The Republic of Cyprus reaffirms its unwavering commitment to the promotion, protection and effective enjoyment of human rights, both domestically and internationally, and acknowledges that the matter currently inquired by the PEGA Committee has raised questions regarding the actual status of certain rights and freedoms in the EU itself.

Cyprus' competent authorities vigilantly monitor and assess all export license applications for dual-use goods on a case-by-case basis, in full accordance with relevant sanctions regimes, including the European Union Global Human Rights Sanctions Regime, as well as the EU Regulation for the control of exports, brokering, technical assistance, transit and transfer of dual-use items [Regulation (EU) 2021/821], while guided by the strict criteria of the relevant Council Common Position (2008/944/CFSP) in regard to defining common rules governing the control of exports of military technology and equipment. Within the same framework, the Cyprus Government has issued Regulation 528/2021 in order to fully implement Regulation (EU) 2021/821.

For the purpose of ensuring a high level of scrutiny during all stages of the evaluation process of export license applications for dual-use goods, all competent authorities of the Republic utilize specific e-licensing export software developed in the EU. This software provides all competent authorities with a transparent information system which, among other things, creates the conditions for effective intragovernmental coordination.

Furthermore, the risk that dual-use goods might be diverted and possibly employed for other purposes than those officially stated, is always taken into careful consideration. The competent authorities of the Republic will continue to review existing procedures with the aim of achieving the best possible intragovernmental coordination, especially on cases implicating serious human rights violations.

As an example of best practices, the Ministry of Energy, Commerce and Industry (MECI), which is the competent authority for issuing export licenses, frequently convenes the relevant governmental consultative committee, consisting of representatives from various relevant authorities who provide their technical expertise and knowledge, where export applications are examined. Applications for export of dual-use goods to third countries have been rejected on several occasions.

As regards reports on the alleged connections between Cyprus and NSO Group Technologies ('the NSO Group'), according to the Department of

Registrar of Companies and Intellectual Property, the NSO Group does not appear to be a registered legal entity in Cyprus or to hold shares in any legal entity registered in Cyprus. It is noted, nevertheless, that we have identified six companies in Cyprus which have either been established or bought by Board members of the NSO Group. Three of these are accounting companies, while the other three engage in research and development of products unrelated to software; the only export activity identified concerns exports of hardware products by one of the research and development companies.

Regarding the Pegasus software in particular, it does not appear to have been developed in Cyprus or exported from Cyprus. Moreover, out of the 85 cases investigated by the Cybercrime Unit of the Cyprus Police since 2019 to this date concerning attacks against information systems, none were related to Pegasus or any other equivalent intrusion software.[1]

With regard to the national legal framework protecting fundamental rights relevant to the PEGA Committee's inquiry, the Constitution of the Republic of Cyprus protects the confidentiality of correspondence and communication of every person. More specifically, Article 17(2) of the Constitution provides that there shall be no interference with the exercise of this right, unless such interference is permitted in accordance with the law, in the following cases:

A. Of convicted or unconvicted prisoners.

B. Following a court order issued pursuant to the provisions of the law, upon an application by the Attorney-General of the Republic, and the interference shall constitute a measure which is necessary in a democratic society only in the interests of the security of the Republic or for the prevention, investigation or prosecution of the following serious criminal offences:

a. Premeditated murder or homicide,
b. trafficking in adult or minor human beings and offences relating to child pornography,
c. trade, supply, cultivation or production of narcotic drugs, psychotropic substances or dangerous drugs,
d. offences relating to coin or bank notes of the Republic, and
e. offences relating to corruption in respect of which, in case of conviction, a sentence of imprisonment of five years or more is provided.

[1] The cases investigated were all distributed denial of service (DDoS) and ransomware attacks against companies, institutions or individuals.

C. Following a court order issued in accordance with the provisions of the law, for the investigation or prosecution of a serious criminal offence in respect of which, in case of conviction, a sentence of imprisonment of five years or more is provided and the interference concerns access to relevant electronic communication data of movement and position and to relevant data which are necessary for the identification of the subscriber or/and the user.

Furthermore, Law 92(I)/1996 on the Protection of the Confidentiality of Private Communication (Monitoring of Communication and Access to Recorded Content of Private Communication), regulates the possibility of lifting the confidentiality of private communication, under the conditions expressly provided for in Article 17(2) of the Constitution, and penalizes the illegal interception and/or surveillance and/or access to any private communication.[2]

According to Article 4(1) of Law 92(I)/1996, '*[n]o person can import, manufacture, advertise, sell or otherwise distribute electronic, mechanical, electromagnetic, acoustic or other device or machine when that person knows or ought to know that the device or machine has been primarily designed, produced, adapted or manufactured, in order to allow or facilitate the interception or monitoring of private communication*'. Violation of the above-mentioned provision constitutes a criminal offense sanctioned by five (5) years imprisonment and/or a fine of fifty thousand euros (€50.000).

It is noted that according to the aforementioned Article, the Department of Electronic Communications (DEC) of the Deputy Ministry of Research, Innovation and Digital Policy is the competent authority to authorize '*the manufacture for export purposes and the manufacture, in order to be at the disposal of the Chief of Police and the Commander of Intelligence Services, of electronic, mechanical, electromagnetic, acoustic or other device or machine that has been primarily designed, produced, adapted or manufactured, for the purpose of allowing or facilitating the interception or monitoring of private communication*'.

Further, it is emphasized that Article 4(1) is under evaluation from all competent authorities in order to strengthen its effectiveness. Within this framework the DEC, in cooperation with all competent authorities, maintains a registry of companies related to dual-use goods referred to in Article 4(1) and has established an oversight mechanism through the collection of additional information from these companies through a questionnaire prepared for that purpose as well as on-site visits. In addition, we cooperate with other

---

[2] It is noted that Article 8 of the European Convention on Human Rights has been fully incorporated into Article 17 of the Constitution.

countries for sharing best practices and governance mechanisms for the continuous enhancement of our oversight mechanisms.

Also, the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems has been implemented in national law; Article 7 of Law 147(I)/2015 penalizes illegal (a) access to information systems, (b) system interference, (c) data interference, and (d) interception, as well as the production, sale, supply for use, import, distribution or making available in any way, without permission, tools used for committing such offences.

Moreover, attention is drawn to the safeguards and warrants that are provided within the national legal framework regarding the legal surveillance of private communication, i.e. Articles 6-8 and 17A of the Law 92(I)/1996, and Article 6 of the Cyprus Intelligence Service Law 75(I)/2016.

Article 6 of the Law 92(I)/1996 provides the conditions under which the Attorney-General, upon recommendation by either the Chief of Police and Deputy Chief of Police or the Chief of the Cyprus Intelligence Service ('the Service'), may request an ex parte court order for surveillance of private communications. The requirements that need to be met by all relevant authorities in order to make such court order possible, are codified by Articles 6A-8. More particularly, there are certain provisions in place regarding:

(a) the process by which persons are granted authorization to conduct surveillance of private communications on behalf of the Police and the Service, given that a relevant court order has been issued (Article 6A),
(b) the information that needs to be included in all applications submitted by the Attorney-General for the purpose of securing relevant court orders (Article 7), and
(c) the characteristics and limitations of such court orders (Article 8).

Concerning the Service, it should be pointed out that between 1970 - 2016 it was part of the Police; prior to the enactment of Law 75(I)/2016, there was no law particular to the Service's operations. Since the Service became independent from the Police, the legality of its special operational activities, which pertain to fundamental human rights, is evaluated by a three-member committee as stipulated by Article 6 of Law 75(I)/2016.

The Committee is appointed by the Council of Ministers, following a recommendation by the President of the Republic. The evaluation of the Service's special operational activities does not, in any case, constitute a priori, approval of the Service's activities or a mean to circumvent

constitutional procedures. Ensuring full adherence of the Service's activities to judicial orders issued for the interception of private communications falls within the mandate of the three-person Committee. The Committee can initiate an ex officio inquiry and investigation over the Service's facilities, technical equipment and archived material.

In order to strengthen the oversight framework of the Republic, Law 92(I)/1996 was amended by Law 13(I)/2020, and according to the newly introduced Article 17A(1), the Committee is responsible for evaluating the application of the provisions of Law 92(I)/1996. Within this context, Article 17A(2)(a) provides that an inquiry and investigation may also be initiated by the Committee towards the Police's facilities, technical equipment and archived material. Should it deem appropriate, the Committee can appeal the Attorney-General of the Republic, or the Commissioner for Personal Data Protection or the Commissioner of Electronic Communications and Postal Regulation for further action.
In addition, the Committee produces an annual report in which it describes its activities, formulates observations and recommendations, identifies omissions and proposes any appropriate legislative amendments for the purpose of safeguarding communication privacy [Article 17A(6) of Law 92(I)/1996]. The annual report it produces is submitted to the President of the Republic and shared with the Speaker of the House of Representatives, the Attorney-General, the Minister of Justice and Public Order, the Chief of Police and the Chief of the Service [Article 17A(7)]. Thus, the Committee constitutes a fundamental pillar of effective and transparent oversight of the Service's, as well as of the Police's, special operational activities.

Finally, it is noteworthy that the budget of the Service is covered by the State budget which is submitted to and reviewed by the Parliamentary Committee on Institutions, Merit and the Commissioner of Administration (Ombudsman); it is approved by the Plenary of the House of Representatives. No amount is made available to the Service without the a priori authorization of the House of Representatives, following a recommendation by the Parliamentary Committee on Institutions, Merit and the Commissioner of Administration, after the latter is duly notified [Article 31(1) & (2) of the Law 75(I)/2016].

The Government of the Republic of Cyprus reaffirms its readiness to cooperate with the European Parliament's relevant bodies to hold perpetrators of serious human rights violations and abuses to account, and welcomes the role of the PEGA Committee in ensuring the effective implementation of Union law.