Guidance Note – Implementation of Firewalls in cases of EU entities owned or controlled by a designated person or entity

This document does not constitute a legally binding act. Legal provisions of Union legislation take precedence over the contents of this document and should always be consulted. The authentic texts of the EU legal instruments are those published in the Official Journal of the European Union. This guidance was prepared by Commission services to provide guidance for the implementation of EU sanctions. Only the Court of Justice of the European Union is competent to authoritatively interpret Union law.

Executive summary

The implementation of asset freezing measures adopted in the context of Regulation 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine can be particularly complex in cases where an EU entity is owned or controlled by a designated person or entity, in particular because the asset freeze extends to all assets owned, held or controlled by this non-designated entity.

To mitigate possible negative effects of these measures on EU operators and the EU internal market, the Commission services consider that it is possible to implement 'safeguards' to prevent the designated person from exercising control rights connected to ownership or effective control over the non-designated EU entity. Such a framework (also known as a 'firewall') aims at removing the exercise of rights connected to ownership or effective control by the designated person so that the EU entity's business operations can continue, while keeping the funds and economic resources owned by the designated person frozen. This document provides guidance to support the implementation and recognition of firewalls by Member States, thereby enhancing their effectiveness and the uniform application of EU restrictive measures.

1. Introduction

1.1 Value of this Guidance Note

The Commission, in its role as a guardian of the EU Treaties, monitors the implementation of Union law by Member States, under the control of the Court of Justice of the European Union. The purpose of this document is to give practical guidance on compliance with EU sanctions while handling cases where an EU entity is owned or controlled[1] by a designated person[2]. It seeks to ensure that EU law is applied consistently across the territory of the Union by setting out criteria relevant for Member States' national competent authorities ('NCA') which are in charge of implementing sanctions.

1.2 Ownership and Control' in EU sanctions

EU restrictive measures ('sanctions') establish that the freezing of funds and economic resources covers the assets belonging to, owned, held or controlled by those specifically listed in the respective annexes to the EU legal acts. Such a provision typically reads: "*[a]ll funds and economic resources belonging to, owned, held or controlled by any natural or legal persons, entities or bodies, or natural or legal persons,*

1 See Article 6b(5d) of Regulation 269/2014 and Article 5n(9a) or Regulation 833/2014.

2 This guidance note refers to 'designated person' in reference to 'natural or legal persons, entities or bodies' for ease of understanding.

entities or bodies associated with them, as listed in Annex [X], shall be frozen"[3] (emphasis added). EU sanctions also provide that no funds or economic resources can be made available, directly or indirectly, to or for the benefit of a designated person[4].

Therefore, if a designated person is deemed to own an entity, its assets must be frozen. Restructuring of ownership (e.g. the sale of shares by a designated person) is also prohibited by virtue of the asset freeze. Such a sale can only be done if the relevant EU Regulation contains a derogation to this end and the NCA grants an authorisation. In such a case, the proceeds of the sale must be frozen. In case of situations of ownership by a designated person, divestment by the designated person, when provided for in the Regulation[5], should be the preferred option to release the asset from the asset freeze.

If a designated person has control over an entity, there is a rebuttable presumption that the control extends to all assets owned by the latter. Such assets must be frozen. Otherwise, designated persons could circumvent the asset freeze imposed on them by continuing to have access to funds or economic resources through the non-designated third parties that they control[6]. In a similar vein, the making available of funds or economic resources to a non-designated entity, which are controlled by a designated person, amounts to making them indirectly available to the latter.

In order to mitigate certain undesired effects, EU regulations provide for certain limited exceptions from the asset freeze and prohibition to make funds or economic resources available to owned or controlled entities. These exceptions (derogations) presuppose an authorisation by the competent NCA which can carry out the necessary verifications and ensure that sanctions are not breached or circumvented. In spite of these legal exceptions (derogations), in practice it has proved very complex for entities owned or controlled by designated persons to continue operating after the designation of the latter. Existing derogations typically do not cover all possible transactions that an entity may need to carry out. The scope of such derogations cannot be expanded without rendering the asset freeze on the designated person ineffective. In addition, the long-term freezing of a non-designated entity's assets can have drastic negative consequences for the entity, all the way to possible bankruptcy.

1.3 Objectives of a firewall

Entities owned or controlled by designated persons may have significant importance for the EU economy and world market, by operating in sensitive sectors with considerable market share and/or by employing a significant workforce in the EU. Furthermore, such entities may belong to the same group and be present (e.g. through subsidiaries) in several EU Member States or third countries imposing similar sanctions.

Therefore, the Commission supports the implementation of safeguards (firewalls) to prevent the designated person from executing certain rights connected to ownership or effective control over the entity. A firewall brings about a structural change in an entity's corporate governance to remove the designated person from the day-to-day operations and any business decisions of the entity and the resulting resources and profits. It ring-fences the entity's assets and forestalls the making available of any

[3] For instance, Article 2(1) of Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

[5] For instance, Article 2(2) of Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

[6] See Commission opinion of 19.6.2020 on Article 2 of Council Regulation (EU) No 269/2014.

economic resources to the designated person. By doing so, a firewall enables an entity to operate, under strict conditions, unimpeded by the ownership or control of a designated person or entity. This means that the EU-based company operating under a firewall can have access to funds and economic resources, including the provision of services. The firewall ensures that no such funds or economic resources are made directly or indirectly available to that person. Irrespective of the firewall, the funds and economic resources of the designated person remain frozen.

The following sections provide guidance on the possible layout of a firewall. They aim to specify the conditions under which this framework should be implemented and recognised, in order to ensure its effectiveness and a homogeneous implementation by the Member States.

*_*_*

2. Practical implementation of a firewall

2.1 Requirements for a firewall

a) Entities for which a firewall may be established

The implementation of a firewall should take into account the positioning and significance of the entity on a national market or the European market, both in terms of market positioning and employment volume.

As a minimum standard, firewalls should be introduced for entities operating in sectors considered as "essential", including, but not limited to, the sectors of food production, pharmaceuticals, fertilisers, chemicals, water management and sanitation, nuclear power.

The establishment of a firewall is the preferred option for EU-based entities, as it aims to protect the interests of entities present on the European market. The relevance of focusing firewalls on EU-based entities is further reinforced by the interventions that may be necessary on the management of the entity (see section 2.2).

b) The removal of the designated person

The firewall should be constructed as a mechanism that ensures that the designated person is not involved in day-to-day and business decisions of the entity and that no resources from the entity will be accrued directly or indirectly. The designated person should not have the possibility to assert influence over the conduct of the EU entity or have any responsibility in the entity. It should be ensured that the designated person does not engage in any executive activities like those of a director or member of the board of directors, nor assume any decision-making role or any role which entails any responsibility in the entity.

2.2 The implementation of a firewall

a) Firewalls by legislation

A Member State may set up a firewall by intervening directly on the governance of the 'decoupled' entity through legislation. The structure of a firewall by legislation will differ from country to country given the disparity of legal systems in the EU. Several areas of law, such as insolvency or competition law, may provide inspiration or be a basis for such a framework.

The legislation must grant the NCA the ability to appoint a third party such as a temporary administrator or supervisor. This third party must act independently and report directly to the NCA. The third party must be suitable, with good repute and sufficient experience to fulfil its duties.

The third party would take actions necessary to ensure the proper implementation of EU sanctions, and provide the NCA with regular accounts regarding the creation and operation of the firewall. The third party would furthermore ensure that transactions carried out by the entity are not directly or indirectly benefitting the designated person.

To ensure the independence of the temporary administrator or supervisor, the NCAs may refer to the criteria outlined in the Annex.

If a Member State lacks the legislative toolset to implement such a firewall, it may consider adopting or amending legislation.

b) Firewalls by operators

The establishment of a firewall by an operator refers to the case where an entity decides to implement safeguards to decouple itself from a designated person which owns or controls it. This initiative aims to remove the presumption of control over the assets of a non-listed legal person, entity or body incorporated or constituted under the law of a Member State which is owned or controlled by a natural or legal person, entity or body and to avoid the underlying risks, notably financial and credit institutions' refusal to carry out transactions in connection with this entity. However, to be effective, the resulting changes in governance practices, as decided directly by the operator, must comply with the strict conditions that a firewall requires, particularly in terms of independence. Ultimately, the firewall must remove the ownership and control of the designated person, as explained in section 2.2.

To ensure that the safeguards established by the entity effectively rule out any presumption of control by the designated person, operators are encouraged to rely on an external audit, acting in full independence. The external audit process should be based on particular information provided by the entity, including its articles of association, bylaws, shareholder structure, as well as a description of the changes that have taken place that would allow for the removal of control by the designated person (e.g. notably board minutes attesting to management changes in the entity).

The external auditor should also have direct access to the entity's executives (directors) other than the designated person in order to be able to testify that the entity's operations are not subject to the influence of the designated person.

Finally, it is expected that the chief executive (who is not a designated persons) of the entity will give written undertakings, engaging his/her responsibility on the established firewall. If deemed relevant, a firewall established by the operator could entail the intervention of a third party exercising a similar role as described for a firewall by legislation[7].

The audit must determine that the designated person is neither in a position to exercise influence or have any responsibility in the entity, nor can in any way benefit from the assets of the entity (e.g. dividends, loan arrangements etc.).

Criteria for firewalls by operators and the use of external audits in this context can be found in annex 2 of the guidance.

In order to remove any obstacles that might have prevented the establishment of firewalls, two derogations regarding the setting-up, certification or evaluation of a firewall have been added to the legal

[7] See section 2.2 (a) and the Annex.

acts. Article 6(b)5(d) of Council (EU) Regulation 269/2014 allows for the provision of and the payment for such services, on a strict necessity base, for the purpose of setting up a firewall (otherwise impossible due article 2 that provides an asset freeze and the prohibition to make economic resources available), while Article 5(n)(9a) of Council (EU) Regulation 833/2014 authorise to provide services that may be necessary for the setting up of a firewall (in particular, legal advisory services and auditing services), whereas they would be directly or indirectly for the benefit of a Russian entity (otherwise impossible due Article 5n that prohibits to provide certain services to Russian companies).

If a firewall is not effectively established, the presumption is not rebutted and the NCA must not grant an authorisation to release the entity's assets frozen. In addition, in the event of non-compliance with the firewall commitments, the entity and the relevant individuals must be held accountable according to Member State penalties applicable to infringements of the provisions of the relevant EU Regulation.

c) Exchange of information regarding cross-border situations

Designated persons can be involved in entities located in multiple Member States. For instance, a designated person can exercise control over several EU subsidiaries or an owned or controlled entity may own several EU subsidiaries. It may be the case that one such entity is located in a non-EU country implementing similar measures. Accordingly, the implementation of a firewall may be necessary in several jurisdictions.

Where a cross-border situation appears, Member States should immediately reach out to other relevant Member States to engage collectively on the situation. Such exchanges could facilitate a shared assessment of ownership or control over the respective subsidiaries and discuss the possible need for firewalls. The Commission can facilitate the exchange of information for specific cases. The implementation of firewalls in only certain Member States may disturb the activities of the other related entities or the group as a whole, for instance if one such entity is an essential provider of internal services. This is detrimental to the uniform application of EU sanctions and runs counter the objectives supported by these safeguards.

For the sake of clarity and to avoid adverse effects, the NCA where the 'owned or controlled' entity is incorporated should be the one in charge of creating and/or monitoring the implementation of the firewall. Once implemented, in all cases firewalls should be recognised – provided that they are established according to the criteria that are set in this guidance, in order to work effectively, as discussed in the following section (section 3).

3. Recognition of firewalls

As discussed above, the establishment of an adequate firewall should 'decouple' the owned or controlled entity from the designated person. In practice, once a firewall is in place, the entity's frozen assets can be released and economic resources can be provided to the 'decoupled' entity. The previously controlled entity may resume its business operations. Yet, a firewall will only be operational where other operators engage with the decoupled entity. Recognition guarantees that a firewall which is set up in one Member State can produce effects in other Member States, ensuring its effectivity.

Where a firewall by legislation and/or voluntary changes to corporate governance by an operator comply with the letter and spirit of this guidance document, the pre-requisite for recognition should be satisfied.

3.1 Implementation of recognition by Member States

a) Firewall by legislation

Firewalls by legislation could enjoy recognition in other Member States – for example under Regulation 2015/848 on cross-border insolvency proceedings.

Outside an existing legal framework such as Regulation 2015/848, the criteria set out in the Annex 1 guide the appointment and role of a third party appointed in the context of firewalls set up via legislation. In doing so, the criteria seek to bridge differences in national frameworks to facilitate mutual recognition of firewalls and support uniform implementation of EU sanctions.

Where the criteria for recognition of a firewall are met, other Member States are invited to recognise such a framework. Member States are encouraged to publish translations of their legislation to facilitate this process.

Operators may be reluctant to recognise a firewall by legislation implemented in a Member State other than their place of business. Member States should support such recognition. When requested or at its own initiative, a Member State that has implemented a firewall by legislation should present its framework and share relevant information with other Member States. Member States should be in a position to satisfy themselves that the measures put in place indeed constitute an effective firewall. The Commission welcomes technical discussions in its Expert Group on EU sanctions.

Member States may choose to conclude a technical agreement for recognition of the firewall, which would be shared amongst all Member States and the Commission. The Commission would facilitate such agreements. This document could be published and relied upon by operators.

A Member State's refusal to recognise a firewall can be justified where the framework set up by a legislator does not meet the letter or spirit of the criteria in this guidance, or if there is insufficient information about the framework upon request.

b) Firewall by operators

As set out in section 2.2 (b), an operator that sets up a firewall may resort to an external third party, such as an auditor, to implement and/or certify the effectiveness of the changes to the entity's corporate governance.

In addition, a Member State must also organise an authentication process by which it would recognise the removal of control. In this case, an NCA must carry out the necessary checks to guarantee that the letter and spirit of this guidance have been respected. The NCA should also receive assurance that the designated person is no longer involved in the entity, for example by written statements from senior management.

A Member State may condition the authentication of a firewall upon the conduct of an external audit. In this case, the NCA should have the possibility to engage directly with the auditor to carry out its authentication and access all audit and corporate documents. The NCA may amend the scope of the audit as appropriate and reserve its right to refuse recognition where the auditor was not suitable or competent to perform such a mission.

Once the compliance of the firewall is established, the NCA must issue an official written confirmation. This document can be circulated by the entity as necessary to other Member States or any relevant party

(e.g. banks, clients, *etc*.). Such an authentication should be recognised by other Member States similarly to firewalls by legislation.

3.2 Recognition of firewalls in cross-border situations

Where a cross-border situation appears (see section 2.2 (c)), and whereas a firewall has been established in one or more subsidiaries of the same group, Member States must immediately reach out to other relevant Member States to share information to demonstrate the effectiveness of the firewall. To this end, Member States should rely on the 'technical agreement' obtained in the framework of a firewall by legislation (see section 2.2 (a)) and on the 'written undertakings' issued by the entity in the framework of a firewall by operator (see section 2.2 (b)).

While it is up to the competent national authorities to determine the recognition of firewalls, under the circumstances as they deem appropriate, their mutual recognition will be facilitated, provided that they are established according to the criteria specified in this guidance.

Annex 1: Criteria for the appointment of a third party in implementing a firewall by legislation

Regarding the <u>administration or supervision:</u>

- Surveillance and oversight (e.g. via an appointed administrator or supervisor) by an independent third party:
- General reporting obligations of the third party or board of directors to the NCA (e.g. on the nature of contacts between entity and the designated person, evidence to demonstrate that the firewall is implemented and subsequently respected).
- The administrator/supervisor replaces the designated person in the execution of the following rights:
    - attending meetings of the general meeting of shareholders, associates, board of directors, or any other meeting on the management of the entity;
    - accessing locations of operation of the entity;
    - accessing documents received by or emanating from the entity, related to financial-accounting, legal or otherwise;
    - remuneration for activities carried out.
- The administrator or supervisor must take actions necessary to ensure the proper implementation of EU sanctions and that transactions carried out by the entity are not directly or indirect benefitting the designated person.
- The administration or supervision is a temporary measure. It may last for as long as the relevant EU restrictive measure is in place. EU sanctions are kept under regular review to ensure that they continue to contribute towards achieving their stated objectives.

Regarding the <u>administrator or supervisor:</u>

- The administrator or supervisor is either a natural or a legal person (e.g. an accounting company).
- The decisive requirement is the independence of the administrator or supervisor.
- The administrator or supervisor must provide guarantees in terms of honourability, experience and competence to carry out the functions entrusted to it. To assess and monitor the administration and supervision, the supervisor or administrator should have regular direct reporting obligations to the NCA.
- The administrator or supervisor should be compensated by the administered/supervised entity.
- The liabilities of the administrator or supervisor are subject to national provisions. It may be held responsible for a violation of EU sanctions, for instance by assisting the circumvention of these measures.

Regarding <u>procedures for the appointment of the administrator or supervisor</u>:

- An application for the appointment of an independent administrator or supervisor may be made by the entity to the NCA of a Member State.
- Alternatively, an external administrator or supervisor may be installed by the entity itself with a notification made to the NCA for verification.

Annex 2: Criteria for firewalls by operators and the use of external audits in this context

Regarding the engagements to be undertaken by the entity implementing the firewall:

- The entity implementing the firewall must take actions necessary to ensure the proper implementation of EU sanctions and that transactions carried out by the entity are not directly or indirect benefitting the designated person (e.g., dividends, loan arrangements).
- The entity implementing the firewall and its leadership must give credible written assurance that allow for the removal of control by the designated person.
- The entity implementing the firewall and its executives (directors) must provide Member States NCA all information and documentation necessary to properly assess the actions undertaken and the assurances given by the entity implementing the firewall (e.g., articles of association, written assurances by senior management, bylaws, board minutes).
- The liabilities of the entity implementing the firewall and the relevant individuals are subject to national provisions. It may be held responsible for a violation of EU sanctions, for instance by assisting the circumvention of these measures.

Regarding the choice of auditor:

- The auditor is either a natural or legal person (e.g., an accounting company).
- The decisive requirement is the independence of the auditor, which generally rules out natural or legal persons that act as legally mandated statutory auditing companies for the entity implementing the firewall.
- The auditor must provide guarantees in terms of honourability, experience and competence to carry out the functions entrusted to it (e.g., membership in or certification by relevant professional bodies).
- The auditor should be compensated by the entity implementing the firewall.
- Member States' NCA may impose additional requirements, such as the auditor being established in the Member State's jurisdiction.
- Due to the reluctance of many operators to engage with entities linked to designated persons, it may be necessary for a Member State's NCA to support the entity implementing the firewall in finding an auditor, for example by issuing comfort letters.
- The liabilities of the auditor assessing the firewall implemented are subject to national provisions. It may be held responsible for a violation of EU sanctions, for instance by assisting the circumvention of these measures.

Regarding the scope of the audit:

- The auditor must assess the proper implementation of EU sanctions by the entity implementing the firewall, including that transactions carried out by the entity are not directly or indirect benefitting the designated person.
- The entity implementing the firewall must ensure that the auditor has access to all information and documentation necessary to carry out its mandate.
- Member States' NCA may impose specific requirements on the type of transactions being covered by the audit (e.g., transactions including the entity's ownership structure, intra-entity transactions not linked to the normal course of business).

- In the case of cross-border situations, Member States' NCA should recognise audits assessed and monitored by other Member States' NCA or a non-EU country implementing similar measures. To streamline the process in cross-border situation, transactions being covered by an audit assessed and monitored by one Member State or a non-EU country implementing similar measures should not be included in the scope of an audit assessed and monitored by another Member State.
- The liabilities of the auditor as well as the entity implementing the firewall are subject to national provisions. Both may be held responsible for a violation of EU sanctions, for instance by assisting the circumvention of these measures.

Regarding the <u>methodology of the audit</u>:

- To assess and monitor the audit, the auditor should have regular direct reporting obligations to the NCA. The NCA furthermore should have the possibility to engage directly with the auditor and access to all audit and corporate documents. The NCA might furthermore reserve its right to approve or reject proposals pertaining to the audit made by the entity implementing the firewall, including by amending the scope or methodology of the audit.
- Member States' NCA may impose specific methodological requirements governing the audit, such as professional or industry standards.
- Member States' NCA may impose specific requirements on the methodology used to assess specific types of transactions (e.g., risk-based approach versus full screening of all transactions).
- The audit is a temporary measure. It may last for as long as the relevant EU restrictive measure is in place. EU sanctions are kept under regular review to ensure that they continue to contribute towards achieving their stated objectives.
- The first audit must cover at least the time since the designated persons inclusion in the sanctions list. Subsequently, Member States' NCA should mandate periodic audits at appropriate regular intervals.