4.3. Analysis of risks related to the e-Residency programme

4.3.1. E-Residency

E-Residency provides foreign citizens secure access to the Estonian e-services. The holder of an e-resident's digital ID card can digitally sign documents and log in to all portals and information systems that recognize the Estonian ID card. The e-resident's digital ID is not a physical identity document or a travel document and does not have a photograph. E-Residency does not give citizenship, tax residence, a residence permit, and permission to enter Estonia or the European Union. The grounds for refusing to issue an e-resident's digital identity card have been the same as the grounds for refusing to issue a visa or a temporary residence permit and the grounds for the imposition of an entry ban. In addition, it must be taken into account that no person has a subjective right to receive e-Residency, because this is a benefit that the Estonian state can provide to reliable persons. However, the use of e-Residency by third-country nationals as a part of immigration schemes has been observed in the attempts to make migrants more reliable in the residence permit or visa procedure.

Estonia is the first and so far the only country in the world to provide e-Residency. Similar programs are being developed in Lithuania, Ukraine, and Portugal. Since December 2014, the e-resident's digital ID gives foreigners the opportunity to do things digitally and independently of the location. Thus, for example, a person from outside the European Union can create a base centre for doing business in the European Union – he or she can establish a company in Estonia and actively participate in its management while living in India or the United States, for example. E-residency is also excellent for entrepreneurs who have already invested in Estonia and founded a company, e.g. Finns who run their local businesses via internet.

In addition to founding a company, Estonian e-residents can remotely manage the company and digitally sign documents and contracts, file income tax returns electronically, gain access to the international payment service providers, and make e-banking transactions if they have a bank account opened in Estonia – e-Residency does not involve a bank account or the right to it, but in order to obtain a bank account, a separate procedure must be followed, during which the reliability of the origin of the person and his/her funds is assessed. At the same time, there are cases when an e-resident acquires a shelf company together with an existing bank account, thus gaining easier access to financial services as a member of the management board.

Summary:
E-Residency allows foreigners to use Estonia for undesirable business, which allows them to hide the real content and purpose of the company's activities and the beneficiaries thereof. This is especially problematic with regard to third countries with which Estonia does not have cooperation relations in the field of justice, security, or law enforcement, which means that Estonia cannot obtain reliable information on applicants from the specified countries or effectively prosecute their offenses later.

4.3.2. Risks related to the e-Residency programme and their prevention and combating

A large number of public and private services were available to potential e-residents even before the launch of the programme through private identification tools, such as bank links. As any private identification measure is less secure in terms of the certainty of the identification than a

state-issued identity document, the introduction of e-Residency has ensured that the link between the operation and the person who performed it is established with greater certainty.

However, it is possible that the risk assessments prepared by the competent authorities were not sufficiently recognized when setting up the e-Residency program. Ensuring the certainty of personal identification in the case of persons from countries with which Estonia does not have cooperation relations in the field of justice, security, and law enforcement is particularly problematic. It is also not possible to effectively check the background of the nationals of such countries or, where necessary, to prosecute the offenses committed by them at a later stage.

The possibility created by e-Residency to operate as an entrepreneur may significantly complicate the investigation of criminal offences, since, for example, when catching a person who has committed tax fraud or fraud and conducting proceedings, his or her permanent residence abroad can be a significant problem. As a result, the investigation of offenses, the taking of evidence, court proceedings, bankruptcy proceedings, etc. may be delayed or failed.

One of the main prerequisites for managing the risks related to the e-Residency programme is the fact that the state knows who Estonian e-residents are and to whom it has entrusted the Estonian digital identity. When issuing a digital identity card of the Republic of Estonia to a foreigner, the Police and Border Guard Board identifies the foreigner on the basis of the identity document of the country of his or her citizenship submitted by the foreigner. Upon identifying a person and carrying out background checks, it is important to take into account the fact that there may be significant shortages in the understanding of the person's actual background if the person comes from a country with which Estonia does not have cooperation in the field of justice, security, and law enforcement. In essence, the state has not identified the person to a greater extent than in the visa or residence permit procedure. The risk of identity misuse is increased upon the identification of e-Residency applicants by external service providers instead of the Estonian embassies, to whom the state delegates the task of identifying a person and capturing biometrics.

An e-resident's digital ID is a document issued by the state certifying the digital identity of a person, which does not involve any greater state guarantees for the use of the issued document than any other state identity document issued by the state. Estonia, as the issuer of the document, bases the identification of a person on an identity document issued by his or her country of citizenship and recognized by the Republic of Estonia, and on the basis thereof issues the person a document certifying the digital identity of an Estonian person. The state guarantee therefore consists in the digital ID being issued to an authorized and identified person, verifying as far as possible that the document is not forged and that the person presenting the document is the same person to whom the document was issued. In addition, the state has the option to immediately suspend the use of the e-resident's digital ID certificate if misuse is suspected – this option is important for preventing and combating misuse, but it requires sufficient resources. As the e-Residency programme is expanding, so is the need for resources, respectively. As a person's digital signature or authentication solutions are also used outside Estonia, the suspension of the certificate depends on the transmission of misuse case data to the Police and Border Guard Board. The detection of offenses committed abroad depends on the foreign country's ability to detect and report violations.

Misuse of a document may consist of:

1) committing offenses with a digital ID, including fraud, tax fraud, financial crime, money laundering, and organised crime or terrorist financing, or
2) giving a digital ID to another person for use.

By now, some of the risks have also materialised.

E-Residency itself does not pose a risk of misuse, but can make committing an offence easier and cheaper – thus more attractive.

The following activities are envisaged in order to mitigate the risks, to ensure the reliability of e-residents and monitor the legal use of the document:

- when issuing a digital ID to an e-resident, a background check of the reliability of persons is performed to the extent possible (the state does not have the resources or on-site information to perform a thorough background check, the country of residence of the applicant may not have the motivation or legal basis to perform a background check), involving the relevant authorities and making inquiries into the relevant Estonian and European Union databases to the extent permitted by the administrative procedure – if there is any doubt as to the reliability of the person, the applicant will not be issued a digital ID. As this is an administrative procedure, it is not possible to use the international cooperation measures used in criminal investigations. With regard to third countries without a judicial, security, and law enforcement cooperation relationship, the possibilities for international cooperation would not be possible even if this tool were allowed in the administrative procedure;
- to enable e-Residency only in the countries with which Estonia has cooperation relations in the field of justice, security, and law enforcement, and to expand e-Residency to the respective country only after the establishment of cooperation relations;
- service providers must, where necessary, monitor the use of digital IDs to find patterns of misuse and anomalies – for that purpose e-residents can be distinguished in information systems by the features contained in certificates, and in addition, in-depth information work is being carried out among service providers, targeting in particular the providers of critical services and the services of highest interest to the e-residents;
- the Information System Authority provides information and expert support to digital service providers in developing and conducting the monitoring of services;
- on the basis of a suspicion that a digital ID is being misused or is no longer in the possession of its holder or on the basis of a corresponding notice, the PBGB as the issuer of the document investigates the case and has the right to immediately suspend e-Residency, thereby the validity of certificates and thus the right to use all digital services;
- in the event of misuse, the state can terminate the use of a digital ID as an advantage by declaring the document invalid.

As the e-Residency programme is growing and changing, it is necessary to take into account the speedily-changing environment, to continuously assess the risks, to plan appropriate mitigation measures, and to increase the corresponding resources. Without sufficient resources, it will not be possible to prevent and combat the misuse of e-Residency or to mitigate the resulting risks. In cooperation among various parties, an e-Residency risk analysis (recognized as information for internal use) has been prepared separately, which reflects the risks related to e-Residency, mitigation measures, and those responsible. The mapping of the respective mitigation measures and the implementation of the measures takes place under the leadership

of the Ministry of the Interior and the e-Residency programme council periodically evaluates and approves the mitigation activities.

4.3.3. Statistics

As at 31 Dec 2020, the total number of e-residents is 76,070, of which 13% were women and 87% men. TOP 5 citizenships are Finland, Russia, Ukraine, Germany, and China.

Table 19. Decisions to issue e-resident's digital IDs in 2014-2020

	Status given to a total of	Top 5 countries
2014	114	1. Finland 2. Russia 3. USA 4. Latvia 5. Lithuania
2015	7127	1. Finland 2. Russia 3. USA 4. Italy 5. Ukraine
2016	7,495	1. Finland 2. Great Britain 3. Russia 4. USA 5. Ukraine
2017	13,436	1. Ukraine 2. Finland 3. Germany 4. Great Britain 5. Russia
2018	22,367	1. Japan 2. Russia 3. China 4. Ukraine 5. Germany
2019	16,630	1. Russia 2. Germany 3. Ukraine 3. India 4. China
2020	12,955	1. Russia 2. Germany 3. China

		4. Ukraine 5. Spain

Source: Police and Border Guard Board

Since 2016, digital IDs of 90 e-residents have been revoked.

According to Enterprise Estonia, 15,907 enterprises founded by e-residents have been registered as at 29 Feb 2021. Registration does not differentiate e-residents by citizenship.