

Disclosure of information regarding measure imposed on supervised entity

Supervisory measure against **Infra-Investments, d. o. o.** due to breaches identified in the area of anti-money laundering and combating the financing of terrorism (hereinafter: AML/CFT)

Information regarding person responsible for breach	
Business name and registered office of legal person	Infra-Investments, trgovina in storitve, d. o. o., Dunajska cesta 136, Ljubljana, registration no. 8015368000 (hereinafter: the company)
Information regarding breach	
Description of circumstances and conduct constituting a breach of the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia, Nos. 68/16, 81/19, 91/20 and 2/21, including amendments; hereinafter: the ZPPDFT-1)	<p>Banka Slovenije conducted an inspection of operations at the aforementioned company between 15 January 2021 and 16 April 2021.</p> <p>Breaches of the provisions of the ZPPDFT-1 were identified in the inspection, for which reason Banka Slovenije issued the company an order on the rectification of breaches, in accordance with the first paragraph of Article 151 of the ZPPDFT-1 in connection with Article 42a of the Bank of Slovenia Act (Official Gazette of the Republic of Slovenia Nos. 72/06 [official consolidated version], 59/11 and 55/17; hereinafter: the ZBS-1) and the first paragraph of Article 279 of the Banking Act (Official Gazette of the Republic of Slovenia, Nos. 92/21 and 123/21 [ZBNIP]; hereinafter: the ZBan-3), against which the company did not lodge an objection by the prescribed deadline.</p>
Nature of identified breaches	Taking into account the penal provisions of the ZPPDFT-1, the identified breaches are of the most serious nature.
Operational part of order for rectification of breaches	
<p>1. On the basis of an inspection of the operations of Infra-Investments d. o. o., Dunajska cesta 136, Ljubljana, registration no. 8015368000 (hereinafter: the company), in the area of anti-money laundering and combating the financing of terrorism (hereinafter: AML/CFT), which was initiated on the basis of Banka Slovenije request for inspection referenced PDO-24.70-002/20-1 of 18 December 2020, Banka Slovenije finds that the company is in breach of:</p> <p>a) points 2 and 5 of the first paragraph of Article 17 of the ZPPDFT-1 when it defined in its AML/CFT policy, with regard to transactions via Bitcoin ATMs, a limit on one-time transactions of EUR 1,000 and thus failed to ensure customer due diligence in the prescribed manner in the case of related transactions (point 2 of the first paragraph of Article 17 of the ZPPDFT-1), and when the amount of a transaction is lower than the aforementioned amount and there are reasons to suspect ML/TF in connection with that transaction, the customer who executes that transaction or the funds that are the subject of that transaction (point 5 of the first paragraph of Article 17 of the ZPPDFT-1). In the latter cases, the company cannot ensure compliance with the first paragraph of Article 69 of the ZPPDFT-1 with its current mode of operations; and</p> <p>b) the second paragraph in connection with the third paragraph of Article 13 of the ZPPDFT-1 when it assessed the risk of transactions via Bitcoin ATMs as negligible, although such transactions are deemed a high-risk service in accordance with the supranational risk assessment,¹ and by failing to conduct customer due diligence for the users of such services (customers) for transactions of up to EUR 1,000, and because such transactions are</p>	

¹ The supranational risk assessment report published by the European Commission in 2019 can be found under the reference COM(2019) 370 final, while the accompaniment to the report is published under the reference SWD(2019) 650 final.

completely anonymous on account of the associated distribution channel. Taking into account the above-stated facts, the company's risk assessment is inappropriate, as it does not reflect the proper method for assessing risks inherent in the services that it provides (the company assessed risks in connection with anonymous transactions in the exchange of virtual currencies into fiat currencies and vice versa as negligible, while it assessed risks in connection with OTC transactions via the company's current account as higher than risks in connection with the exchange of virtual currencies into fiat currencies and vice versa via Bitcoin ATMs).

To rectify the aforementioned breaches, the company must:

- a) comprehensively update previously adopted bylaws and eliminate identified discrepancies in accordance with the ZPPDFT-1 and, to that end, define appropriate operating procedures in its AML/CFT policy and implement them in practice, as the result of which the company will be capable of ensuring: (i) the performance of customer due diligence as set out in Article 16 of the ZPPDFT-1, including in the case of related transactions (point 2 of the first paragraph of Article 17 of the ZPPDFT-1) and the case of a transaction, regardless of the amount, where there are reasons to suspect ML/TF in connection with a transaction, customer or funds (point 5 of the first paragraph of Article 17 of the ZPPDFT-1), and (ii) the necessary reporting of identified suspicious transactions in accordance with the first paragraph of Article 69 of the ZPPDFT-1); and
- b) define and issue a risk assessment that will appropriately reflect inherent risks in connection with specific services, taking into account the fact that a service is deemed high-risk in terms of ML/TF when it involves transactions with virtual currencies via Bitcoin ATMs, where transactions are completely anonymous. In accordance with the fourth paragraph of Article 13 of the ZPPDFT-1, the company must also take into account the report on the findings of the national risk assessment and the supranational risk assessment.

The company shall embark without delay on activities to rectify the breaches cited in point 1 of this order on the rectification of breaches (hereinafter: the order). The final deadline for the rectification of the breaches is 31 December 2021. The company shall also submit a written report to Banka Slovenije within 10 days of the final deadline on the measures taken to rectify the breaches, as set out in the first paragraph of Article 281 of the ZBan-3.

2. In connection with the activities to rectify the breaches cited in point 1 of this order, the company shall draft an action plan clearly defining the activities for the rectification of the breaches, and shall submit it to Banka Slovenije by 30 July 2021.
3. In connection with the activities to rectify the breaches cited in point 1 of this order, the company shall designate the persons at the company responsible for rectifying the identified breaches, and shall report their names to Banka Slovenije by 30 July 2021.
4. An objection to this order shall not stay its enforcement (third paragraph of Article 375 of the ZBan-3 in connection with first paragraph of Article 151 of the ZPPDFT-1 and Article 42a of the ZBS-1).
5. The breaches identified in this order also constitute misdemeanours pursuant to the penal provisions of the ZPPDFT-1, and Banka Slovenije shall therefore initiate misdemeanours proceedings against the company and the responsible persons in these cases.
6. In accordance with Article 161 of the ZPPDFT-1, in connection with the imposed supervisory measures Banka Slovenije shall publish the following information on its website after the imposed

measure becomes final:

- the business name and registered office of the legal person or the name of the natural person;
- a description of the circumstances and conduct that represent a breach of the law or require the enforcement of the ordered measure;
- the nature of the identified breaches or the type of deficiencies for which the measure was ordered;
- the operational part of the decision by which the proceedings are legally finalised; and
- details of any rectification of a breach or implementation of an ordered measure.

Information regarding the potential rectification of a breach or implementation of an ordered measure:

The company has submitted an action plan for the rectification of breaches to Banka Slovenije in a timely manner, and reported the names of the persons at the company responsible for rectifying the identified breaches in a timely manner. The final deadline for the rectification of the breaches is 31 December 2021. The company shall also submit a written report to Banka Slovenije within 10 days of the final deadline on the measures taken to rectify the breaches.

Information as to whether judicial protection proceedings have been initiated against the decision in accordance with the ZBan-3

Judicial protection proceedings have not been initiated, and the decision is *res judicata*.