

EXPLANATORY MEMORANDUM

General explanation

On 17 May 2019, the Council of the European Union (hereinafter: EU) adopted the cyber sanctions regime consisting of Decision (CFSP) 2019/797¹ and Regulation (EU) 2019/796.² This specific sanctions regime enables the EU to take measures worldwide against persons and organizations that are responsible for a cyber-attack or an attempted cyber-attack, or are involved in a cyber-attack in any other way (e.g. through financial or technical support). The measures that may be imposed on persons and organizations include the freezing of funds or other assets and travel restrictions.

Based on this legal framework, the EU may therefore impose sanctions on (a) persons or entities who are responsible for cyber-attacks or attempted cyber-attacks, (b) who provide financial, technical or material support for such attacks, or who are otherwise involved in such attacks, and (c) persons or entities associated with them may also be subject to sanctions. Cyber-attacks include any of the following activities: access to information systems, information system interference, data interference or data interception.

The persons and entities subject to the restrictive measures are listed in Annex I to Regulation (EU) 2019/796 and the Annex to Decision (CFSP) 2019/797, respectively, and such restrictive measures may be adopted to deter and counteract against cyber-attacks with a significant effect which constitute an external threat to the European Union or its Member States.

The persons and entities subject to the restrictive measures are mentioned for the first time in the Annex to Council Implementing Regulation (EU) 2020/1125 and Council Decision (CFSP) 2020/1127 of July 30, 2020 implementing Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member

¹ See Council Decision (CFSP) 2019/797 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJEU 2019, LI 129).

² See Council Regulation (EU) No. 2019/796 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJEU 2019, LI 129).

States.³ The Council of the European Union has decided that the persons and entities listed in aforementioned Annex to Implementing Regulation (EU) 2020/1125 and Decision (CFSP) 2020/1127, respectively, should be added to the list of persons and entities that are subject to the restrictive measures provided for in Regulation (EU) 2019/796 and Decision (CFSP) 2019/797.

The reasons for listing the persons and entities concerned appear in the relevant entries in those Annexes. The restrictive measures concern 6 persons and 3 entities responsible for or involved in several cyber-attacks. These include *inter alia* an attempted cyber-attack on the Organization for the Prohibition of Chemical Weapons (OPCW)⁴ in the Netherlands, and the attacks that became known as “WannaCry”, “NotPetya” and “Operation Cloud Hopper”.

Within the framework of the common foreign and security policy of the Kingdom and in order to protect the integrity and reputation of Aruba and its financial sector, the Government has decided, using Articles 2 and 2a of the Sanctions Ordinance 2006 (AB 2007 No. 24), to implement the cyber sanctions regime concerning restrictive measures against cyber-attacks threatening the European Union or its Member States aimed at the freezing of funds or other assets. This State Decree provides for the freezing of funds or other assets of natural persons, legal persons and entities involved in cyber-attacks.

The introduction of this amending decree does not entail any financial consequences for the Government. Finally, it should be noted that, since this State Decree is intended to implement a number of international decisions without delay, the Government has decided not to hear the Advisory Council. The possibility to do so is offered by the second paragraph of Article 2 of the Sanctions Ordinance 2006.

In the following explanatory notes on the individual Articles, the Articles of this State Decree will be discussed in more detail.

³ See Council Decision (CFSP) 2020/1127 of July 30, 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States and Council Implementing Regulation (EU) 2020/1125 of July 30, 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

⁴ The Organization for the Prohibition of Chemical Weapons (OPCW) is an autonomous international, multilateral organization that has its seat in The Hague and cooperates with the United Nations.

Explanatory notes on the individual Articles

Article 1

This Article contains a number of necessary definitions. It cannot be ruled out that more natural persons, legal persons, entities or bodies will be added to the various Annexes to aforementioned Regulation (EU) 2019/796 and Decision (CFSP) 2019/79. In order to avoid that an amendment is required each time, a dynamic reference is provided for, in particular, for the Annexes to Regulation (EU) 2019/796 and Decision (CFSP) 2019/797.

Article 2

Based on this Article, the funds and other assets of persons, enterprises or institutions listed in the various Annexes to the EU sanctions are frozen. The Government is of the opinion that this provides for a sufficient legal basis to implement the freezing measures, in any case.

Article 3

The first paragraph entrusts the Central Bank of Aruba (the Bank) with the timely and digital publication of the Annex via the website www.cbaruba.org. This will ensure that the intended freezing measures can be implemented efficiently and effectively. The EU sanctions can also be found in the Official Journal of the European Union and are easily accessible via the website <http://eur-lex.europa.eu>.

The fact that the Annex will be subject to constant adjustment must also be taken into account. In addition to financial service providers, the Designated Non-Financial Businesses and Professions (DNFBPs), including lawyers, accountants, tax consultants, brokers, civil-law notaries, car dealers and jewelers, should also be familiar with these adjustments at all times.

Article 4

This Article requires everyone not to provide services and to refrain from acts that result or can reasonably result in a natural person, legal person or other entity listed in the Annex to the EU Regulation and the EU Decision, respectively, disposing in any way of the funds or other assets frozen pursuant to Article 2. This applies not only to services within the meaning of Article 1 of this State Decree, but also to any act that has the effect of placing a fund or an asset under the control of a designated

person. For the record, it should be noted that the violation of this prohibition has been made punishable under Article 17 of the Sanctions Ordinance 2006.

Article 5

This Article requires service providers to take immediate action, insofar as they have funds or assets of a natural person, legal person or other entity listed in the Annexes to the EU sanctions in their custody, as a result of which those funds and assets cannot be transferred, converted, moved or made available to a natural person, legal person or other entity listed in the Annex to the EU sanctions in violation of the freezing order.

Article 6

Finally, Article 6 contains the provision on the entry into force. This amending decree enters into force as of the day following the date of issue of the Official Bulletin of Aruba, given that international sanctions are being implemented.

The Minister of General Affairs, Integrity,
Government Org., Innovation and Energy,
[was signed]

The Minister of Finance, Economic Affairs
and Culture,
[was signed]

The Minister of Justice, Security
and Integrity,
[was signed]