Disclosure of information on supervisory measure of 30 January 2023 imposed on credit institution

Information on person responsible for breach	
Business name and registered office of legal person	Primorska hranilnica Vipava d.d., Glavni trg 15, 5271 Vipava, registration number: 5214246000
Information on breach	
Description of circumstances and conduct entailing breach of ZBan-3 or Regulation (EU) No 575/2013	Breaches of the ZBan-3 (cited in detail in the operative part of the order below) were identified on the basis of an inspection, as a result of which Banka Slovenije issued the savings bank with the Order on the rectification of breaches referenced PBH-24.60-007/22-003 of 30 January 2023
Nature of identified breaches	Breach in the area of operational risk management

1. Primorska hranilnica Vipava d.d., of Glavni trg 15, 5271 Vipava, registration number: 5214246000 (hereinafter: the savings bank), has breached the first paragraph of Article 181 of the ZBan-3 in connection with:

1.1. Article 5 and the first paragraph of Article 17 of the Regulation on internal governance arrangements, the management body and the internal capital adequacy assessment process for banks and savings banks (Official Gazette of the Republic of Slovenia, No. 115/21; hereinafter: the internal governance regulation) and paragraph 2, point (a) of paragraph 13, and paragraph 14 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04 of 28 November 2019; hereinafter: the ICT guidelines),[1] by failing to put in place an adequate framework for the management of operational risk, and ICT risk in particular within this framework, that is aligned with regulatory changes in the area of ICT risk.

To rectify the breach the savings bank must put in place an adequate framework for the management of operational risk, and ICT risk in particular within this framework, such that it complies with changes in the sectoral regulations. The savings bank must regularly, at least once a year, assess its exposure to operational risk, properly define its appetite for the take-up of operational risk, and put in place mechanisms to ensure the appropriate quality of the data used for this purpose (including data quality in the capture of operational risk events);

1.2. paragraphs 33, 34 and 36 of the ICT guidelines, by failing to put in place sufficient and effective physical security measures to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards, and by failing to put in place sufficient and effective procedures to prevent the occurrence of security issues in ICT systems and ICT services, and to minimise their impact on ICT service delivery.

To rectify the breach the savings bank must put in place appropriate and effective measures to protect sensitive areas from environmental hazards, and appropriate and effective physical security measures in the system premises, put in place mechanisms to ensure that its network is only accessible to authorised devices having regard for the classification of ICT resources, and put in place access controls on the basis of appropriate electronic records or an appropriately maintained and viewed record of entries to the system premises, limited with regard to need by appropriate network segmentation. It must put in place mechanisms to

[1] The EBA Guidelines on ICT and security risk management are binding on banks and savings banks pursuant to the second paragraph of Article 2 of the Regulation on the application of the Guidelines on ICT and security risk management (Official Gazette of the Republic of Slovenia, No. 52/20).

identify and prevent penetrations and to prevent data loss or other equivalent mechanisms to protect its network, put in place encryption of data at rest and in transit in accordance with the data classification, define secure endpoints of the configuration of critical ICT resources, put in place mechanisms to prevent unauthorised persons from installing and using (unauthorised) software, and put in place appropriate updating of software;

1.3. paragraphs 56, 57 and 58 of the ICT guidelines, by failing to implement adequate and effective performance and capacity planning and monitoring processes to prevent, detect and respond to significant performance issues in a timely manner.

To rectify the breaches the savings bank must provide for adequate surplus capacity to enable the restoration of operations even after a catastrophic event with a sustained loss of capacity at its data centre, whereby the risk profile of the secondary location with adequate capacity may not be the same as the risk profile of the current data centre, align the backup of critical data and data restoration capacity with the target recovery state and the target recovery time after a catastrophic event, and put in place appropriate surplus or other equivalent capacity in the work of telecommunications connections, energy supply and air conditioning of server premises.

2. The savings bank has breached Article 182 of the ZBan-3 in connection with paragraphs 80 and 87 of the ICT guidelines and Section 3 (business continuity plan) of Appendix 3 (Operational risk) of the internal governance regulation, by failing to put in place business continuity plans, business continuity plans for ICT, and testing programmes for the business continuity plans and business continuity plans for ICT.

To rectify the breach the savings bank must formulate adequate business continuity plans and business continuity plans for ICT, put in place a testing programme for the business continuity plans and business continuity plans for ICT, and ensure that the business continuity plans and business continuity plans for ICT are tested at least once a year, whereby the scope of the testing is sufficiently representative to draw conclusions about the capacity to ensure an effective response to serious disruptions to operations (e.g. recovery after a catastrophic event).

3. The savings bank's management board must submit a detailed action plan stating the measures selected to rectify the breaches referred to in points 1 and 2 of this order to Banka Slovenije by 28 February 2023. The action plan of the savings bank's management board must define the timetable for the implementation of individual measures, and the persons responsible for the implementation of individual measures and activities in accordance with the internal organisational structure of the savings bank.

4. The savings bank must:
- rectify the breaches referred to in indents 1.2 and 1.3 of point 1 of this order by 30 June 2023, and deliver a report to Banka Slovenije by 15 July 2023, attaching documents and other evidence from which it is evident that the breaches have been rectified;
- rectify the breaches referred to in indent 1.1 of point 1 and in point 2 of this order by 31 December 2023, and deliver a report to Banka Slovenije by 15 January 2024, attaching documents and other evidence from which it is evident that the breaches have been rectified.

5. An objection to this order shall not stay its enforcement.

6. In accordance with Article 310 of the ZBan-3, the following information in connection with this supervisory measure shall be published on the Banka Slovenije website after these proceedings have been completed:
1. information about the breach:
- a description of the circumstances and conduct entailing a breach of the ZBan-3 or Regulation (EU) No 575/2013,

- the nature of the identified breaches; 2. the operative part of the decision by which the relevant proceedings are completed; 3. information as to whether judicial review proceedings have been initiated against the decision in accordance with the ZBan-3. In accordance with the second paragraph of Article 311 of the ZBan-3, the publication of the identity of the person responsible for the breach shall be withheld until the rectification of the breaches referred to in the first and second points of the operative part of this order.
Information as to whether judicial review proceedings have been initiated against order on rectification of breaches in accordance with ZBan-3
The savings bank has not initiated judicial review proceedings against the order on the rectification of breaches.
Information on any rectification of breach or implementation of ordered measure
The credit institution rectified the breaches by the set deadline. Banka Slovenije issued decisions on 21 November 2023 and 14 May 2024 determining that the breaches had been rectified.