Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

COUNCIL REGULATION (EU) 2019/796

of 17 May 2019

concerning restrictive measures against cyber-attacks threatening the Union or its Member States

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 215 thereof,

Having regard to Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States[(1)],

Having regard to the joint proposal of the High Representative of the Union for Foreign Affairs and Security Policy and of the European Commission,

Whereas:

(1) On 18 October 2018 the European Council adopted conclusions which called for the work on the capacity to respond to and deter cyber-attacks through Union restrictive measures to be taken forward, further to the Council conclusions of 19 June 2017.

(2) On 17 May 2019 the Council adopted Decision (CFSP) 2019/797. Decision (CFSP) 2019/797 establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. Persons, entities and bodies subject to the restrictive measures are listed in the Annex to that Decision.

(3) This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial and the right to the protection of personal data. This Regulation should be applied in accordance with those rights.

(4) The power to establish and amend the list in Annex I to this Regulation should be exercised by the Council in order to ensure consistency with the process for establishing, amending and reviewing the Annex to Decision (CFSP) 2019/797.

(5) For the implementation of this Regulation, and in order to ensure maximum legal certainty within the Union, the names and other relevant data concerning natural and legal persons, entities and bodies whose funds and economic resources are to be frozen in accordance with this Regulation should be made public. Any processing of personal data should comply with Regulations (EU) 2016/679[(2)] and (EU) 2018/1725[(3)] of the European Parliament and of the Council.

Changes to legislation: *There are outstanding changes not yet made to Council Regulation (EU) 2019/796. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(6) Member States and the Commission should inform each other of the measures taken pursuant to this Regulation and of other relevant information at their disposal in connection with this Regulation.

(7) Member States should lay down rules on sanctions applicable to infringements of the provisions of this Regulation and make sure that they are implemented. Those sanctions should be effective, proportionate and dissuasive,

HAS ADOPTED THIS REGULATION:

Article 1

1 This Regulation applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.

2 Cyber-attacks constituting an external threat include those which:

a originate, or are carried out, from outside the Union;

b use infrastructure outside the Union;

c are carried out by any natural or legal person, entity or body established or operating outside the Union; or

d are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.

3 For this purpose, cyber-attacks are actions involving any of the following:

a access to information systems;

b information system interference;

c data interference; or

d data interception,

where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.

4 Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia:

a critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;

b services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;

c critical State functions, in particular in the areas of defence, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;

d the storage or processing of classified information; or

e government emergency response teams.

5 Cyber-attacks constituting a threat to the Union include those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international

***Changes to legislation:** There are outstanding changes not yet made to Council Regulation (EU) 2019/796. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

organisations, its common security and defence policy (CSDP) operations and missions and its special representatives.

6 Where deemed necessary to achieve common foreign and security policy (CFSP) objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Regulation may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.

7 For the purposes of this Regulation, the following definitions apply:

a ‘information systems’ means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes digital data, as well as digital data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

b ‘information system interference’ means hindering or interrupting the functioning of an information system by inputting digital data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;

c ‘data interference’ means deleting, damaging, deteriorating, altering or suppressing digital data on an information system, or rendering such data inaccessible; it also includes theft of data, funds, economic resources or intellectual property;

d ‘data interception’ means intercepting, by technical means, non-public transmissions of digital data to, from or within an information system, including electromagnetic emissions from an information system carrying such digital data.

8 For the purposes of this Regulation, the following additional definitions apply:

a ‘claim’ means any claim, whether asserted by legal proceedings or not, made before or after the date of entry into force of this Regulation, under or in connection with a contract or transaction, and includes in particular:

(i) a claim for performance of any obligation arising under or in connection with a contract or transaction;

(ii) a claim for extension or payment of a bond, financial guarantee or indemnity of whatever form;

(iii) a claim for compensation in respect of a contract or transaction;

(iv) a counterclaim;

(v) a claim for the recognition or enforcement, including by the procedure of *exequatur*, of a judgment, an arbitration award or an equivalent decision, wherever made or given;

b ‘contract or transaction’ means any transaction of whatever form and whatever the applicable law, whether comprising one or more contracts or similar obligations made between the same or different parties; for this purpose, ‘contract’ includes a bond, guarantee or indemnity, particularly a financial guarantee or financial indemnity, and credit, whether legally independent or not, as well as any related provision arising under, or in connection with, the transaction;

c ‘competent authorities’ refers to the competent authorities of the Member States as identified on the websites listed in Annex II;

d ‘economic resources’ means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services;

Changes to legislation: *There are outstanding changes not yet made to Council Regulation (EU) 2019/796. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

e ‘freezing of economic resources’ means preventing the use of economic resources to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them;

f ‘freezing of funds’ means preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character or destination or any other change that would enable the funds to be used, including portfolio management;

g ‘funds’ means financial assets and benefit of every kind, including, but not limited to:

(i) cash, cheques, claims on money, drafts, money orders and other payment instruments;

(ii) deposits with financial institutions or other entities, balances on accounts, debts and debt obligations;

(iii) publicly-and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts;

(iv) interest, dividends or other income on or value accruing from or generated by assets;

(v) credit, right of set-off, guarantees, performance bonds or other financial commitments;

(vi) letters of credit, bills of lading and bills of sale; and

(vii) documents showing evidence of an interest in funds or financial resources;

h ‘territory of the Union’ means the territories of the Member States to which the Treaty is applicable, under the conditions laid down in the Treaty, including their airspace.

Article 2

The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following:

(a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;

(b) the number of natural or legal persons, entities or bodies affected;

(c) the number of Member States concerned;

(d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;

(e) the economic benefit gained by the perpetrator, for himself or for others;

(f) the amount or nature of data stolen or the scale of data breaches; or

(g) the nature of commercially sensitive data accessed.

Article 3

1 All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen.

***Changes to legislation:** There are outstanding changes not yet made to Council Regulation (EU) 2019/796. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

2 No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies listed in Annex I.

3 Annex I shall include, as identified by the Council in accordance with Article 5(1) of Decision (CFSP) 2019/797:

a natural or legal persons, entities or bodies who are responsible for cyber-attacks or attempted cyber-attacks;

b natural persons or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;

c natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies covered by points (a) and (b) of this paragraph.

Article 4

1 By way of derogation from Article 3, the competent authorities of the Member States may authorise the release of certain frozen funds or economic resources, or the making available of certain funds or economic resources, under such conditions as they deem appropriate, after having determined that the funds or economic resources concerned are:

a **[**[X1]necessary to satisfy the basic needs of the natural or legal persons, entities or bodies listed in Annex I**]** and dependent family members of such natural persons, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums, and public utility charges;

b intended exclusively for the payment of reasonable professional fees or the reimbursement of incurred expenses associated with the provision of legal services;

c intended exclusively for the payment of fees or service charges for the routine holding or maintenance of frozen funds or economic resources;

d necessary for extraordinary expenses, provided that the relevant competent authority has notified the competent authorities of the other Member States and the Commission of the grounds on which it considers that a specific authorisation should be granted, at least two weeks prior to the authorisation; or

e to be paid into or from an account of a diplomatic or consular mission or an international organisation enjoying immunities in accordance with international law, insofar as such payments are intended to be used for official purposes of the diplomatic or consular mission or international organisation.

2 The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Editorial Information

X1 Substituted by Corrigendum to Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (Official Journal of the European Union L 129 I of 17 May 2019).

Article 5

1 By way of derogation from Article 3(1), the competent authorities of the Member States may authorise the release of certain frozen funds or economic resources provided that the following conditions are met: