RULES
on the exchange of information and data between public authorities
in connection with actions against money laundering and terrorist financing

Art. 1
Objective

The objective of these Rules is to promote a broader and more effective co-operation between public authorities in actions against money laundering (ML) and terrorist financing (TF) by more specifically prescribing the sharing of information and data related to such actions, cf. Art. 40 of the Act on Actions Against Money Laundering and Terrorist Financing.

Art. 2
Scope

These Rules apply to those authorities that are members of the Steering Committee on Actions Against Money Laundering and Terrorist Financing referred to in the first paragraph of Art. 40 the said Act, when they communicate information and data between them relating to actions against ML/TF.

The Rules also apply to the dissemination of information and data under Act No. 64/2019, on Freezing of Assets and Entry on the List of International Coercive Measures, in connection with terrorist financing and the proliferation of weapons of mass destruction (WMD).

Art. 3
Grounds for sharing data

The authorities who fall within the scope of these Rules are obliged, either on their own initiative or upon request, to communicate information and data related to actions against ML/TF to other public authorities covered by the Rules, provided the information or data concern matters falling within the competence of the authority to which they are communicated.

Communication of information on the initiative of an authority may, for example, occur when the relevant authority considers that certain information or data may concern functions of another authority. In such cases, there is no need to establish definitively that the information or data does concern functions of another authority; rather, it is sufficient that the relevant authority considers that this could be the case. The relevant authority shall then, on its own initiative, send such information and data to the authority in question.

Communication of information and data on request could occur, for example, when the authority competent to handle a case concerning actions against ML/TF requests information or data relating to the case from another authority.

Furthermore, communication of information or data can also take place in connection with mutual assistance between authorities in cases involving actions against ML/TF.

When an authority requests information or data on the basis of these Rules, it shall inform the authority from whom information or data is requested of the grounds for the request, unless such disclosure could negatively impact the investigation or progress of a particular case or otherwise result in perverting justice.

Art. 4

Exchange of information and data

All dissemination of information and data under these Rules shall be carried out as securely as possible. As a rule, especially sensitive information and data, whether in physical or digital form, should be sent by courier. *Sending by courier* means that an employee of the authority that communicates information or data, or another person on its behalf, shall take the information or data, for example, in a sealed envelope or on a memory stick, to the authority to whom it is communicated and upon delivering it there obtain a confirmation of reception.

Notwithstanding the first paragraph of this Article, especially sensitive information and data may be sent by other means, e.g. by e-mail or registered letter, if the authority communicating information or data is of the opinion, for instance considering the nature of the information, that such means of transmission is sufficiently secure under the circumstances, for example, due to its encryption. The same applies when sending by courier is impossible.

In the case of information or data which is not especially sensitive, in the sense of the first paragraph of this Article, authorities may use other means of transmission. The most secure method of transmission available at any given time shall always be used, however.

The authority communicating information or data is responsible for this and for its security until it has been delivered to the authority to which the information or data is being communicated. This applies regardless of whether the communication takes place on the authority's own initiative or in response to a request. Information and data are deemed to *have been delivered to* an authority in this sense when they have been presented to, or received by, the employee handling the issue concerned at the relevant authority or any other employee who has been designated as competent to receive such information or data on behalf of the authority.

Once information or data has been submitted to the relevant authority, in the sense of the third paragraph of this Article, the latter is responsible for ensuring its preservation and security.

Communication of information and data, whether on an authority's initiative or upon request, shall be effected as promptly as possible. Generally speaking, the communication shall take place *within two working days* from the time a request is received or it is revealed that a particular case falls under the competence of another authority.

Art. 5

Information and data which should be communicated

Only information and data related to actions against ML/TF may be disseminated on the basis of these Rules.

In the case of information or data covered by these Rules, the authority which is to communicate the information is obliged to include all the information referred to in a request which concerns the matter in question in each instance.

An example of information and data which an authority may be obliged to communicate on its own initiative to other authorities under these Rules is information on the number of notifications sent to the Financial Intelligence Unit (FIU), the number and type of recommendations sent to obliged entities, and

information on new risks and vulnerabilities in connection with ML/TF which have been identified in specific areas or markets.

Art. 6

Use of shared information and data

Any authority receiving information and data under these Rules may only use the data and information provided in work on actions against ML/TF in accordance with its duties under the relevant Act.

Art. 7

Confidentiality

When communicating information and data pursuant to these Rules, the authorities communicating information or data are relieved of their obligations of confidentiality, cf. the first paragraph of Art. 40 of the Act on Actions Against Money Laundering and Terrorist Financing.

Authorities that receive under these Rules shared information or data which should be kept secret are bound by their confidentiality obligations and may not, on pain of liability under provisions of the Criminal Code on violations in public service, disclose such information or data to unauthorized persons, unless otherwise required by law or a court order.

Notwithstanding the provisions of the first paragraph, the FIU is not obliged to communicate information or data pursuant to these Rules, if such disclosure is likely to negatively affect current investigations or analyses. The same applies in cases where disclosure of information or data could cause damage to the parties in question which is not proportionate to the necessity for the information or data in question, or when the information or data requested does not accord with the purpose of the request. Assessment of whether such conditions apply is in the hands of the FIU.

Notwithstanding the provisions of the second paragraph of the Article, representatives on the Steering Committee referred to in Art. 39 of the Act on Actions Against Money Laundering and Terrorist Financing may communicate information or data within their own authorities which fall within their competence. An authority receiving information pursuant to this provision is bound by a duty of confidentiality pursuant to the first paragraph of the Article.

Art. 8

Forwarding of information and data

An authority that has received information or data under these Rules may absolutely not disclose the information or data to any third party without the express consent of the authority which communicated to it the information or data.

Art. 9

Personal data protection

Processing of personal data according to these Rules shall comply with the Act on Protection of Privacy regarding Processing of Personal Data, No. 90/2018, and the Act on Processing of Personal Data for Law Enforcement Purposes, No. 75/2019.

Art. 10

Feedback

When the FIU communicates information or data under these Rules, the authorities to which information or data is communicated shall provide the FIU with feedback on the information and data it has

communicated. By *feedback* is meant that the FIU is provided with a written response or comments on the information or data that was communicated. The feedback shall include, among other things, information on the use of the information or data communicated and on the results of the checks or investigations that have been carried out on the basis thereof.

Art. 11

Co-operation agreements

The authorities to which these Rules apply may conclude co-operation agreements between themselves, enabling them to further specify their co-operation on actions against ML/TF, including detailed arrangements for communication of information and data pursuant to these Rules. Such agreements shall be made in writing and reviewed at least every two years. A specimen of such a co-operation agreement is included as an appendix to these Rules.

Art. 12

Entry into force

These Rules, which are set in accordance with the sixth paragraph of Art. 40 of Act No. 140/2018, on Actions Against Money Laundering and Terrorist Financing, were approved at a meeting of the Steering Committee on Actions against Money Laundering and Terrorist Financing on 10 July 2019.

On behalf of the Steering Committee:

_____

Áslaug Jósepsdóttir
Chairman