Disclosure of the supervisory measure against credit institution of 24. 1. 2017

Information on person responsible for breach	
Business name and registered office of legal person	
Information on breach	
Description of circumstances and conduct entailing breach of ZBan-2 or Regulation (EU) No 575/2013	On the basis of the request for on-site inspection no. PBH-24.60-005/16-001 of 23 May 2016 and Bank of Slovenia authorisation no. PBH-24.60-005/16-002 of 23 May 2016, between 6 June and 30 August 2016 Bank of Slovenia staff conducted an on-site inspection of credit institution in the area of liquidity risk, interest rate risk, operational risk and organization of the credit institution. On the basis of the findings of the on-site examination and the discussion at the 571th meeting of the Governing Board of the Bank of Slovenia, a resolution was passed issuing an order on the rectification of breaches in the area of risk control of operational risk (ensuring adequate staff for support and control services and in providing IT services (management of information technology, incident management, management of IT assets and business continuity management).
Nature of identified breaches	The breaches identified in the area of risk control on operational risk, are cited in the operational part of the Order on the rectification of breaches.

Operational part of the decision by which the relevant proceedings are completed

1. Credit institution has breached:
   - points 1 and 2 of the first paragraph of Article 128 of the ZBan-2 in connection with Articles 9, 13 and 14 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, Nos. 73/15 and 49/16; hereinafter: the internal governance regulation), by failing, as a result of inadequate HR policy, to put in place suitable replacements and a succession plan in the management of the Information Technology support function (hereinafter: the IT function) and the Operations support function, thereby failing to manage the operational risk inherent in the lengthy absence or the unexpected termination of the employment relationship of the aforementioned key function holders, and also failing to ensure unimpeded functioning with regard to the credit institution's operational needs and the scale and complexity of the risks to which it is exposed;
   - points 1 and 2 of the first paragraph of Article 128 of the ZBan-2 in connection with Articles 9 and 13, the first paragraph of Article 32 and the fourth paragraph of Article 33 of the internal governance regulation, by failing, as a result of inadequate HR policy, to provide for a sufficient number of qualified employees with regard to the credit institution's operational needs, and the scale and complexity of the risks inherent in the IT function, and failing to provide for adequate internal controls within the aforementioned function, and by failing to ensure the requisite segregation of powers and responsibilities in the implementation of work procedures, in particular organisational separation, the implementation of the four eyes principle, and mutual vetting, owing to the assignment of tasks from various areas of IT to the same employee;
   - the second paragraph of Article 138 and the second paragraph of Article 147 of the ZBan-2 in connection with Articles 9 and 13 and the first paragraph of Article 20 of the internal governance regulation, by failing, as a result of inadequate HR policy, to provide for a sufficient number of qualified employees with regard to the credit institution's operational

needs, and the scale and complexity of the risks inherent in the risk management function, in particular in the area of operational risk and interest rate risk, where regular tasks have not been performed or have not been performed in timely fashion (e.g. in the area of operational risk: an inventory of business processes, an annual assessment of risk exposure), and in the security engineer function, where the credit institution not have a suitable replacement.

To rectify the identified breaches the credit institution must draw up analysis and upgrade its HR policy to provide for a sufficient number of qualified employees. In so doing it must also provide for the adequate deputisation of the management of the Operations and IT support functions. In drawing up the analysis and upgrading the HR policy, the credit institution should take account of the nature, scale and complexity of the risks inherent in its business model, and the requirements with regard to the effective implementation of risk management processes at the credit institution. The analysis must include targets with regard to ensuring a sufficient number of qualified employees, and the measures to meet these targets.

2. The credit institution has breached point 3 of the first paragraph of Article 128 of the ZBan-2 in connection with Articles 6 and 7, the second paragraph of Article 19, Article 31, point 3 of the first paragraph and the fourth paragraph of Article 33 and the first paragraph of Article 82 of the internal governance regulation, because it has deficient internal control mechanisms in the sense of rules for and controls of the implementation of the credit institution's organisational procedures, business procedures and work procedures in the area of its information system.

   To rectify the identified breach the credit institution must provide for adequate rules for and controls of the implementation of procedures in the area of information technology management, incident management, the management of information resources, and business continuity management.

   The credit institution must put in place and implement a policy for risk take-up and management in the area of information technology, on the basis of which the regular and systematic identification, monitoring and management of risks are ensured. Information technology risk management must include the regular drafting of reports for the credit institution's management board on exposures to these risks, and on this basis must provide for the formulation, implementation and control of adequate measures for the management of risks in the area of information technology.

   The credit institution must provide for a comprehensive system for the management of security incidents in the area of information technology that includes the use of appropriate support tools and systems (SIEM).

   The credit institution must provide for an effective system for the management of information resources by updating custody over information resources and upgrading the internal rules and controls in the area of ensuring the compliance of licensed software that the credit institution uses in its operations.

   The credit institution must conduct appropriate risk analysis in the area of business continuity management, and on this basis must provide for appropriate measures in the sense of duplication of key components of the information system.

   The credit institution must take appropriate account of all of the credit institution's identified material risks, including risks inherent in the introduction of new products and the use of external contractors, in the ICAAP.

3. The credit institution's management board must submit an action plan detailing the measures selected to rectify the breaches referred to in points 1 and 2 of this order to the Bank of Slovenia by 28 February 2017, and must rectify the aforementioned breaches by 30 August 2017.

   In the action plan the credit institution'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 credit institution's internal

organisational structure.

The credit institution must report to the Bank of Slovenia on the implementation of measures on a monthly basis in accordance with the action plan, by the tenth day of the current month for the previous month (regular report), or without delay in the event of the occurrence of material facts and circumstances affecting the implementation of the action plan (*ad hoc* report), compiling the first regular report for the situation as at 31 March 2017.

By 28 February 2017 the credit institution must report to the Bank of Slovenia the name of the responsible member of the management board and the names of the responsible persons designated in accordance with the credit institution's internal organisational structure, or the names of the credit institution's external contractors, who will be responsible for implementing individual activities to rectify breaches and for preparing and implementing the action plan referred to in point 3 of this order.

4. In accordance with Article 277 of the ZBan-2, the following information in connection with this supervisory measure shall be published on the Bank of Slovenia website after these proceedings have been completed:
   - information on the breach:
   - a description of the circumstances and conduct entailing the breach,
   - the nature of the identified breaches;
   - the operational part of the decision by which the relevant proceedings were completed; and
   - information as to whether judicial protection proceedings have been initiated against the decision in accordance with the ZBan-2.

   In accordance with the second paragraph of Article 278 of the ZBan-2 in connection with the first paragraph of Article 278 of the ZBan-2, the identity of the person responsible for the breach, i.e. the identity of the bank, shall not be published.

Information as to whether judicial protection proceedings have been initiated against the decision in accordance with the ZBan-2

Judicial protection proceedings have not been initiated against the decision.