "the 2015 Recommendation" (OECD, 2015), the OECD uses the term "digital security" rather than "cyber security", "information security" or "IT security". The OECD defines "digital security" as the management of economic and social risks resulting from breaches of availability, integrity and confidentiality (AIC) of information and communication technologies (ICTs) and data. This definition represented a shift from the 2002 OECD *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* ("Security Guidelines") (OECD, 2002), which focused mostly on technical aspects rather than managing digital security risks to economic and social activities reliant on the use of ICTs.

However, there is no universally agreed terminology to capture the different facets of digital security in every context. Terms vary across countries, and reflect different government cultures and histories: there is no "right" or "wrong" terminology. In 2015, OECD countries favoured "digital" over "cyber" as the latter is often associated with concepts such as "cyber warfare", "cyber defence" or "cyber influence". Furthermore, "cyber" is absent from economic circles, which more generally stick to the digital semantic: digital economy, digital transformation, digitalisation and so on. "Digital" facilitates the recognition of "digital security" as an economic issue by policy makers and business leaders. "Information security" was left aside as a technical management term primarily reflecting the view of the technical community (e.g. ISO/IEC 27000 Information Security Management Systems standards). "Information security" also carries ambiguity in an international context as it has a different scope in countries such as the People's Republic of China and the Russian Federation, which use it also to capture policies against disinformation, influence and information manipulation. Disinformation, influence and the spread of harmful content are important issues exacerbated by the digital transformation. They can sometimes overlap with digital security, for example, when digital security attacks are used to alter the integrity of data in order to manipulate public opinion or to prevent access to government services. They are, however, different from the management of the economic and social consequences of breaches of AIC, as they involve different policy tools and legal considerations related to free speech and media regulation.

Beyond semantics, the communities addressing each dimension of digital security (Figure 5.3) often have different cultures and backgrounds, and their objectives can sometimes converge, overlap or compete, depending on the context and precise issue. Cryptography policy (OECD, 1998) is a typical example of competing objectives, with businesses, organisations and consumers promoting the unregulated use of cryptography to support trust and facilitate e-commerce, digital governments and innovation online, while law enforcement and intelligence agencies advocate regulation to facilitate access to encrypted data in order to combat criminals and terrorism.

Figure 5.3. The four dimensions of "cybersecurity"



In Latvian policy documents, the concepts of "cyber security", "IT security" and "information security" seem to refer, depending on the context, to either one of these definitions:

- the protection of technical assets, such as networks, ICTs and data (the "Technology" facet of Figure 5.3)
- the management of risks related to the use of ICTs, which do not focus on economic and social activities, but instead touch upon issues relating to national security, influence over strategies in democratic elections and harmful content (the "National security" and "Law enforcement" facets of Figure 5.3).

For instance, the *Cyber Security Strategy of Latvia (2014-2018)* defined cyber security as "the collection of tools, policies, concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets". Alternatively, the *Cyber Security Strategy of Latvia (2019-2022)* relies on a "vision of cyber security policy as a secure, open, free and reliable cyberspace that guarantees the safe, reliable and continuous receipt and delivery of services essential to the state and society, and respects the individual's human rights in a physical and virtual environment". The latter document also acknowledges that "Latvia needs to take advantage of the digital environment to ensure economic and social welfare, while at the same time reducing the overall level of cybersecurity risk without unnecessarily limiting the flow of technology, communications and data".

This shift is a positive development, with the Latvian government now recognising that digital security impacts other aspects of the digital economy (openness, freedom), suggesting that a risk-based approach is warranted and that trade-offs are necessary. The strategy also acknowledges the emergence of cyber-physical systems, which make the virtual (or "cyberspace")/physical dichotomy less relevant, as more and more economic and social activities "go digital". Overall, this semantic evolution reflects a deeper change in the way that Latvia approaches digital security, recognising it as an enabler of the digital transformation, rather than as an end in itself.

Governance

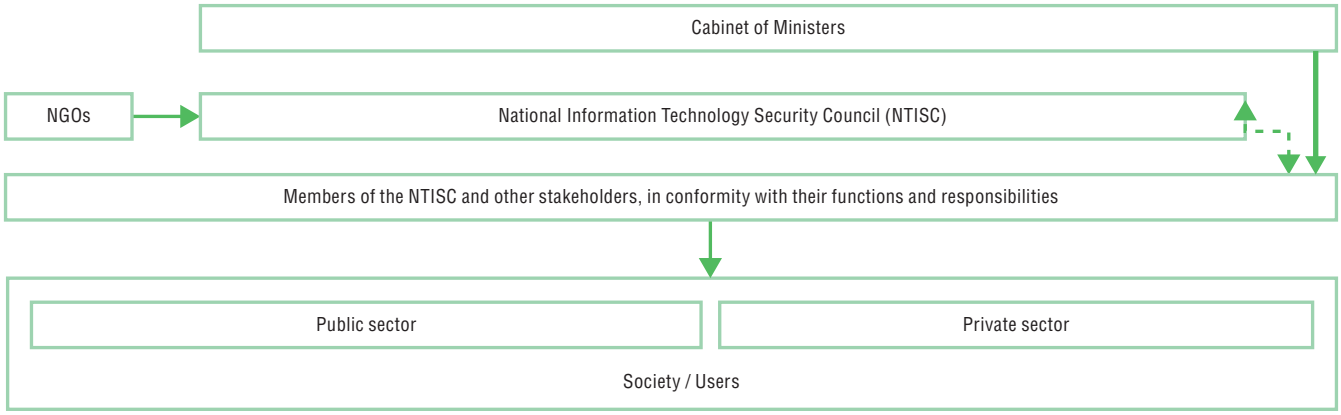
Overall governance framework for digital security policy in Latvia

Since 2014, the MoD has co-ordinated the development and implementation of digital security policy, involving many ministries across the Latvian government.[3]

In order to co-ordinate the development of policies related to digital security in Latvia, and manage potential conflicts between institutions, the NITSC was established. This council has been described alternatively as a permanent high-level working group and a formal body. The NITSC is chaired by the MoD, usually at the level of the Secretary of State. It meets at least once every four months and gathers together – usually high-level – representatives from numerous institutions, including ministries and

law enforcement agencies. Other stakeholders are invited to participate on an ad-hoc basis,[4] as the main function of the NITSC is to ensure effective intragovernmental co-operation. Figure 5.4 provides a visual representation of the governance framework for digital security in Latvia (MoD, 2019).

Figure 5.4. Digital security governance framework for Latvia (2019-2022)



Note: NGO = non-governmental organisation.

Source: MoD (2019), *Cyber Security Strategy of Latvia (2019-2022)*, *https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf*.

The NITSC has no specific dedicated budget, and administrative support is provided by the MoD. The National Cyber Security Policy Co-ordination (CSPC) section within the MoD provides support on behalf of the secretariat for the NITSC. The MoD also ensures the work of the Supervisory Committee of Electronic Identification.

The Ministry of Foreign Affairs (MFA) co-ordinates digital security-related international co-operation, with the involvement of the MoD for NATO and EU-related digital security issues.

The Ministry of Environmental Protection and Regional Development (VARAM) is responsible for state information systems and co-ordinates the digitisation of public services. The State Regional Development Agency (SRDA) ensures the operation and development of solutions for shared use of state ICT, including the national eID and digital signature platform, the national eIDAS gateway, the public procurement system and the public services portal Latvija.lv as well as the official eAddress solution. The VARAM also leads the overall development of a digital and information society policy, and the Deputy State Secretary of VARAM is the deputy chair of the NITSC.

The Ministry of the Interior (MoI) and the State Police (SP) implement law enforcement policies to tackle cybercrime.

CERT.LV provides support to state authorities in the detection of digital security incidents. CERT.LV is also responsible for organising responses in the event of digital security incidents, including crisis management. It monitors and analyses developments in digital security, produces statistics on and reacts to incidents and co-ordinates their prevention, carries out research, organises educational events and training, and supervises the implementation of obligations specified under the Law on the Security of Information Technology. Beyond its primary mission to provide support for public institutions, CERT.LV also supports entrepreneurs and individuals. The budget of CERT.LV has increased significantly over recent years, from approximately EUR 120 000 in 2011 to EUR 882 000 in 2015 and 1 328 000 in 2019, reflecting the commitment of the Latvian government to increasing digital security capabilities.

The Constitution Protection Bureau (CPB), the national intelligence and security agency, oversees the protection of critical infrastructures. The CPB also actively participates in co-operation initiatives between the Baltic States and the United States, by providing expertise and guidance in the field of critical energy infrastructure. CPB and CERT.LV work together to test the resilience of critical information technology infrastructures and provide guidance to public and private operators of such infrastructures.

The Ministry of Welfare (MoW) implements social policy and policy for the protection of children online.

The Latvian State Radio and Television Centre (LSRTC), a state joint-stock company, is the only provider of qualified trust services (i.e. electronic signatures, seals and forms of identification).

The National Armed Forces (NAF) and the National Guard Cyber Defence Unit (CDU) provide support in the event of crises. While the main responsibility of NAF is to develop and strengthen military information technology and communication systems and networks, NAF also plays a significant role in enhancing overall cyber defence capabilities.

Towards a whole-of-government and multi-stakeholder approach

In order for digital security strategies to be successful, it is necessary to engage effectively with all relevant actors across government *and* within the broader multi-stakeholder community (i.e. instance researchers, businesses, civil society, etc.). While many strategies recognise the importance of this two-pronged approach (whole-of-government co-ordination and multi-stakeholder engagement), effective implementation can prove challenging, as it requires adequate resources, trust and, sometimes, a cultural shift.

The current governance framework for digital security policy in Latvia, described in the previous section, partially fits the whole-of-government approach, and could be described as "partially centralised" (MoD, 2014). The creation and implementation of this framework in 2012-14 marked a turning point in Latvia's approach: digital security was no longer considered solely a technical problem of institutions in charge of networks (the Ministry of Transport); instead, it became a public policy issue requiring the involvement of the entire government.

Within this framework, the Latvian approach, so far, has consisted of emphasising national security aspects, which has helped digital security risk gain momentum as a key policy issue, and leveraging resources within government. As an illustration, the NITSC is chaired by the Secretary of State of the MoD, which in turn supervises CERT.LV.

While this approach has brought undeniable benefits, it also has some shortcomings. Approaching digital security mainly through a national security framework may limit the ability of stakeholders to fully engage and own digital security risk, as national security is often associated with state matters. For instance, industry and civil society stakeholders are usually only invited on an ad-hoc basis to NITSC meetings, and do not participate in the design and implementation of the strategy. While stakeholders are invited to participate in this process through public comments, effective participation is often low. Such limited engagement could result from a lack of long-term, trust-based and sustainable multi-stakeholder partnerships, which are fundamental to enabling meaningful and effective participation (OECD, 2015). It could also result from an insufficiently co-ordinated and structured multi-stakeholder community. The national security focus may also limit the ability of other parts of the government to approach digital security as an economic opportunity (e.g. research, innovation, skills entrepreneurship, etc.). If there is insufficient co-operation with and involvement on the part of ministries in charge of economic development and sectoral co-ordination, there is also a risk that these ministries will not develop the requisite technical skills and understanding of the challenges involved, to participate meaningfully in the design and implementation of the digital security strategy.

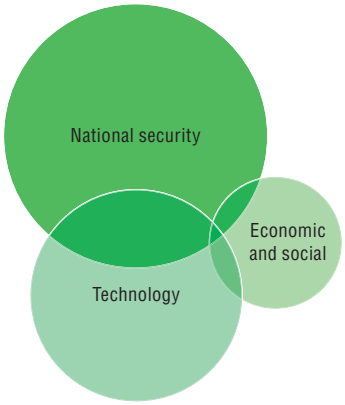
To summarise, the current approach in Latvia (Figure 5.5) is structured around a national security framework (NITSC) which relies on a strong technical foundation (CERT.LV). However, the economic and social dimension seems less present, and the policy is usually implemented through a technical (via CERT.LV) or national security lens.

Most governments have struggled to establish an appropriate governance framework for digital security, as it is difficult to strike the right balance between economic and social concerns, national security, law enforcement and technical facets (Figure 5.3). There is no one-size-fits-all model, and governance frameworks and co-ordination mechanisms vary considerably across OECD countries, reflecting national history, geopolitical context, style of government and maturity in this area.

In many OECD countries, the process of building a digital security governance framework often starts with the national security, cybercrime (e.g. adoption of a cybercrime legislation) or technological dimension, focusing on increasing technical response capacity, for example through creating a computer emergency response team (CERT). The process then expands gradually to encompass economic and

social prosperity. However, some countries reached a consensus that national security-oriented agencies were not necessarily best placed to develop and implement economic and social policies, arguing that this was not their core mission and that they too often lacked the culture of transparency and multi-stakeholder engagement essential to building trust-based and sustainable partnerships.

Figure 5.5. Digital security policy in Latvia



Notes: This figure illustrates the degree of government attention to three of the four components of the digital security framework, as shown in Figure 5.3. Criminal law enforcement, which is included in Latvia's current framework, is not shown as it is beyond the scope of this review.

In order to address all facets of cyber security holistically, rather than in a fragmented manner, digital security strategies must be supported at the highest level of government (i.e. the head of state or head of government), and establish new governance and co-ordination mechanisms to ensure balance between complementary and sometimes competing objectives across the different dimensions (OECD, 2015; 2012) However, each country must adopt a governance model tailored to its culture and style of government.

For example, Australia, Japan and the United Kingdom assigned policy co-ordination to the Prime Minister through the Cabinet Office. France established a national co-ordination agency within a pre-existing co-ordination body under the Prime Minister (ANSSI). The United States set up a "Cybersecurity and Infrastructure Security Agency" (CISA) within the Department of Homeland Security. Canada, Germany and the Netherlands placed the main responsibility for digital security under an existing ministry (respectively, the ministries of Public Safety, the Interior, and Security and Justice). Israel created a national agency reporting directly to the Prime Minister (INCD).

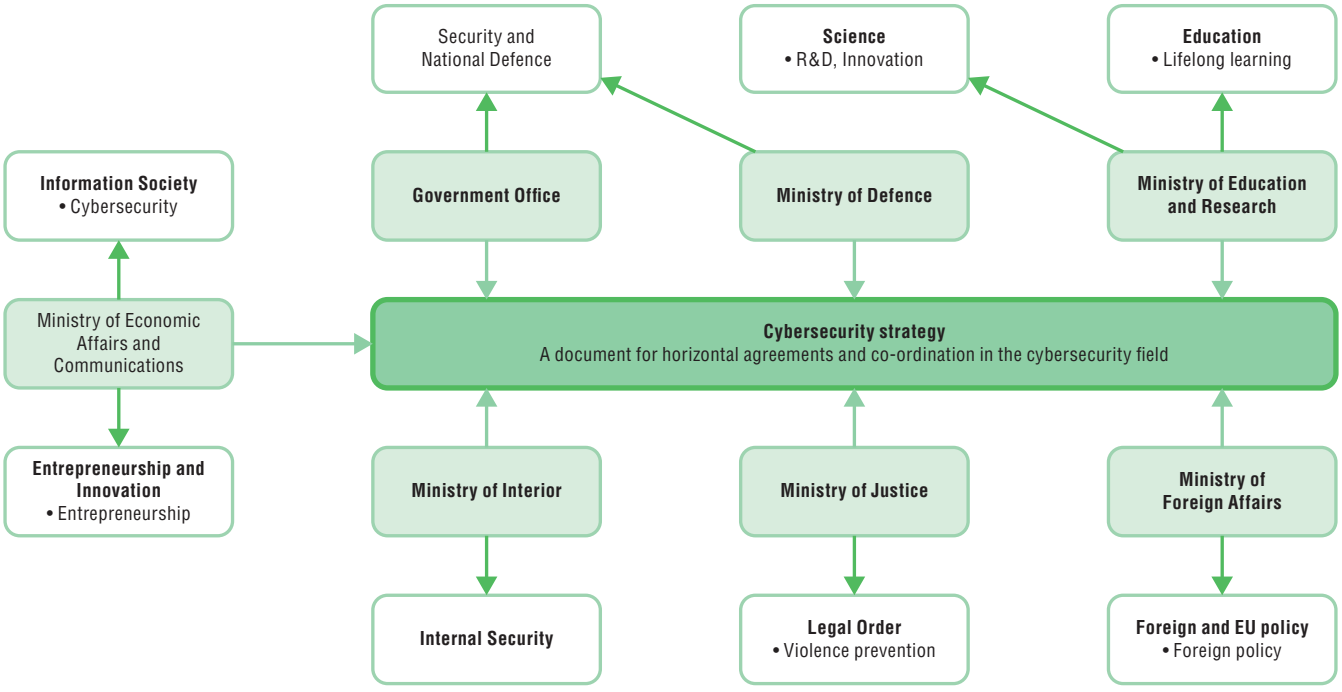
In Denmark, responsibility for overall co-ordination of the digital security strategy is split between the Agency for Digitisation (within the MoF) and the Centre for Cyber Security (MoD). The agency is in charge of digital security in the public sector and is responsible for a number of citizen-focused initiatives. The centre advises public authorities and private companies that support critical activities. The agency chaired the working group that developed the digital security strategy.

In Estonia, the Ministry of Economic Affairs is in charge of co-ordinating the development and implementation of digital security policy (Figure 5.6). The other ministries (Defence, Research, Education, Interior, Justice, etc.) are also fully involved within their own domain of competence.

In all these cases, there are also different arrangements with respect to how multi-stakeholder co-ordination is concretely carried out, and where government operational capacity is located. This ranges from within the policy co-ordination agency (France, Israel) to a sub-structure attached or reporting to the ministry (Germany, the Netherlands), or a separate structure (the UK National Cyber Security Centre). Furthermore, policies to foster the digital security of critical activities and infrastructure create a need to engage sectoral regulators (e.g. in the telecommunications, health, finance, transport and energy sectors) to ensure that related digital security regulation takes into account existing market and regulatory constraints.

Economic-oriented and multi-stakeholder-driven initiatives have been launched in many OECD countries. Governments have facilitated sector-specific partnerships aimed at sharing information and best practices for digital security challenges, for example through Information Sharing and Analysis Centres (ISAC). Another good practice is to launch partnerships with Internet service providers (ISPs) and other stakeholders to detect and clean infected connected devices. For instance, the Dutch Government has taken steps to monitor and enhance the digital security of connected devices through a public-private partnership that includes ISPs, the Ministry of Economic Affairs and the University of Delft. The goal of this initiative is to share information across manufacturers/vendors as well as with end users, to encourage product distributors to consider removing affected products from the shelves, and incentivise consumers to patch or deactivate products if critical vulnerabilities are discovered.

Figure 5.6. Governance framework for digital security policy in Estonia



Source: MoEAC (2019), *Cyber Security Strategy of Estonia (2019-2022)*, *www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

In Latvia, the current governance framework is indicative of a willingness to engage with the multi-stakeholder community, although the means to ensure their effective participation could be enhanced. While the NITSC is described in the *Cyber Security Strategy* as "the central national authority for the exchange of information and co-operation between the public and private sector", it seems that non-governmental stakeholder groups (the private sector as well as civil society) are only invited to participate on an ad-hoc basis. They do not fully contribute to the design and implementation of the strategy, even though they are invited to do so through public comments. This could indicate that the multi-stakeholder community is not structured enough to sufficiently participate in digital security policy making. In addition, the NITSC only meets once every four months, and serves mostly as a channel to discuss issues within government, rather than as an agile and business-friendly or civil society-friendly forum. This may also explain in part why business leaders in Latvia do not necessarily consider digital security as their own priority, as it is presented in the governance framework mainly as a national security issue.

Finally, various policy documents describe the NITSC alternatively as a "consultative" body, a "co-ordination" platform, the authority monitoring the "implementation" of the Cyber Security Strategy and the body in charge of evaluating digital security policy implementation. The governance framework does not clearly separate the functions of design, consultation, implementation and evaluation of the digital security strategy, as the NITSC, under the leadership of the MoD, seems to perform all these

functions. This may lead to limited external oversight and a lack of valuable feedback, and hence hinder improvement of the strategy over time.

Legal framework

The main legal framework for digital security in Latvia is the Law on the Security of Information Technologies, adopted in 2010 and amended several times since. The law applies to national and local government authorities, operators of critical infrastructure of information technologies (CIITs), operators of essential services and digital service providers, as well as electronic communications providers. It designates key organisations and their responsibilities in the area of digital security (e.g. NITSC and CERT.LV).

The Law on State Information Systems, adopted in 2002 and amended in 2014, relates to the networks used and maintained by governmental authorities. Among other provisions, it determines the unified procedures by which national information systems are created, registered, maintained, used, reorganised or discarded, and governs their management of digital security.

Other relevant regulations of note include:

- Cabinet regulation No. 422: "Procedures to ensure minimal security requirements of information and communication technologies' systems" (2015, updated in 2017 and 2019), which has the goal of harmonised and higher security levels in ICT systems across state and municipal institutions
- Cabinet Regulation No. 764: "General Technical Requirements of State Information Systems" (2005, latest amendments in 2009)
- Cabinet Regulation No. 496: "Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures" (2010, amended since)
- Cabinet Regulation No. 100: "Procedures for the planning and implementation of security measures of the information technologies of critical infrastructure" (2011).

A thorough audit of existing laws and regulations in the field of digital security, and their implementation, has apparently not yet been undertaken by the Latvian authorities.

Recent initiatives

Information Society Development Guidelines (2014-2020)

The *Information Society Development Guidelines* (2014-2020) serve as the Latvian national digital strategy. Their main objective is "to provide an opportunity for everyone to use the possibilities offered by ICTs, to develop a knowledge-based economy and to improve the overall quality of life by contributing to the national competitiveness, and increasing an economic growth and job creation". However, the Guidelines focus mainly on enhancing access and use of ICTs as well as e-government services such as online identity and state ICTs.

Action Direction 5.7 of the Guidelines relates to "Trust and Security" and specifically (under section 5.7.1) to "ICT Security", with a specific focus on capacity building.

Overall, the Guidelines seem to be limited in terms of linkages with other policy documents significant for digital security policy (e.g. Cyber Security Strategy), indicating that digital security in Latvia considered primarily as a national security issue. This perception is not unique to Latvia. In many OECD countries, the different building blocks of digital strategies operate in silos, with little co-ordination across vertical fields.

Cyber Security Strategy

The main digital security policy initiative in Latvia is the *Cyber Security Strategy of Latvia (2019-2022)*, which replaces the *Cyber Security Strategy of Latvia (2014-2018)*.

The overarching goal of the former strategy was to achieve "a secure, open, free and reliable cyberspace that guarantees the safe, reliable and continuous supply of services essential for the state and society".

The strategy applied to the government, including national and municipal administrations, the private sector and individuals. It relied on four principles (development, co-operation, responsibility and openness) and five key areas of action:

- governance of national, state-owned and critical ICT infrastructure
- the promotion of rule of law in cyber space and the reduction of cybercrime
- crisis management
- education, awareness raising and research
- international co-operation.

The new strategy (2019-2022) seems to differ slightly reflecting lessons learned over the past few years. While its vision begins in the same way (the goal is to achieve "a secure, open, free and reliable cyberspace that guarantees the safe, reliable and continuous supply of services essential to the state and society"), it also takes into account the need to respect "individual's human rights in a physical and virtual environment". This is a positive evolution that acknowledges the competing goals often at stake when devising digital security policy (e.g. privacy and national security). The new strategy also recognises the development of cyber-physical systems, and the need to move beyond the virtual-physical dichotomy.

Regarding the key areas of action, the last four are essentially the same, with the exception of "crisis management", which is now described in terms of "strengthening the resilience of ICT and provision of critical ICT and services to the public". The first key area of action has evolved from "governance" to "promotion of cyber security, reduction of digital security risks". This seems to indicate that the process of structuring the governance framework for digital security in Latvia, which was the first goal of the initial strategy, is now at least partially complete, and that the challenge for the Latvian authorities is to use this existing framework to fully engage all stakeholders in the management of digital security risk. This is a positive step, and implies that the Latvian authorities have acknowledged the need to go beyond a whole-of-government approach towards a whole-of-society approach that includes, in particular, the actors and communities involved in economic and social prosperity. This shift also implies the integration of a risk management approach. In fact, the new strategy acknowledges that ICTs "are not completely safe and can be target to attacks. The threat of an attack on ICTs cannot be completely prevented, but the risk of an attack can be greatly mitigated so as not to disrupt the economic and social development of society, to avoid economic damage and to benefit from ICTs in both public administrations and the private sector".

However, these positive changes in the new Cyber Security Strategy still need to be implemented in practice. For the Latvian government, one of the challenges will be to involve all relevant stakeholders and address digital security risks in the whole economy, with lead institutions whose primary audiences are either IT teams (CERT.LV) or the military (MoD). To be successful, a cultural shift may be needed, as well as the deeper involvement and/or support of other institutions such as VARAM, the Ministry of Economy (MoE) or the Prime Minister, whose scope is more horizontal by nature.

Other initiatives

The Latvian government has organised other initiatives in the field of digital security such as "safer internet day", "e-skills week" and "cyber security month", which aim to raise awareness and share good practices. In addition, digital security crisis exercises are carried out with public institutions, under the leadership of CERT.LV and the MoD, in accordance with the strategy.

CERT.LV has led by example with the publication of their vulnerability disclosure policy. CERT.LV accepts vulnerability reports for their own resources as well as for any other organisation in Latvia. In the latter case, CERT.LV acts as a co-ordinator among the involved parties (e.g. security researchers and organisations).

CERT.LV also provides training and information on digital security risks to IT professionals and the public. For example, it publishes regular information on online viruses and threats through its IT security portal *be safe*. The portal runs a check of each visitor's IP address against a database of infected IP addresses and informs them of any vulnerability or infection according to CERT.LV data. CERT.LV

is also engaged in educating specific professional groups including IT security officers, employees, managers, students and pupils. In 2012, CERT.LV launched the initiative Responsible Internet Service Provider (ISP), a quality label awarded to ISPs that co-operate with the team. Such co-operation includes providing incident information to end users, co-operating with the Internet Centre of the Latvian Internet Association to remove illegal material from the Internet, and providing an Internet content filter that can be set up for free on demand. Currently, Latvia has 13 "responsible ISPs", which cover approximately 77% of the Latvian Internet access market.

CERT.LV also organises educational events such as "Cyber Chess" and other knowledge-sharing activities. These events engage representatives from the private sector in digital security exercises (e.g. Kristaps and Locked Shields) which require them to solve a range of tasks together with colleagues from the public sector.

The National Guard Cyber Defence Unit (CDU) brings together experts who are interested in developing regular co-operation on digital security issues, improving expertise and knowledge at national and international level, and participating and organising training for the prevention of digital security attacks, as well as providing support to public bodies, where appropriate. The main objective of the CDU is to assist the Information Technology Security Incidents Response Institutions to prevent and respond to digital security incidents, and mitigate their consequences.

The MoD co-operates with LIKTA (the Latvian Information and Communication Technologies Association), which has 160 members, to organise among others the annual award for "the best cybersecurity initiative".

The Federation of Security and Defence Industries of Latvia (FSDI Latvia) represents the Latvian security and defence industry. At the national level, the organisation actively collaborates with the Defence Ministry, the Interior Ministry, the Foreign Ministry, the Economics Ministry and Parliament. FSDI Latvia has established the Latvian Security and Defence Cluster, which consists of small and medium companies and research institutions, as part of an EU project.

International co-operation

Latvia has developed close trilateral co-operation with its neighbouring countries Estonia and Lithuania. Policy makers from the three countries meet regularly (at least twice a year) to expand existing co-ordination, exchange information on the latest digital security trends and, in some cases, to co-ordinate a common position on digital security issues in international discussions. On a practical level, CERT.LV co-operates with Lithuanian and Estonian CERT units, exchanging information on the latest security threats, viruses and other risks, and meeting regularly in different fora. In 2015, the Estonian, Latvian and Lithuanian ministries of defence officially signed a Memorandum of Understanding on Co-operation in Cyber-security. However, there seems to a lack of co-operation among the ministries of economic affairs of the Baltic countries regarding digital security matters, even though the Estonian Ministry of Economic Affairs is the overall co-ordinator for digital security policy in Estonia (Figure 5.6).

The general manager of CERT.LV was the chair of TF-CSIRT – the European CSIRT forum – from 2014 to 2019. In this role, she supported the growth and development of the European CSIRT community, fostered collaboration in the digital security area among academia, government and public sectors, and successfully represented the European CSIRT community in different international fora.

Latvia is participating in several international training events and exercises. Examples include the three Cyber Europe exercises of the European Union Cyber Security Agency (ENISA).

Latvia is also taking part in the work of NATO, the European Union, the OSCE and the UN. It has ratified the Convention on Cyber Crime of the Council of Europe and its Additional Protocol concerning the criminalisation of racist and xenophobic acts committed through computer systems. In addition, Latvia is an active supporter of deeper co-operation among Nordic-Baltic countries, Poland and the United States.

Conclusions and policy recommendations

Latvia needs to further build upon the 2015 OECD *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

The 2015 OECD Digital Security Risk Recommendation includes eight principles that encapsulate a "digital security risk management" approach (Box 5.1), based on the understanding that digital security is an economic and social priority as well as a technical or national security issue. This implies that:

- The overarching objective of digital security is to increase the likelihood of success of economic and social activities: digital security should be an enabler for prosperity, not an end in itself.
- Organisations cannot eliminate digital security risk altogether, but can assess and reduce risks to an acceptable level in the light of the economic and social objectives at stake.
- Digital security measures in public and private organisations can have negative effects on the economic and social activities they are expected to protect. In order to avoid this situation, leaders and decision makers in public and private organisations should integrate digital security risk management into their business decision-making processes, rather than delegating digital security risk management to technical experts. Leaders and decision makers in organisations should manage the economic opportunities and security risks stemming from the use of digital technologies in tandem.

Box 5.1. Principles of the OECD *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

General principles

1. **Awareness, skills and empowerment**. All stakeholders should understand digital security risk and how to manage it.
2. **Responsibility**. All stakeholders should take responsibility for the management of digital security risk.
3. **Human rights and fundamental values**. All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.
4. **Co-operation**. All stakeholders should co-operate, including across borders.

Operational principles

1. **Risk assessment and treatment cycle**. Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.
2. **Security measures**. Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.
3. **Innovation**. Leaders and decision makers should ensure that innovation is considered.
4. **Preparedness and continuity**. Leaders and decision makers should ensure that a preparedness and continuity plan is adopted.

Source: OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity*, *www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*.

Latvia has made significant steps towards the implementation of this Recommendation with the recognition of digital security as a public policy issue requiring a whole-of-government approach in the *Cyber Security Strategy of Latvia (2014-2018)* and in the *Information Society Development Guidelines*. In addition, the Cyber Security Strategy of Latvia (2019-2022) recognises the importance of a risk management approach, and acknowledges that trade-offs need to be made to implement an effective strategy for digital security, noting that while digital security measures aim to promote trust, they can

also undermine confidence. In fact, such measures may conflict with, or be perceived as conflicting with, human rights and fundamental values, in particular privacy and freedom of expression. Digital security and human rights can reinforce or undermine each other depending on how they are managed. In addition, although digital security measures aim to protect economic and social activities, they can also inhibit them by increasing costs, reducing performance and, most importantly, reducing the open and dynamic nature of the digital environment, which is essential to realising the full benefits of the digital transformation.

The above analysis of Latvia's governance structure and initiatives for digital security highlighted a strong adherence to the majority of the principles of the OECD Recommendation. However, implementation of the Co-operation, Responsibility and Innovation principles remains incomplete. If digital security is perceived mainly as a technical or a national security issue, then risk ownership and interactions between business leaders and decision makers from the private sector as well as civil society, and the institution in charge of digital security, will likely be limited. Institutions in charge of national security are also less likely to promote transparency and horizontal co-operation, and to manage programmes related to digital security innovation, SMEs and start-ups.

More importantly, the Latvian approach emphasises technology, law enforcement and national security, but pays less attention to the economic and social dimensions (Figure 5.3). Although the *Cyber Security Strategy of Latvia (2019-2022)* seems to better integrate human rights and fundamental values, as well as risk assessment and treatment, the economic and social perspective seems under developed. This may limit the ability of the government and organisations to appropriately assess risks, raise awareness and empower all stakeholders to assume their fair share of responsibility. The following areas, in particular, could be developed further: programmes to better incentivise economic actors to take appropriate security measures (e.g. certification, multi-stakeholder partnerships); sectoral and cross-sectoral initiatives to promote digital security, for instance through information sharing initiatives (ISACs); and programmes related to digital security innovation and connecting relevant stakeholders (e.g. entrepreneurs, researchers, businesses, governments, etc.).

The obstacles to enhancing digital security in Latvia identified in the *Information Society Development Guidelines* (VARAM, 2014) are approximately the same as those identified in 2016 in the mid-term review for implementation of the first *Cyber Security Strategy* (MoD, 2016). They include a lack of human and financial resources for institutions in charge of digital security; a lack of digital security skills in Latvia; and a lack of ownership of digital security risks by stakeholders, in particular senior leadership, such as decision makers and business leaders. As long as digital security is approached and perceived primarily as a technical and national security issue, and not as an enabler of economic and social prosperity, it will be difficult for Latvian authorities to generate awareness in a meaningful manner and to truly empower users and communities. In Estonia, for instance, the fundamental principles of their Cyber Strategy recognise digital security as "an enabler" of economic growth, and cite transparency and open communication as core values (MoEAC, 2019).

Latvia needs to build upon its strengths to step up its digital security policy framework

CERT.LV and the MoD have emerged as key actors in the digital security policy framework. However, other institutions in Latvia have not yet deployed a similar level of commitment in terms of human and financial resources dedicated to digital security. This could prevent these institutions from being fully involved in the design and implementation of Latvia's digital security strategy.

To bridge this gap, other institutions in Latvia should develop their own capabilities for and approaches to digital security. CERT.LV and the MoD could help build such capacity, for instance through common workshops, upskilling seminars and temporary staff sharing.

The roles of CERT.LV and the NITSC need to be enhanced

In recent years, CERT.LV has emerged as a trusted institution able to support the private sector, including Latvian SMEs, in the event of security incidents. While the NITSC has been described in the *Cyber Security Strategy* as the "central national authority for the exchange of information and co-operation between the public and private sector", it seems that CERT.LV is actually at the core

of multi-stakeholder co-operation in Latvia. Beyond its linkage with the private sector, CERT.LV has built strong connections with civil society and the technical community, as demonstrated by its interactions with the IT Security Expert Group and the Cyber Chess annual conference. The role of CERT.LV has also been instrumental in recent policy developments at the European Union level as well as within the broader CERT community, for instance regarding the responsible disclosure of vulnerabilities. However, the main audience of CERT.LV remains IT teams within public and private organisations. One of the challenges ahead for Latvia is to move ownership of digital security risk from these IT teams to the boardroom.

Latvia could leverage the success of CERT.LV to better educate and involve other ministries in the implementation of the digital security strategy, for instance through sharing staff and co-organising events and workshops.

As discussed above, the creation of the NITSC was an important step in building a whole-of-government approach for digital security; however, some shortcomings have been identified. The role of the NITSC remains unclear: it is alternately defined as an intragovernmental co-ordination body; a consultative group for the MoD, an authority in charge of designing, implementing, monitoring and evaluating the *Cyber Security Strategy*; and a gateway between the government and other stakeholders. While the current high-level format of the NITSC has enabled Latvia to step up digital security as a key public policy issue, it may also limit the ability of its members to fully leverage the issue for meaningful exchange and co-ordination. The risk is that the NITSC may become a monolithic structure where officials discuss initiatives without truly addressing key policy issues.

Different avenues could be explored to fully leverage the potential of the NITSC:

- Increase the frequency of meetings, for instance by a working-level meeting, as a complement to the high-level meeting, focused on addressing key policy issues and delivering results in a more agile manner.
- Better engage with other stakeholder groups, with the support of CERT.LV. Use a "forum" format to allow business leaders to discuss freely the challenges they face in terms of digital security on a regular, rather than an ad-hoc, basis.
- Meet once or twice a year under the leadership of the Prime Minister's office. This would indicate clearly that digital security is not solely a national security issue, but rather one that pertains to economic and social activities.

Latvia needs to better integrate an economic and social policy dimension into its governance framework for digital security

The digital security policy framework in Latvia combines a strong technical dimension (CERT.LV) with a strategic dimension (NITSC), but lacks a policy dimension that encompasses economic and social perspectives. The following avenues could be explored to address this gap:

- Increase whole-of-government engagement and co-ordination, with clear mandates and plans for "horizontal" ministries (e.g. the MoE and VARAM) to design and implement policies focused on the economic and social dimensions of digital security (sectoral partnerships, innovation, certification, etc.)
- Better integrate the *Cyber Security Strategy* with the *Information Society Development Guidelines*.
- Reinforce the *Cyber Security Strategy*'s action plan, with measurable goals oriented towards economic and social prosperity.
- Develop trilateral co-operation with Latvia's neighbouring countries Estonia Lithuania. At present, such co-operation on digital security policy exists only between CERT.LV and the MoD. A new work stream could be established linking Baltic ministries in charge of economic affairs, to discuss digital security from an economic and social perspective. (In fact, the Ministry of Economic Affairs is responsible for co-ordinating digital security policy in Estonia.) Policy makers from the three countries could meet regularly (at least twice a year) to expand co-ordination and exchange information on the linkages between digital security and economic and social prosperity.

Box 5.2. Policy recommendations

Latvia can build on existing solid foundations to address the challenges and opportunities of digital security. The Latvian Computer Emergency Response Team (CERT.LV) is recognised internationally for its technical expertise, and has led by example in regard to the adoption of co-ordinated vulnerability disclosure policies. The Latvian Ministry of Defence (MoD) is also strongly committed to promoting digital security as a strategic issue, as evidenced in the recently adopted *Cyber Security Strategy of Latvia (2019-2022)*. Most importantly, the *Cyber Security Strategy* rightly recognises digital security as economic and social risk management challenge, rather than just a technical issue. The creation in 2011 of the Latvian National Information Technology Security Council (NITSC) was a good first step towards building a whole-of-government approach to digital security.

However, public policies and the governance framework for digital security in Latvia do not yet sufficiently reflect this economic and social risk management approach. Furthermore, the design and implementation of digital security policy in Latvia are still focused on a national security framework. As a consequence, the economic and social dimensions of digital security are not sufficiently addressed in organisations and public policies (e.g. skills, innovation, SMEs). In addition, stakeholders are not consulted sufficiently in digital security policy making. To tackle these issues, Latvia should consider:

- supporting its digital security strategy at the highest level of government
- reinforcing its whole-of-government approach to digital security, by stepping up the involvement of "horizontal" ministries (e.g. in charge of economic and regional development) in digital security policy making and initiatives
- better integrating the digital security strategy with the national digital strategy (*Information Society Development Guidelines*)
- establishing upskilling and workforce-sharing programmes between public institutions, so that other ministries can benefit from the experience of CERT.LV and the MoD, as well as promoting digital security career paths
- encouraging the establishment of a multi-stakeholder community and increasing multi-stakeholder co-operation through trust-based and sustainable partnerships, (e.g. extending the role of the NITSC by organising "forum" format events to effectively engage the community)
- increasing international co-operation, in particular with other Baltic countries, in the area of digital security for economic and social prosperity, in addition to existing programmes in the areas of national security or IT security.

Developing trust through greater privacy

The General Data Protection Regulation (GDPR) provides the main legislative framework for personal data protection in Latvia as well as in another EU countries. The Personal Data Processing Law (PDPL) was adopted to regulate certain issues concerning the direct application of the GDPR in Latvia, such as determining the status of a supervisory authority and national requirements in specific situations of personal data processing.

Adoption of the PDPL took into consideration the GDPR, and thus covers the basic principles of the *OECD Privacy Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. All controllers, whether public or private, must comply with the requirements mentioned in the PDPL.

This section reviews the main features of the PDPL and its implementation. It takes into account potential challenges that have emerged in the context of the GDPR, and the main activities of the supervisory authority under the PDPL and the GDPR.

Legal framework on data protection

The PDPL along with the GDPR and the Law on the Processing of Personal Data in Criminal and Administrative Offenses constitute the current legal framework governing the processing of personal data for the public and private sector in Latvia. The PDPL is divided into 8 chapters and contains

37 sections and 5 transitional provisions. The PDPL entered in full force on 5 July 2018 and was accompanied shortly thereafter by Cabinet Regulation No. 478, entitled "Regulations regarding the Selection of the Candidates for the Office of the Director of the Data State Inspectorate and the Removal of the Director from the Office", which entered in force 18 October 2019.

A number of other laws govern privacy and the processing of personal information in different fields in Latvia. These include the following:

- The **Law on Operation of the Schengen Information System** determines which institutions have access to this system, and mandates the DSI to supervise personal data processing within this system.
- The **Electronic Documents Law** determines the legal status of electronic commerce and electronic signatures, as well as provisions for the storage of electronic documents and rules for the accreditation and supervision of certification service providers and trusted certification service providers.
- The **Electronic Communications Law** mandates the Data State Inspectorate (DSI) to supervise the protection of personal data in the electronic communications sector in accordance with rights specified under the PDPL.
- The **Human Genome Research Law** determines the supervisory functions of the DSI regarding genetic data, including the treatment of complaints regarding genetic data processing that data subjects can submit to the DSI.
- The **Law on the Security of Information Technologies** stipulates the activities that should be conducted in the event of an information security incident.
- The **Law on the Rights of Patients** determines patients' rights and protections, including personal data protection.
- The **Latvian Administrative Violations Code**, which is due to expire on 1 July 2020, determines the sanctions (and their extent) that can be imposed in cases of personal data protection breaches, as well as the procedures to impose such sanctions.
- The **Administrative Procedure Law** applies to administrative procedures in institutions whenever other laws do not provide specific rules.
- The **Criminal Law** determines criminal liability regarding personal data breaches. If the DSI concludes that a case could imply criminal liability, it may forward the case to the State Police.
- The **Law on Protection of Children's Rights** governs the prohibition on disseminating information about children, such as personally obtained information on child victims or witnesses, or children that have committed a violation of the law.

Separate regulations also prescribe technical and organisational measures for the protection of personal data.

CM Regulation 117/2004 regarding the Manner of Appraisal of Electronic Records, Procedures for the Storage thereof and Transfer to the State Archives for Storage prescribes the manner of appraisal of electronic records, the procedures for the storage thereof, and the time periods for the transfer of such records to state archives for storage. The regulation applies to state and local government institutions and legal persons, which pursuant to regulatory enactments shall transfer electronic records for state storage.

CM Regulation 473/2005 provides additional procedures for developing, preparing, storing and circulating electronic documents at state and municipal institutions, and the procedures by which the circulation of electronic documents is carried out between state and municipal institutions or between these institutions and natural persons and legal persons.

Institutional oversight

The Data State Inspectorate (DSI) was established on 2 January 2001 and operated in accordance with the former Personal Data Protection Law (expired 5 July 2018). The DSI now operates in accordance with the PDPL, the GDPR, the Law on the Processing of Personal Data in Criminal and Administrative Offenses and Cabinet Regulation No. 478 of 18 October 2019.

The DSI employs 25 people and had a reported budget of EUR 640 998 in 2019. Given the breadth of its responsibilities since the enactment of the PDPL and GDPR, staffing and resources need to be increased.

In particular, the DSI lacks sufficient resources to hire dedicated IT and technical staff to investigate privacy violations in the digital space.

The DSI also supervises the national component of the Schengen Information System, verifying that the rights of data subjects are not infringed in the processing of personal data, and represents the Republic of Latvia in the Schengen Information System Joint Supervisory Authority, the Europol Joint Supervisory Authority, the Europol Appeals Committee and the Joint Supervisory Authority of the Customs Information System, the European Data Protection Board and the Advisory Committee of the Council of Europe on the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108), as well as other actions of the European Union and international data protection authorities (DPAs).

The next sections examine the degree to which the DSI is effective at implementing the PDPL and the GDPR, and analyses available statistics related to monitoring and evaluation of the DSI's activities.

Aim and reach of the Data State Inspectorate (DSI)

Pursuant to the PDPL, the objective of the DSI is to protect fundamental human rights and freedoms in the area of data protection. The DSI conducts its activities and functioning on an independent basis taking into account the principles of equality before the law, presumption of innocence, veracity and lawfulness.

The specific activities and tasks of the DSI (in addition to those listed in Article 57 of the GDPR) are contained in Section 4 of the PDPL (Box 5.3).

Box 5.3. Main regulatory powers and activities of Latvia's DSI under the PDPL

1. Supervise the conformity of processing of personal data to the requirements of laws and regulations.
2. Promote efficiency of data protection.
3. Ensure data protection certification procedures.
4. Ensure qualification check of data protection officers and maintain a list of the data protection officers who have passed the qualification examination.
5. Provide recommendations to the the Cabinet (Saeima), local governments and other institutions according to its competence with regard to amending of laws and regulations, as well as participate in the development and opinion of draft laws and regulations prepared by other institutions.
6. Provide opinions on the conformity of data processing systems to be created in the State administration institutions to the requirements of laws and regulations.
7. Provide opinions to the national accreditation body on the conformity of the certification body pursuant to the Data Protection Regulation.
8. Co-operate with foreign supervisory authorities engaged in data protection, openness of and access to information, and unsolicited commercial communication.
9. Ensure that information requests from data subject are forwarded to the European Judicial Cooperation Unit (Eurojust) and European Police Office (Europol).
10. Represent the Republic of Latvia in international organisations and events in the area of data protection.
11. Conduct studies, analysis, provide recommendations and opinions, as well as inform the public of current issues in the areas of its competence.
12. Perform tasks set forth in other laws and regulations.
13. Publish information on its website regarding violations of the requirements of the Data Protection Regulation committed by legal persons, public and private institutions and officials, as well as other public institutions, and its elimination.

Other main obligations of the DSI under the PDPL and the GDPR include the elaboration of an annual report on its operation and functioning, which is submitted to the Saeima, the Cabinet, the Supreme Court, the European Commission and the European Data Protection Board (by 1 March), and made available on its website (Section 13).

Likewise, Section 5 of the PDPL (in addition to the rights contained in Article 58 of the GDPR), provides to the DSI a list of rights and powers to enforce the PDPL (Box 5.4).

Box 5.4. Rights of the DSI under the PDPL

1. To conduct inspection of data processing following the requirements contained in laws and regulations.
2. To draw up reports on administrative violations, examine administrative violation matters and impose administrative sanctions for violations.
3. To request and receive documents, copies and other materials necessary for the inspection, including information of limited accessibility free of charge from private persons, State administration institutions and government officials.
4. To visit State administration institutions and production facilities, warehouses, commercial and other non-residential premises owned, possessed or used by legal and natural persons in the territory of Latvia in order to verify conformity of the operation of the controller to the requirements contained in laws and regulations within the scope of its competence.
5. To become acquainted freely, according to its competence, with all types of information available in registers, information systems and databases and access it (irrespective of owner of the information) in order to obtain the information necessary for the inspection.
6. To request and receive, according to its competence, the information, documents and other materials regarding services provided to persons which are necessary for the inspection.
7. To request and receive an opinion of an independent and objective expert within the scope of the inspection.
8. To provide answers in the English language when examining complaints of non-residents in co-operation with other supervisory authorities.
9. To bring an action before courts for violations of this Law or the Data Regulation.

Pursuant to Section 6, subsection 2 of the PDPL, the Director of the DSI has the obligation to establish advisory councils, as well as working groups for the examination of issues in the areas of competence of the DSI. At the initiative of the Ministry of Justice (MoJ), the Data Protection Advisory Support Council (DPASC) was established in 2018. The aim of the DPASC is to promote the application of principles of common understanding and good governance in the implementation of the GDPR, to dispel myths and to prevent misinterpretations not only in public administration but in society as a whole.

Furthermore, the DPASC serves as a platform for discussion on matters pertaining to the GDPR and its application, sharing best practices and expertise, promoting data protection and discussing issues of mutual interest. The Council is managed by the Secretary of State of the MoJ, and comprises the DSI and representatives from the largest sectors (media, health, welfare, education, etc.).

The Latvian Association of Local and Regional Governments (LALRG) regularly organises discussions and publishes information on data protection. LALRG is a public organisation associating with local governments of the Republic of Latvia on a voluntary basis. In accordance with Article 96 of the Law on Self-Governments, the LALRG has the authority to represent local governments in negotiations with the Cabinet of Ministers, since the LALRG represents more than a half of all types of local governments. All the local governments of Latvia (9 cities and 110 municipalities) are members of the LALRG. Other institutions can also contact the MoJ and the DSI. At the beginning of 2019, data protection experts from ministries and their subordinate institutions gathered to discuss the most pressing issues in relation to implementation of the GDPR, including data protection, and to share best practices and expertise.

The PDPL contains five transitional provisions. Section 5 states that the Cabinet shall assess the effectiveness of the regulation regarding the qualification exam for data protection officers contained in the PDPL, and submit an assessment regarding the possibility of abolishing this examination to the Saeima by 30 June 2021.

Enforcement

The DSI is responsible for enforcement of the PDPL and the GDPR and other national laws governing privacy and data protection.

On 26 August 2019, the DSI imposed a financial penalty on an online retailer to the amount of EUR 7 000 for non-compliance with the GDPR, specifically for not respecting and protecting the rights to erasure of data subjects and for not co-operating with the supervisory authority. The sanctions were applied because the retailer failed to carry out its duty as a controller to execute the data subject's request and also did not provide the DSI with the requested information within the specified time period. The retailer also failed to comply with an order issued by the DSI in accordance with GDPR Article 58(2)(c) and (g) and Article 23 of the PDPL.[5]

Concerning decisions on fines, in 2019, the DSI received 1 236 complaints related to possible violations of personal data processing. In response, 246 inspections were made and fines were imposed in 9 cases. The range of fines imposed in administrative infringement cases ranged from EUR 300 to EUR 150 000. A warning was issued in seven cases.

The number of decisions taken in administrative violation cases corresponding to 2018 and 2017 is shown in Table 5.1.

Table 5.1. Decisions taken in administrative violation cases

	Decisions taken (number)	Decisions on termination of a case (number)	Penalty applied (number)	Including		Total amount of fines (EUR)
				Fine imposed (number)	Warning issues (number)	
2017	151	86	65	35	30	46 593
2018	97	71	26	12	14	10 230
2019	45	29	16	9	7	163 523

Source: DSI (2020), *Activity Report 2019, Data State Inspectorate Republic of Latvia*, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

Likewise, the DSI reports that out of 20 challenged decisions of the Inspectorate officials regarding administrative violation, 12 were appealed to the court. In total, 24 court proceedings were initiated in 2018. The DSI reports that the number of cases appealed to the court decreased in 2018, as 3 fewer challenged Inspectorate decisions were appealed than during 2017.

Technical measures for data protection

The PDPL does not contain any specific provisions or sections dealing with technical and organisational security measures of personal information. Article 32 of the GDPR establishes the obligation of controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Section 68(1) of the Electronic Communications Law of Latvia contains a provision on the security of processing of personal data for providers of electronic communications, which mandates that said providers: 1) ensure that personal data can be accessed only by authorised staff and used for previously specified purposes; 2) ensure that personal data are protected against accidental or unlawful destruction or accidental loss, and unauthorised or unlawful storage, processing, access or disclosure; and 3) document the internal procedures for the investigation and prevention of breach of personal data protection.

Personal data breach notification

Article 33 of the GDPR establishes that the controller shall notify security incidents or data breaches of personal information to the supervisory authority without undue delay and no later than 72 hours after become aware of the situation when the data breach represents a risk to the rights and freedoms of individuals. Article 34 of the GDPR establishes the obligation of data controllers to communicate data breaches of personal information to the data subject without undue delay when the data breach is likely to result in a high risk to the rights and freedoms of natural persons.

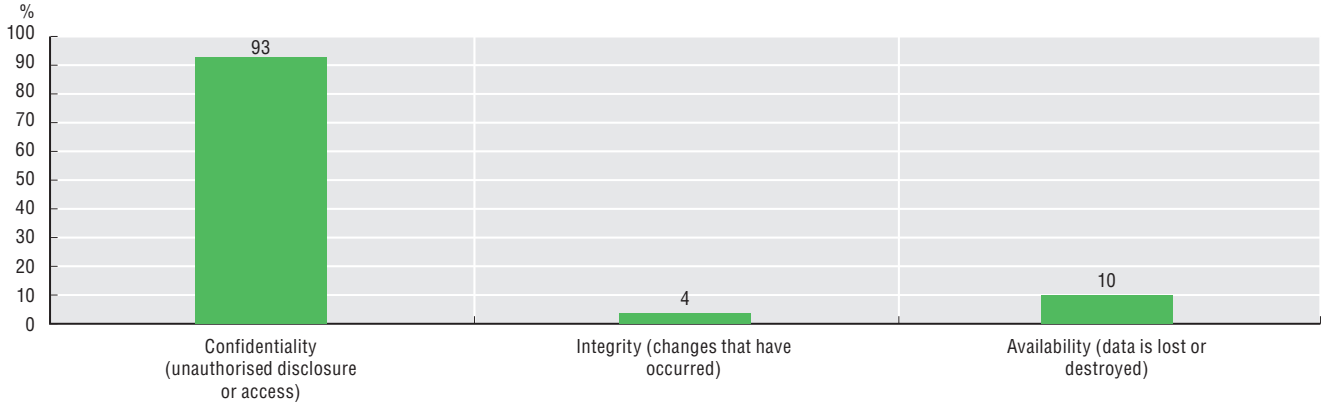
Activities that should be performed in the event of a data breach are established under the GDPR and the Law on the Processing of Personal Data in Criminal and Administrative Offenses. The GDPR and the *Guidelines on Personal data breach notification under Regulation 2016/679* regulate obligations on data breach notifications for data controllers and data processors.[6]

The Law on the Security of Information Technologies prescribes the activities that should be performed in the event of information security incidents.

The main purpose of the Law on the Security of Information Technologies is to improve the security of information technologies among the state, local government authorities and private institutions. The law establishes obligations to notify security incidents and actions to prevent security vulnerabilities. Section 6(2) stipulates that state or local government institutions or the possessor of CIITs shall within 90 days conduct all the actions necessary to eliminate the security vulnerability and inform the competent incident response institutions. Further, pursuant to section 7(4), the Security Incidents Response Institution may be allowed to perform processing of personal data that is not related to the prevention of such incidents, only if it prepares and sends the DSI a description of the planned processing and protection of personal data. The Security Incidents Response Institution shall prepare and submit to the DSI a report on the processing of personal data performed during the previous year by the end of January the following year.

The DSI's 2019 Annual Report reports that the DSI received 1 236 complaints and applications related to alleged breaches in the processing of personal data. The applications and complaints under Article 57 of the GDPR were submitted by both data subjects and other public authorities (most often law enforcement authorities), as well as organisations and associations. The DSI received 107 reports about personal data breaches, some of which contain several types of breaches (Figure 5.7).

Figure 5.7. Reported personal data breaches in Latvia



Source: DSI (2020), *Activity Report 2019*, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

Privacy management programmes

The accountability principle is one of the original eight basic principles of the 1980 Privacy Guidelines. The 2013 revision of the Privacy Guidelines included a new section, "Implementing accountability", which fleshes out the elements required of data controllers to implement the accountability principle, notably introducing the concept of "privacy management programmes" (PMPs). Under the revised

Guidelines, PMPs are the primary operational vehicle through which an organisation is expected to give practical effect to the basic principles contained in Part 2 of the Guidelines. Specifically, the added section states that a data controller should give ensure compliance with the Guidelines in respect of all personal data under its control by implementing a PMP tailored to the structure, scale, volume and sensitivity of its operations, and that provides appropriate safeguards based on privacy risk assessment including plans for responding to inquiries and incidents. In addition, the data controller should be prepared to demonstrate the operation of its PMP and provide notice, as appropriate, to authorities and data subjects where there has been a significant security breach affecting personal data. PMPs are still in an early phase of development in Europe and very few countries have adopted comprehensive guidelines and best practices for public sector institutions.[7]

On 18 December 2018, the DSI developed a *List of Processing Operations requiring data protection impact assessments* pursuant to Article 35(4) of the GDPR. The document contains a list of examples that data controllers should take into consideration when the processing of data may result in a high risk to the rights and freedoms of natural persons. The document lists 13 different possibilities when data controllers whose main place of establishment is the territory of Latvia are required to conduct a data impact assessment.

The DSI has also published several recommendations (e.g. on commercial communications and personal data processing in social networks). The DSI works closely with associations to develop specific guidelines for personal data processing in different fields.[8]

Policy making

NGOs can participate in policy making by commenting on draft legislation shared with the public for comments during the drafting process. NGOs are consulted before each new initiative and draft law proposal, mostly based on the invitation of the MoJ, who leads the drafting of legal acts in the area of privacy. Important NGOs include the Association of Data Protection Officials, the Latvian Information and Communications Technology Association and the Finance Latvia Association. For example, the CM regulation on the certification and supervision of credit information bureaus was elaborated in consultation with the Finance Latvia Association and the Association for Certified Personal Data Officers. Another example is the development of annual recommendations by the DSI in co-ordination with NGOs, including private actors, such as the recommendation on "Personal data processing within online social networking services", which was elaborated after the analysis of opinions of different social network service providers.

The DSI 2018 Annual Report states that the DSI has supported the development of guidelines for the protection of personal data applicable to associations of different sectors. For example, it mentions that the DSI worked on the development of guidelines on data protection with Finance Latvia Association and the Latvian Association for People Management, and also provided support to the Latvian Council of Sworn Advocates in the preparation of another set of guidelines for data protection.

Cross-border enforcement co-operation

Section IV of the *2013 OECD Revised Privacy Guidelines* highlights the importance of cross-border co-operation in the enforcement of privacy laws and the facilitation of mutual legal assistance among privacy enforcement authorities.

Articles 61 and 62 of the GDPR underline the obligation of supervisory authorities to provide mutual and effective co-operation concerning consultations, inspections and investigations regarding data protection, and establishes the criteria needed to conduct joint investigations and joint enforcement measures against controllers and data processors located in more than one member state of the European Union, respectively.

Until 2016, the DSI co-operated with foreign DPAs on a case-by-case basis and on a regular basis with other Baltic States. Following the adoption of the GDPR, the DSI co-operates with the DPAs of the EU countries on a regular basis in accordance with the GDPR.

The DSI 2018 Annual Report notes that on 15 June 2017, the DSI signed a Memorandum of Co-operation regarding the introduction of the Consult First principle, which promotes a customer-oriented focus in national regulatory activities. In applying the Consult First principle, the DSI has encouraged the controller to fulfil their duties laid down in the GDPR in 179 cases. The report provides that controllers have complied with the DSI's encouragement in 25 cases (78%).

Latvia is not yet part of the Global Privacy Enforcement Network (GPEN) or similar international networks for the enforcement of privacy and data protection laws.

Latvia ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) on 30 May 2001 and its Additional Protocol Regarding Supervisory Authorities and Transborder Data Flows on 21 November 2017, respectively. Latvia signed the Protocol amending Convention 108 (Convention 108+) on 10 October 2018 but has not proceeded with ratification.

The DSI 2018 Annual Report states that the DSI continues to participate in the work of the Advisory Committee of the Council of Europe's Convention 108 by participating in meetings, providing the required statistical information and commenting on prepared working documents.

Monitoring

The DSI produces an annual report and submits a summary of the report to the MoJ. This report details the DSI's main activities, provides information on financial resources and staff and a summary of court cases, as well as information on the main issues that occurred over the year. It also outlines the DSI's priorities for the coming year. In accordance with the relevant CM regulation, the annual reports and their summaries are available (in Latvian) on the website of the DSI.

Complaints received by the DSI are analysed quarterly and addressed according to the planned priorities of the DSI for the current year. In some cases, complaints are analysed on a. more ad-hoc basis, for example if the DSI receives several complaints on the same matter within a short period of time.

Education and awareness

The DSI 2018 Annual Report states that the DSI in co-operation with the MoJ has developed information materials for the population on the scope of application of the GDPR. Known as "Myths and Truth", these which explain to national citizens their rights, as well as the duties of controllers and data processors under the GDPR. The DSI organised 52 lectures and seminars on the protection of personal data and the application of the GDPR to representatives of the public and private sector, and attended 76 seminars, conferences, discussion meetings and working parties organised by other institutions and economic operators.

Data governance frameworks

Access to and sharing of data is crucial for innovation in the digital economy. For example, access to data can enhance public service delivery and facilitate the identification of emerging governmental and social challenges.

The management of the Open Data Policy is co-ordinated by the Government of Latvia.

The Latvian Open Data Portal was created by the European Regional Development Fund with the support of the Public Administration Information and Communication Technology Architecture Management System (PIKTAPS).[9]

Latvia is part of the Open Government Partnership (OGP) and, as mentioned on the Latvian Open Data Portal, *The Third Action Plan for Open Government Partnership of Latvia* encompasses action to promote openness, responsibility, public participation and the use of ICTs. This plan involves actions to improve and implement various online services. One of the 12 commitments is the development of an open source public data portal. However, in order to reach the targets of 2017-2019 OGP plan, Latvia has committed to involving society in the selection of datasets. Accordingly, the website therefore has a function allowing users to vote on data they want opened up.

Conclusions and policy recommendations

Latvia has made significant progress in the enforcement of privacy and data protection rights since the enactment of the GDPR and the PDPL. The DSI has started to enforce legal frameworks in a proactive fashion and to levy administrative fines against organisations for non-compliance with the general obligations set forth in the laws. However, the DSI should be provided with the human and financial resources necessary to effectively perform its tasks, which include advising and investigating privacy and data protection in the digital space.

The 2013 revision of the OECD Privacy Guidelines introduced the concept of PMPs which serve as the core operational mechanisms through which organisations implement privacy protection. Specifically, Paragraph 15(a)(i) specifies that a data controller's PMP should put into effect the OECD Privacy Guidelines "for all personal data under its control". The development of guidance by Advisory Committee of the Council of Europe's Convention 108 the DSI to more proactively enforce the provisions of the GDPR on privacy by design and privacy by default, as well as on PMPs, is pending and should take into account the guidelines developed by the EDPB as well as existing best practices in OECD countries.

Concerning accountability obligations, the DSI has developed a list of processing operations requiring privacy impact assessments. However, the DSI still needs to further develop guidelines for accountability obligations set forth under the GDPR, such as adherence to codes of conduct and promoting the use of existing certification schemes following the developments in this area across OECD countries. At the time of writing, the DSI also needed to put in place examinations for data protection officers.

Regarding international co-operation, the DSI has been quite active in the European context, particularly in terms of its participation in the Data Protection Board (EDPB) and the Advisory Committee of the Council of Europe's Convention 108. The DSI, however, has not yet joined the Global Privacy Enforcement Network (GPEN), which could facilitate and enhance its co-operation with other countries and regions.

A clear distinction between the use and processing of special categories of data and the protection of privacy rights remains a particular task that deserves special attention in the context of AI and the development of the IoT. The DSI should thus ensure that the rights of data subjects continue to be enforced under the GDPR and the national data protection legal framework. Further safeguards that help to improve the protection of data subject rights in the context of AI and the IoT remain tasks to be further developed. This could be achieved through further participation in and collaboration with international fora on data protection and privacy including the work of the OECD in these fields.

Box 5.5. Policy recommendations

Latvia should take further steps to enhance privacy by:

- providing the Data State Inspectorate (DSI) with the human and financial resources necessary to perform effectively its tasks, including advising and investigating privacy and data protection in the digital space
- encouraging the development by the DSI of guidance based on existing good practice to promote accountability as well as "privacy management programmes" (PMPs)
- encouraging co-operation between the DSI and other countries, including outside the European Union, for example by joining the Global Privacy Enforcement Network (GPEN)
- establishing appropriate governance of AI and the IoT, including through further participation and collaboration with international fora such as the OECD.

Consumer protection

Policy framework

Latvia's Consumer Rights Protection Law[10] and Unfair Commercial Practices Prohibition Law[11] contain general principles covering: 1) information disclosures; 2) product safety; and 3) unfair, misleading and aggressive commercial practices, which apply to both traditional and e-commerce transactions.

Consistent with the European Union's (EU) Consumer Rights Directive 2011/83/EU, the Consumer Rights Protection Law was amended in 2014 by a Regulation Regarding Distance Contracts,[12] which identifies key pre-contractual information disclosure requirements (regarding the business, product and transaction). The Regulation also covers the conditions for confirming distance contracts which, under Article 17, shall be provided to consumers via a durable medium and within a reasonable time after the conclusion of the contract (at the latest at the time of the delivery of the goods or before the performance of the service). The Regulation also introduces a new right of withdrawal for consumers engaging in distance contracts (including via e-commerce).

In addition to the above laws, specific e-commerce provisions are contained in the Law on Information Society Services,[13] the Electronic Communication Law[14] and the aforementioned Unfair Commercial Practices Prohibition Law.

- The **Law on Information Society Services** outlines key information that service providers must provide to consumers, including pre-contractual information about the business, the product and the transaction. It also covers codes of conduct, the conditions for storing information on a terminal equipment, requirements regarding commercial communications, liability, and the role and responsibilities of supervisory bodies, such as Latvia's Consumer Right Protection Centre and the DSI.[15] Article 4 of the law identifies general information to be provided by service providers. Article 5 lays down information to be provided by the service provider before placing the order. Article 7 specifies information about the contract terms and codes of conduct to be provided by the service provider.
- The **Electronic Communication Law** covers the rights and obligations of users, electronic communications providers, owners of private electronic communication networks and state administrative institutions, which are associated with the regulation of the electronic communication sector. It also contains provisions on electronic communications services and the use and administration of scarce resources, including spectrum allocation and assignment of radio frequencies. Furthermore, the law sets forth the rights and obligations of the respective regulatory agencies in the different sectors under regulation. It lays out specific obligations applying to entities and businesses with significant market power, obligations on universal services, data protection obligations for the electronic communications sector, and obligations to retain data in the provision of voice telephony, public telephony and the provision of public Internet access services.
- The **Unfair Commercial Practices Prohibition Law** also covers online advertising targeting children, misleading and unfair commercial practices, and product safety.

Additional requirements governing online transactions and, in particular, advertising to children are provided in the Advertising Law[16] (Section 5), which sets out penalties for non-compliance with the law and secondary regulation.

Payment services, electronic money and payment cards are regulated by the Law on Payment Services and Electronic Money,[17] which establishes the rights and obligations of payment service providers and users, and e-money issuers and holders, as well as the requirements for providing payment services for issuing, distributing and redeeming e-money, and the responsibility of both payment institutions and e-money institutions.

Furthermore, Latvia is currently in the process of implementing further policies on consumer protection, consistent with recently adopted EU regulations seeking to promote and improve the European digital single market, including the European Union's Regulation on geo-blocking.[18] Following the entry into force of the European Union's Regulation[19] on co-operation between national authorities responsible for the enforcement of consumer protection laws, amendments to Latvia's Electronic Communications Law were adopted in 2018, which provide the national Consumer Rights Protection Centre (CRPC) with additional powers to request information from electronic communications providers regarding information on the subscriber or user (e.g. webmaster).

Implementation of OECD principles on the protection of digital consumers

This section aims to evaluate the degree to which Latvia's consumer policy framework incorporates general principles for protecting digital consumers, consistent with the OECD *Recommendation of the Council on Consumer Protection in E-commerce*, otherwise known as "the E-commerce Recommendation" (OECD, 2016). The Recommendation's key provisions are contained in Box 5.6. The section also examines

the degree to which Latvia's framework covers the wide variety of forms that e-commerce now takes, including transactions between consumers, transactions via mobile devices and transactions that do not involve a monetary payment.

Box 5.6. General principles for protecting digital consumers

The OECD *Recommendation of the Council on Consumer Protection in E-commerce* sets the key provisions for the protection of digital consumers:

- fair business and advertising practices
- appropriate disclosures
- effective processes for transaction confirmation and payment
- product safety across e-commerce supply chains
- meaningful access to effective mechanisms to resolve disputes
- consumer education and awareness
- authorities' powers to investigate and take action at domestic level
- authorities' ability to engage in international policy and enforcement co-operation.

Source: OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, *www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*.

The E-commerce Recommendation was revised in 2016 to cover a number of new issues and developments, such as the rapid growth and consumer adoption of intangible digital content products, changing and more active consumer behaviour online including through mobile devices, the emergence of a wide range of online and mobile payments, and growing concerns over online product safety. The Recommendation also highlights the need to provide redress to consumers involved in non-monetary transactions, and calls on businesses to provide consumers with clear and conspicuous information on the limitations, functionality and interoperability of digital content products, and to address the privacy and security risks of e-commerce services including payment methods.

Institutional oversight

The E-commerce Recommendation contains updated provisions on the essential role of consumer protection enforcement authorities (CPEAs) and the need to enhance their ability to protect consumers in e-commerce. Part 2 of the Recommendation outlines implementation principles for the regulatory framework, and calls on governments, in co-operation with stakeholders, to achieve the purpose of the Recommendation by:

- reviewing and, if necessary, adopting and adapting laws protecting consumers in e-commerce, having in mind the principle of technology neutrality (53 ii)
- establishing and maintaining CPEAs that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively (53 iii)
- encouraging the continued development of effective co-regulatory and self-regulatory mechanisms that help to enhance trust in e-commerce, including through the promotion of effective dispute resolution mechanisms (53 v).

In Latvia, consumer policy making, implementation and enforcement related to e-commerce falls under the responsibility of the same authorities covering traditional shopping. Consumer policy making is led by the MoE,[20] specifically the Competition, Trade and Consumer Rights Division. Sector-specific policies addressing consumer issues (e.g. health services, transport or telecommunications) are covered by other ministries in co-ordination with the MoE. Given that consumer protection, including dispute resolution, is closely linked to civil and administrative law, the MoJ is also engaged in the development of consumer policy.

The main implementation and enforcement body is the CRPC,[21] under the MoE. While the MoE is responsible for reviewing the legal compliance of the decisions made by the CRPC, it may not interfere with the CRPC's decision-making process or revise an opinion upon which a decision was made. The MoE has the right to intervene and order the CRPC to take a decision, only in cases where the CRPC fails to act according to the law (unlawful failure to act). The Director of the CRPC is appointed for a term of five years by the Cabinet of Ministers on the recommendation of the MoE. In accordance with the Consumer Rights Protection Law, decisions of the CRPC may be appealed in court in accordance with the procedures specified in the Administrative Procedure Law.

The CRPC's main objective is to implement consumer rights and interests. Its responsibilities include handling individual consumer complaints, carrying out market surveillance of most non-food products, and enforcing consumer laws and regulations. Additional enforcement authorities complement the CRPC in specific areas, including the DSI, which is responsible for personal data protection, and some sector-specific ministries that have dedicated budget and staff for consumer protection.

The CRPC has broad regulatory powers (Box 5.7), including the possibility to require businesses to publish relevant information when consumer rights have been violated, for example in cases of false or misleading product information, unfair commercial practices or hazardous products.

Box 5.7. Main enforcement powers of the CRPC

- Request from businesses, the state, local government institutions and natural or legal persons all information necessary for the CRPC to fulfil its functions.
- Ask businesses to undertake voluntary actions within a prescribed period of time to ensure conformity of commercial practices with legal and regulatory requirements, such as to terminate unfair commercial practices.
- Require businesses to publish relevant information when consumer rights have been violated, for example in cases of false or misleading product information, unfair commercial practices or hazardous products.
- Visit any building, premise or places where goods that are not in compliance with consumer protection policy and law are manufactured, stored or traded, or where non-compliant services are being provided; visit any place in which measuring instruments are used, manufactured, repaired or sold.
- Request and receive samples of a good that is suspected to violate consumer rights in accordance with the procedures specified in regulatory enactments for carrying out laboratory or other expert examinations.
- Request the withdrawal of goods from circulation or terminate the provision of services, in cases of non-compliance with consumer protection policy, regulation or technical standards.
- Suspend, during an investigation, the sale of goods or the provision of services until a decision is taken based on a testing result from a laboratory or an expert opinion.
- Impose administrative sanctions and fines.

The CRPC currently has 107 staff members, most of whom are involved in consumer rights enforcement and product safety issues, including: goods and service surveillance, consumer rights protection, consumer consultations and complaints, and cross-border issues. Some consumer law enforcement is carried out by the DSI, in particular in the context of e-commerce. The supervision of e-commerce is performed by specific supervisory departments of the CRPC, with the assistance of support units. Table 5.2 provides budget and staff resource information for the period 2017-19.[22]

In addition to the CRPC, the following institutions can request and receive information, and apply administrative sanctions (fines, prohibitions): the State Health Inspectorate (advertising veterinary and pharmaceutical services) and the National Electronic Mass Media Council (advertising). The State Police may be involved in cases that involve criminal offences, for example related to spam.

Table 5.2. CRPC budget and staff, 2017-19

	Budget (EUR)	Staff (without ECC-Net)
2017	2 383 111	96
2018	2 895 983	107
2019	2 849 981	107

Source: OECD, based on data from CRPC.

The number of consumer complaints regarding distance contracts received by the CRPC has increased significantly in recent years. For example, around 486 complaints were submitted in 2017 compared to 222 in 2016, representing a more than 200% increase. The CRPC has investigated several cases and taken decisions to protect consumer interests, and has also published consumer guidance and alerts in the media to inform consumers about issues associated with specific online retailers and platforms.

Table 5.3 contains consumer complaints data submitted to the CRPC from 2017 to June 2019.

Table 5.3. Consumers complaints received and resolved by CRPC, 2017 – June 2019

	Complaints received	Complaints resolved
2017	3 616	958
2018	3 604	1 002
2019 (until 30 June)	1 940	405

Source: OECD, based on data from CRPC.

Enforcement

The CRPC regularly undertakes enforcement actions in the context of e-commerce. In addition to the regulatory powers described in Box 5.7, the CRPC can mandate the blocking of illegal content on websites that is harmful to children, including from service providers registered outside the European Union. In many cases, the CRPC's enforcement actions are related to unfair commercial practices in e-commerce.

Complaints related to criminal fraud are usually sent to the State Police for corresponding investigation and follow-up through criminal proceedings. Some of the complaints concerned online retailers failing to deliver products or reimburse customers. Table 5.4 provides complaint data received from 2017 to June 2019.

Table 5.4. Complaints related to e-commerce, 2017 – June 2019

	Businesses involved	Consumer complaints received	Resolution
2017	6 online retailers	196	Referred to the State Police
2018	3 online retailers	252	Referred to the State Police
2019 (until 30 June)	1 entertainment event	105	Referred to the State Police

Source: OECD, based on data from CRPC.

Unfair commercial practices are considered a breach of collective consumer interests and are enforced through collective actions on the part of consumers (via administrative proceedings). Individual consumer complaints may not be resolved through such collective actions, but the CRPC is competent to intervene and terminate those commercial activities in violation of consumer law. It may do so on a voluntary basis through voluntary infringement cessation or undertakings, or by issuing administrative decisions. Undertakings received from businesses and the CRPC's administrative decisions may be used as evidence by consumers who seek redress in court or engage in alternative dispute resolution. Not all consumer complaints may, however, trigger collective actions (e.g. one collective case may contain several consumer complaints, a consumer's complaint regarding infringement may not be upheld, a collective case may be underway prior to the consumer complaint, etc.).[23]

While there are no specific statistics available on unfair commercial practices in e-commerce, Table 5.5 provides complaint activity related to different types of commercial practices, some of which relate to e-commerce.

Table 5.5. Official consumer complaints related to unfair online commercial practices, 2017 – June 2019

	Complaints
2017	204
2018	279
2019 (until 30 June)	197

Source: OECD, based on data from CRPC.

Likewise, while there are no specific official statistics available on unlawful practices in e-commerce. Table 5.6 shows contains internal case handling information ("Uzraugs") stored on the internal database system of the CRPC.

Table 5.6. Unlawful e-commerce practices, 2017 – June 2019

	Administrative cases commenced	CRPC calls for voluntary cessation	Written undertakings received	Administrative decisions issued	Penalties applied (EUR)
2017	99	50	8	12	85 000
2018	177	149	1	18	194 900
2019 (until 30 June)	71	39	2	6	52 570

Note: CRPC = Consumer Rights Protection Centre.

Source: OECD, based on data from CRPC.

Monitoring and evaluation

The implementation of consumer protection in the context of e-commerce is assessed in a report submitted annually by the CRPC to the MoE.[24] The CRPC's 2018 Annual Report[25] included several interesting insights, statistics and information about enforcement actions conducted in the area of e-commerce. For instance, concerning fair pricing practices and distance contract terms from online retailers, the report indicates that "25 of the most popular internet shops were inspected and 25 administrative cases proceeded", followed by voluntary cessation of infringement.

Another useful monitoring tool is the Internet Sweep,[26] which is organised by the European Commission and the International Consumer Protection and Enforcement Network (ICPEN) as a means to enforce EU consumer protection law. Sweeps have been conducted in different areas including digital products, online airline ticket sales and online games targeting children. The results provide useful information on possible infringements of consumer protection legislation and help Latvia evaluate the seriousness of the issue, and the effectiveness of consumer policy implementation in the country.

Education and awareness

The CRPC regularly informs consumers about ways to shop safely online, both in response to questions from journalists and through social media channels. The CRPC maintains a website[27] to inform consumers about possible risks associated with misleading and fraudulent commercial practices conducted by specific online shops and platforms.

Furthermore, the CRPC has developed a checklist[28] with tips and useful information for consumers when deciding whether to buy from an online shop.

The CRPC has also distributed information (videos, gifs, infographics) provided by the Network of European Consumer Centres (ECC-Net) on subscription traps and online shopping. In 2018, the CPRC collaborated with the Patent Office on a campaign about counterfeit goods.

During 2019, the CRPC participated in an open day for government institutions.[29] High-school students visited the CRPC and participated in a variety of activities, obtained information about safe shopping online and how to recognise unsafe goods, and learned about consumer rights not only in Latvia, but also in the European Union.

The CRPC has been highly active in promoting consumer rights on social networks. In 2019, on Valentine's Day, it launched a campaign on how to choose an Internet dating website.[30] The CPRC also regularly publishes information on consumer protection rights on the Internet on its website.

In addition to educating consumers, the CRPC has engaged in the promotion of consumer rights to businesses involved in e-commerce activities. In particular, the CRPC has issued non-binding guidelines to help businesses interpret legislative acts, in particular focusing on electronic communication services markets, contractual terms and conditions in e-commerce, group buying, and notice and action procedures to obtain voluntary infringement cessation on websites.

In September 2015, the CRPC published a set of *Guidelines for Online Games Targeting Children*.[31] The authority collaborated with the European Commission and Denmark on in-app purchases, focusing on children gaming mobile applications, the results of which fed into the Guidelines.

National NGOs also play an active role in promoting consumer protection in the context of e-commerce. For example, the Latvian Internet Association[32] runs awareness-raising initiatives on Internet safety, including in the context of e-commerce. LIKTA,[33] in collaboration with the MoE, has conducted several activities such as seminars on e-commerce and e-services, organised an E-commerce Information Day and created an E-commerce Award for the best e-commerce vendor. NGOs also play an important role in implementing unfair commercial practice legislation in the context of e-commerce, by regularly informing the CRPC about possible infringements.

Furthermore, LIKTA promotes e-skills as well as awareness about the topic of online safety. Over 180 000 individuals across Latvia have participated in its training initiative Latvia@World (Latvija@Pasaule) since 2005, which offers training and certification, and has developed different training projects for e-skills and inclusion training.

Dispute resolution and redress

The objective of Latvia's policy on dispute resolution and redress (DRR) is to enable consumers to exercise their rights when entering into contracts with manufacturers, traders or service providers, and to provide consumers with access to fair and effective DRR, whether acting individually or collectively in Latvia, as well in cross-border-related disputes.

Disputes that cannot be resolved between a business and the consumer are dealt with by civil courts or through alternative dispute resolution (ADR) entities. The main ADR institutions are the CRPC and the Public Utilities Commissions (PUC), as well as private ADR organisations.

The CRPC includes a national ADR contact point and maintains a list of ADR institutions, as well as a Consumer Complaints Committee (CCC).

The CCC was established through recent amendments to the Consumer Rights Protection Law in accordance with EU Directive 2013/11/ES on alternative dispute resolution for consumer disputes. The CCC will operate under the authority of the CRPC and settle disputes between consumers and traders (businesses). The CCC will be composed of three or more committee members, representing on equal terms experts from consumer and trader NGOs with one impartial chair member.

Latvia's Law on Consumer Alternative Dispute Resolution[34] has been in force since July 2015. The law sets out rules for alternative dispute resolution entities, ensuring that consumers can issue and protect their legal rights by submitting complaints against businesses, while offering independent, impartial, transparent, effective, fast and fair alternative dispute resolution procedures. The law applies to ADR entities and procedures for out-of-court resolution of domestic and cross-border disputes concerning contractual obligations. Furthermore, the law provides specific rules and responsibilities (duties) for ADR entities and applied procedures, including a framework for co-operation among ADR

entities and between ADR entities and other institutions. The law does not apply to: 1) procedures before dispute resolution entities when the natural persons in charge of dispute resolution are employed or remunerated exclusively by the individual trader; 2) procedures before consumer complaint-handling systems operated by the trader; 3) direct negotiations between the consumer and the trader; 4) procedures initiated by a trader against a consumer; disputes between traders; disputes relating to non-economic services of general interest; 5) disputes regarding health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices; and 6) disputes concerning public providers of further or higher education; and disputes relating to an act or negligence on the part of sworn notaries or bailiffs.

Cabinet Regulation 631/2008[35] regulates procedures for the submission and examination of consumer claims regarding the non-conformity of goods or services with contract provisions.

European Parliament and Council Regulation (EC) 861/2007[36] established a European small claims procedure, intended to reduce costs and simplify and speed up litigation concerning small claims in cross-border cases. In Latvia, claims for small amounts can be submitted in accordance with the Latvian Code of Civil Procedure,[37] which provides simplified proceedings for claims below EUR 2 100.

Implementation and enforcement

The MoE[38] plays an essential role in implementing Latvia's DRR policy, co-operating closely with other ministries and authorities, such as the State Health Inspectorate, the State Food and Veterinary Service, and the PUC, as well as with NGOs.

According to the rules on dispute resolution procedures provided in the Consumer Rights Protection Law (section 26), consumers should lodge a complaint first with the business in order to seek a direct settlement. The CRPC and other institutions provide advice to consumers about their rights in specific situations and appropriate actions to request redress. Consultations may be conducted by phone, e-mail and face-to-face at the CRPC premises. Approximately 40-45% of initial complaints can be resolved through such conciliation procedures. If direct negotiations do not produce a solution, consumers have several other options.

If a consumer files a compliant with the CRPC and no solution can be reached with the business, a dispute settlement procedure may be initiated following Cabinet of Ministers Regulation 613, through which the CRPC engages directly with the business to obtain a solution. This may include an administrative procedure and a binding decision. Such administrative procedures undertaken by state institutions do not impose any costs on consumers, and it is the duty of the responsible institution or the court – if the decision is appealed in court – to gather the necessary information and evidence resolve the dispute.

Several industries in Latvia are providing their own dispute resolution mechanisms. The CCC, which operates under the authority of the CRPC and includes private sector representation, has established an alternative dispute resolution body.

Consumer complaints are collected systematically and addressed by product category and consumer protection issue. In addition, the CRPC and other government agencies and NGOs carry out surveillance activities to analyse market trends on a regular basis. The CRPC undertakes a variety of awareness campaigns, including in co-operation with national businesses and NGOs, to help consumers deal with DRR.

The Consumer Rights Protection Law (sections 22 and 23) gives non-governmental consumer organisations the right to defend consumer interests and to participate in the decision-making process. Furthermore, in accordance with Cabinet Regulation No. 300 Rules of Procedure of the Cabinet of Ministers,[39] non-governmental stakeholders must be involved in the drafting of legislation and policy planning documents. Consumer NGOs also have the right to examine consumer complaints, assist consumers in judicial cases and represent consumer interests in national courts. The work of the NGOs is perceived as an important source of information on developments in consumer markets, including potential or actual violation of consumer rights. Table 5.7 presents statistics on consumer disputes, both domestic and cross-border.

Table 5.7. Domestic and cross-border consumer disputes

	Domestic cases			Cross-border cases ECC-Net		
	Disputes	Redress[1]	Solved[2]	Disputes	Redress[1]	Solved[2]
2017	1 929	..	595	634	..	285
2018	1 976	..	707	489	..	203
2019 (until 30 June)	1 132	..	203	235	..	172

1. Information on redress is not available for the CRPC.
2. An agreement between the parties has been reached (but not necessarily redress).

Source: CRPC.

The above information indicates that Latvia's system of data collection and analysis has improved in recent years, with the CRPC now able to distinguish between domestic fraud and cross-border cases.

Enforcement of laws against spam

The objective of Latvia's policy on spam is to promote fair commercial practices and to ensure compliance with rules for the processing of personal data in the context of commercial communications. Commercial communications include automatic calls, emails and faxes sent to individuals without their explicit consent. Rules for the processing of personal data cover the contact details that may be collected by a service provider, including in particular when such processing is conducted for purposes other than the commercial transaction for which the data were collected.

Legal framework

The general requirements regarding information to be provided by manufacturers or service providers (businesses) to consumers are stipulated in the Consumer Rights Protection Law. The Unfair Commercial Practices Prohibition Law regulates commercial practices which are misleading, aggressive or ignorant in terms of professional diligence. The Personal Data Protection Law provides principles and regulation of personal data protection, in particular the sending of unsolicited commercial messages, or spam, which may be considered a violation. The main purpose of the Law on the Security of Information Technologies[40] is to improve the security of information technologies. The law specifies the most important requirements to guarantee the receipt of essential services supplied through such technologies. It also establishes the Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV),[41] an institution whose mandate includes the supervision and management of the security of information technologies of state and local government authorities, which may include countering spam.

More detailed rules for the protection of personal data and prohibitions on unsolicited commercial communications are established in the Law on Information Society Services. This law prohibits automated commercial communication if the recipient has not given his prior, free and explicit consent, and requires such communication to include the possibility of rejection by the recipient. These legal obligations also apply to automated calling systems that function without human intervention, including e-mail and fax. Additionally, the law establishes the conditions under which a service provider who has acquired electronic mail addresses from customers in the context of commercial transactions may use such addresses for other commercial communications. These include the following circumstances: 1) the commercial communications concern similar products or services from the service provider; 2) the client has not objected to receiving further emails; and 3) the customer has been given a clear, distinct, free-of-charge opportunity to reject further emails.

Enforcement powers

The two main institutions with responsibilities and powers related to spam are the DSI and the CRPC. Both authorities may request and receive information, enforce legal duties and impose administrative sanctions (fines and prohibitions). Furthermore, the State Police of Latvia[42] (Ministry of Interior) may become involved if the spam cases relate to criminal offences, and the CERT.LV may intervene if the cases affect the security of information systems and networks. Both businesses and NGOs related to

consumer protection contribute to the enforcement of spam legislation, including through informing the competent supervision authority about possible infringements.

If a supervisory body detects a violation of the law, it is entitled to: 1) request all information necessary to clarify the circumstances of the case; and 2) order the service provider to cease violating the law and specify a time period in which the business must comply with the law.

In order to avoid conflicts of interest, the CRPC's activities on dispute resolution are separated from its enforcement activities. Dispute resolution is handled by the Department of Consumer Consultation and Complaints and enforcement is conducted by the Department of Consumer Rights Enforcement.

Cross-border co-operation

Latvian spam enforcement authorities co-operate with foreign spam enforcement authorities, mainly within Europe. Specifically, in accordance with the Law on Information Society Services, the CRPC co-operates with authorities from European Economic Area (EEA) states. Furthermore, the DSI participates in a co-operation network for the national authorities of EU countries pursuant to EC Regulation 2006/2004[43] on co-operation between national authorities responsible for the enforcement of consumer protection laws. This co-operation is of particular relevance for spam cases that involve infringement of the Personal Data Protection Law.

There is a lack of sufficient information or evidence on the degree to which the CRPC and the DSI are evaluating the effectiveness of Latvia's spam policy and have undertaken appropriate measures and improvements, such as improved co-operation with foreign enforcement authorities outside of the EEA.

The CRPC has no specific information or statistics concerning spam or related issues and enforcement activities. Data on spam are collected by CERT.LV. Co-operation across agencies to share related information and analyse such data might help to address consumer issues in this area.

Bilateral assistance and cross-border co-operation

Cross-border fraud is mainly addressed through the CRPC's participation in several European and international networks that enhance information exchange and enforcement co-operation. The CRPC is part of the European Co-operation Network of Enforcement Agencies, which was established by the Consumer Rights Protection Law, and is used to address collective consumer cases. Latvia is also part of the ECC network (ECC-Net),[44] a Europe-wide network that helps to resolve individual cross-border disputes within the European Union. Four individuals appointed by the CRPC are currently working for the ECC network. Best practices and enforcement mechanisms are also circulated via the European Commission and the working parties of the EU Council.

Furthermore, the CRPC is a member of ICPEN and participates in EU and ICPEN sweeps to prevent cross-border infringements in different areas, such as tourism or in-app purchases. The CRPC also participates in Fraud Prevention Month, which is co-ordinated by ICPEN.

Latvia has signed several bilateral agreements to combat cross-border fraud. In particular, the CRPC has signed co-operation agreements with the Lithuanian and Estonian consumer protection and market surveillance authorities. Joint meetings are held at least once per year to share work results, discuss joint cases and share best practices. In September 2011, the CRPC also signed a Joint Declaration of Intent with the Standardization Administration of Israel's Ministry of Industry, Trade and Labour (MoITAL) to co-operate on market surveillance and enforcement in the area of non-food consumer product safety.

Latvian consumers encountering fraud involving a business based in a foreign country can file a complaint with the CRPC. If an EU cross-border infringement case is detected in Latvia, the CRPC acts according to the CPC Regulation by sending information and/or enforcement requests to other EU enforcement agencies. If the infringement has been committed by a company acting outside the European Union, the CRPC can use the ICPEN co-operation mechanism. Consumers can also file complaints on an e-consumer website,[45] a global system for co-operation on cross-border cases in which CRPC participates.

Conclusion and policy recommendations

Box 5.8 contains proposed recommendations for Latvia to improve its evidence base for consumer policy decision making, and enhance consumer protection both within and outside the European Union.

Box 5.8. OECD recommendations for Latvia to enhance consumer protection

Latvia should consider:

- Developing consumer complaints data specific to e-commerce in order to better understand the nature and scale of consumer issues associated with e-commerce transactions (consistent with the OECD E-commerce Recommendation, paragraph 53).
- Enhancing consumer awareness of issues associated with e-commerce, and improving their digital competence through awareness programmes, bearing in mind the special needs of different groups based on, for instance, their age, income and literacy (consistent with the OECD E-commerce Recommendation, paragraphs 50-51).
- Assessing the effectiveness of the country's dispute resolution and redress system by exploring, for instance, consumer usage and satisfaction as well as unresolved dispute cases.
- Improving the evidence base on cross-border disputes outside the European Union and enhancing cross-border enforcement co-operation within and outside the European Union.

References

CERT.LV (2020), *CERT.LV reģistrētie incidenti no 01.01.2020. līdz 31.03.2020* (Incidents registered with CERT.LV from 01.01.2020. until 31.03.2020), *https://cert.lv/lv/2020/04/pieejama-statistika-par-2020-gada-1-ceturksni*.

CERT.LV (2018), *CERT.LV Public Performance Report*, Ministry of Defence, Riga, *https://cert.lv/uploads/cert-gada-parskats-2019.pdf*.

DSI (2020), *Activity Report 2019*, Data State Inspectorate Republic of Latvia, Riga, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

MoD (2020), *Publiskais pārskats par CERT.LV uzdevumu izpildi: 2020. gada 1. ceturksnis* [CERT.LV Quarterly Public Review], Ministry of Defence, Riga, *https://cert.lv/uploads/parskati/CERT-LV_Q1_2020_pub.pdf*.

MoD (2019), *Cyber Security Strategy 2019-2022*, Ministry of Defence, Riga, *https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf*.

MoD (2016), *Mid-term Review of the Implementation of the 2014-2018 Cyber Strategy*, Ministry of Defence, Riga.

MoD (2014), *Cyber Security Strategy of Latvia (2014-2018)*, Ministry of Defence, Riga, *www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20%281%29.pdf*.

MoEAC (Estonia) (2019), *Cyber Security Strategy*, Ministry of Economic Affairs and Communications, Tallinn, *www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, OECD, Paris, *www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity*, OECD, Paris, *www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*.

OECD (2012), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD, Paris, *www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf*.

OECD (2002), *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0312*.

OECD (1998), *Cryptography Policy: The Guidelines and the Issues: The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264162426-en*.

VARAM (2014), *Information Society Development Guidelines 2014-2020*, Ministry of Environmental Protection and Regional Development, Riga *www.varam.gov.lv/eng/darbibas_veidi/e_gov/?doc=13317*.

Notes

Israel

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1. WannaCry is a ransomware that caused significant damage to the affected organisations. Mirai infects computers with a botnet, which then performs Distributed Denial-of-Service (DDoS) attacks.
2. The first Computer Security Incident Response Team (CSIRT) in Latvia was created in 2006 and became CERT.LV in 2011.
3. Digital security policy in Latvia spans many areas, including cyber warfare (MoD), cyber crime (MoI), telecommunications (MoT), digital security of financial systems (MoF) and privacy aspects (MoJ).
4. Except for the Bank of Latvia, which has a permanent representative on the NITSC.

5. See the news section of the European Data Protection Board, available at: *https://edpb.europa.eu/news/national-news/2019/data-state-inspectorate-latvia-imposes-financial-penalty-7000-euros-against_en*. A press release from the DSI is available at: *www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-piemero-7000-eiro-lielu-naudas-sodu-internetveikalam-par-personas-datu-apstrades-parkapumiem*.
6. Further information on data breach notification and the notification format is available at the website of the DSI: *www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana*.
7. Some relevant examples are the *Best Practice Guide on Privacy Management Programs (PMP)* developed by the Hong Kong (China) Office of the Privacy Commissioner for Personal Data, which outlines the requirements of privacy management programmes applicable to private and public sectors, available at: *www.pcpd.org.hk/pmp/pmp.html*. Likewise, the Personal Data Protection Commissioner of Singapore has published a Guide to Developing a Data Protection Management Programme, which was revised on July 2019 and aims to assist public and private sector organisations in complying with the *Personal Data Protection Act of 2012*, available at: *http://bit.do/fp4*. Further, the *Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector* were drafted in accordance with the document *Getting Accountability Right with a Privacy Management Program*, published jointly by the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners for Alberta and British Columbia, available at: *www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf*. The Data Protection Agency of Mexico (INAI) developed in August 2018 a set of *Guidelines for Data Protection Management Programs* for entities of the public sector that contain guidance, measures and recommendations to comply with the obligations set forth in the *General Law on Protection of Personal Data for Public Sector Entities* and the *General Guidelines on Personal Data Protection for the Public Sector*. The document is available in Spanish at: *http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4*.
8. The Recommendations and Guidelines of the DSI are available at: *www.dvi.gov.lv/en/legal-acts/recommendations-and-guidelines*.
9. The purpose of data.gov.lv is to gather and circulate data collected by government institutions and organisations in one place for public use, on the basis that these data are valuable for the development of innovation. Available at: *https://data.gov.lv*.
10. See the Consumer Rights Protection Law of 18 March 1999 at: *https://likumi.lv/ta/en/id/23309-consumer-rights-protection-law*.
11. See the Unfair Commercial Practices Prohibition Law of 22 November 2007 at: *https://likumi.lv/ta/en/en/id/167759-unfair-commercial-practices-prohibition-law*.
12. See Regulation No. 255 Regarding Distance Contracts of 20 May 2014 at: *https://likumi.lv/ta/en/en/id/266462-regulations-regarding-distance-contracts*.
13. See the Law On Information Society Services of 4 November 2004 at: *https://likumi.lv/ta/en/en/id/96619-law-on-information-society-services*.
14. See the Electronic Communications Law of 28 October 2004 at: *https://likumi.lv/ta/en/id/96611-electronic-communications-law*.
15. Available at: *www.dvi.gov.lv/en*.
16. See the Advertising Law of 20 December 1999 at: *https://likumi.lv/ta/en/en/id/163-advertising-law*.
17. See the Law on Payment Services and Electronic Money at: *www.fktk.lv/texts_files/0_Law_Payment_Services_Electronic_Money.pdf*.
18. See Regulation (EU) 2018/302 of the European Parliament and of the Council on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0302*.
19. See the Regulation (EU) 2018/302 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No. 2006/2004 at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017R2394*.
20. More information is available at: *www.em.gov.lv/en*.
21. More information on the CRPC is available at: *www.ptac.gov.lv/en/content/about-crpc*.
22. Available at: *http://ptac.gov.lv/sites/default/files/01_tame_ptac_2018_01.pdf*.
23. Received written undertakings are published on the CRPC website at: *http://ptac.gov.lv/lv/table/rakstveida-apnemsanas*. Administrative decisions issued by CRPC are published on the CRPC website at: *http://ptac.gov.lv/lv/table/ptac-l-mumi*.
24. Available at: *www.em.gov.lv/en*.
25. Available at: *http://ptac.gov.lv/sites/default/files/gada-parskats-2018.pdf*.

26. Available at: *https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/sweeps_en*.
27. Available at: *www.ptac.gov.lv/lv/content/aizdomigo-interneta-vietnu-saraksts*.
28. Available at: *www.ptac.gov.lv/lv/content/k-izv-l-ties-dro-u-i-veikalu*.
29. More information is available at: *www.facebook.com/ptacgovlv/posts/1164183977095012*.
30. More information is available at: *www.facebook.com/ptacgovlv/photos/a.274069902773095/1111458369034240/?type=3&theater*.
31. Available at: *http://ptac.gov.lv/sites/default/files/docs/nr_19_vadlinijas_tiessaistes_speles_0.pdf*.
32. See more information at: *www.lia.lv*.
33. More information is available at: *https://likta.lv/en/home-en*.
34. See the Law On Out-Of-Court Consumer Dispute Resolution Bodies of 18 June 2015 at: *https://likumi.lv/ta/en/id/275063-law-on-out-of-court-consumer-dispute-resolution-bodies*.
35. Available at: *www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._631_-_Consumer_Claims.doc*.
36. Available at: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0861&qid=1408967394914&from=LV*.
37. Available at: *https://likumi.lv/ta/en/id/50500-civil-procedure-law*.
38. Available at: *www.em.gov.lv/en*.
39. Available at: *https://likumi.lv/ta/en/id/190612-rules-of-procedures-of-the-cabinet-of-ministers*.
40. See the Law On the Security of Information Technologies of 10 November 2010 at: *www.dvi.gov.lv/en/legal-acts/law-on-the-security-of-information-technologies*.
41. Available at: *https://cert.lv/en*.
42. Available at: *www.vp.gov.lv*.
43. Available at: *https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32004R2006*.
44. More information is available at: *www.ecclatvia.lv*.
45. Available at: *www.econsumer.gov*.