Pursuant to Article 10, paragraph 1, and Article 63, paragraph 4 of the Law on Digital Assets (RS Official Gazette, No 153/2020) and Article 18, paragraph 1, item 3) of the Law on the National Bank of Serbia (RS Official Gazette, Nos 72/2003, 55/2004, 85/2005 – other law, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – CC decision and 44/2018), the Governor of the National Bank of Serbia hereby issues

D E C I S I O N
ON CONDITIONS OF INFORMATION-COMMUNICATION SYSTEM MANAGEMENT FOR VIRTUAL CURRENCY SERVICE PROVIDERS

I. INTRODUCTORY PROVISIONS

1 This Decision sets out the conditions of safe and sound operations pertaining to the management of the information-communication system of a digital asset service provider in the part of operations pertaining to virtual currencies (hereinafter: service provider).

This Decision also regulates minimum standards for managing business continuity and disaster recovery.

2. For the purposes of this Decision, the following definitions shall apply:

1) *virtual currency user* means a natural person, entrepreneur or legal person who is using or has used a virtual currency service or who has approached a service provider with a view to using that service;

2) *virtual currency transaction* means a purchase, sale, acceptance or transfer of a virtual currency or exchange of a virtual currency for another virtual currency and/or other digital assets;

3) *virtual currencies trading platform* means a multilateral system which organises trading in virtual currencies, which is run by the platform operator, and which brings together or facilitates the bringing together of third-party buying and/or selling interests in virtual currencies, and/or exchange of virtual currencies for other virtual currencies and/or other digital assets, in accordance with its non-discretionary rules and in a way that results in a contract;

4) *crypto ATM* means an automated machine for the purchase and sale of virtual currencies for money or the exchange of virtual currencies for other virtual currencies and/or other digital assets;

5) *information-communication system* is a comprehensive set of technological infrastructure (hardware and software components),

organisation, people and procedures for collection, storage, processing, keeping, transfer, display and use of data and information;

6) *information-communication system resources* include software components, hardware components and information goods;

7) *software components* include all types of systemic and application software, software development tools and other software;

8) *hardware components* include computer equipment, communications equipment, data storage media as well as other technical equipment serving as a support to the information-communication system functioning;

9) *information goods* include data in files and databases, programme code, configuration of hardware components, technical and user documentation, general internal regulations, procedures etc.;

10) *information-communication system users* are all persons authorised to use the information-communication system (employees in the service provider, employees in other persons accessing the service provider's information-communication system, virtual currency users who access the service provider's information-communication system through electronic interactive communication channels etc.);

11) *information-communication system risk* is the possibility of occurrence of negative effects on the financial result and the capital, the realisation of business objectives, legal compliance and reputation of the service provider due to inadequate management of the information-communication system or other weaknesses in the system which negatively affect its functionality or security, i.e. jeopardise business continuity;

12) *controls* are policies, procedures, practices, technologies and organisational structures pertaining to the information-communication system, set up in order to ensure a reasonable assurance that business objectives of the service provider will be realised and that undesirable events will be prevented or detected. Controls may differ according to the manner of application (management, technical and physical) and purpose (preventive, detective and corrective);

13) *management controls* include the adoption and application of policies, standards, plans, procedures and other internal regulations, as well as the setting up of an appropriate organisational structure with a view to achieving and maintaining an adequate level of functionality and security of the information-communication system;

14) *technical controls* are the controls applied in hardware and software components of the information-communication system;

15) *physical controls* are the controls which protect information-communication system resources from unauthorised physical access, theft, physical damage or destruction;

16) *preventive controls* are the controls intended for the prevention of problems and incidents;

17) *detective controls* are the controls intended for detection and recognition of problems and incidents and pointing out to the problems and incidents that occurred;

18) *corrective controls* are the controls intended for limiting and removing the problems and consequences of incidents;

19) *incident* is every unplanned and undesirable event that may jeopardise the security or functionality of the information-communication system;

20) *security of the information-communication system* implies preserving confidentiality, integrity, availability, authenticity, provability, irrefutability and reliability in the information-communication system;

21) *confidentiality* means that data and information are not disclosed or accessible to unauthorised persons;

22) *integrity* means that data, information and processes are protected from unauthorised or unforeseen changes, and/or that any such potential changes do not remain unnoticed;

23) *availability* means that data, information and processes are accessible and usable at the request of an authorised person;

24) *authenticity* means that the person's identity truly is what it is claimed to be;

25) *accountability* means that each activity in the information-communication system may be unambiguously traced to its source;

26) *non-repudiation* means inability to repudiate activities carried out in the information-communication system or the receipt of information;

27) *reliability* means that the information-communication system consistently and expectedly performs the envisaged functions and provides accurate information;

28) *authorisation* is a process of granting access rights to information-communication system users;

29) *identification* is a process of introducing the user of an information-communication system when logging in and carrying out activities in the system;

30) *authentication* is a process of verifying and confirming user identity by using one of the following elements or their combination:

– something only the user knows (e.g. password, personal identification number etc.),

– something only the user has (e.g. magnetic card, chip card, token, cryptographic key etc.),

– something only the user is (biometric characteristics such as a a fingerprint, iris, voice, handwriting etc.);

31) *privileged access to the information-communication system* is access to the resources of the information-communication system which enables authorised users (system software administrators, network administrators, database administrators etc.) to bypass technical controls;

32) *remote access to the information-communication system* is access to the information-communication system resources from a remote location via a telecommunications infrastructure over which the service provider does not have full control;

33) *operational and system records* mean chronological records about events and activities on the resources of the information-communication system (records of operating systems, application software, databases, network devices etc.);

34) *malware* is any form of a programme code created with the intention to gain unauthorised access to information-communication system resources, gather information, provoke unexpected behaviour or interruption in the system functioning and/or in some other way potentially undermine confidentiality, integrity or availability of those resources (e.g. computer viruses, the so-called worms, Trojan horses etc);

35) *critical/key business processes* are business processes or functions whose inadequate functioning may significantly jeopardise service provider's operations;

36) *maximum acceptable outage (MAO)* means the longest acceptable period of a business process unavailability, and/or critical time for the process recovery;

37) *backup copy* is the copy of at least those source data (software components and information goods) that are needed for the recovery, and/or re-establishment of the business processes;

38) *electronic services* are virtual currency services referred to in Article 3, paragraph 1 of the Law on Digital Assets which virtual currency users use from a remote location, online, including the use of those services via a crypto ATM, as well as other activities for accessing data related to virtual currency services which could be the subject of fraud or other abuses.

II. MANAGING THE INFORMATION-COMMUNICATION SYSTEM

3. A service provider shall establish an adequate information-communication system, which meets at least the following conditions:

1) possesses functionalities, capacities and performances which enable the provision of appropriate support to business processes in relation to the provision of virtual currency services;

2) ensures timely, accurate and complete information relevant for making business decisions, efficient carrying out of business activities and risk management, and/or for safe and sound operations;

3) is designed with appropriate controls for data validation at entry, in the course of processing and at exit from the system, with a view to preventing inaccuracy and inconsistency in data and information;

4) possesses appropriate controls in order to prevent incidents occurring due to a cyber-attack, theft or other malfunctions and in order to safeguard the security of the information-communication system.

4. The service provider shall establish by a general internal regulation, in accordance with the law, authorisations and responsibilities of its management and supervisory bodies which pertain to the safeguarding of security and functionality of the information-communication system.

The service provider shall supervise, regularly update and improve the process of managing the information-communication system in order to reduce exposure to the risks related to that system.

5. The service provider shall adopt the information-communication system development strategy, which may be an integral part of its business strategy.

The service provider shall change the information-communication system development strategy on as needed basis and especially if that is required by the changes and/or additions to its business strategy.

6. For the purpose of adequate management of the information-communication system, the service provider shall ensure an appropriate organisational structure with a clearly defined allocation of employees' tasks and duties and/or established internal controls which prevent a conflict of interest.

As part of the allocation of tasks and duties referred to in paragraph 1 hereof, the service provider shall in particular clearly define the tasks and duties of employees who have a direct impact on the efficient and appropriate management of the information-communication system security.

7. The service provider shall ensure that all general internal regulations and procedures related to the information-communication system are applied and that all users of that system are acquainted with the contents of those regulations and procedures, in accordance with their authorisations, responsibilities and needs.

8. The service provider shall set the criteria, manner and procedures for reporting to its competent body about the relevant facts relating to the information-communication system functionality and security.

III. MANAGEMENT OF THE INFORMATION-COMMUNICATION SYSTEM RISK

9. The service provider shall set up, within a comprehensive risk management system, the process of managing the information-communication system risk which includes identifying, measuring and/or assessing that risk, as well as its mitigation, monitoring and control.

The service provider shall regularly monitor and assess the adequacy of controls applied in order to mitigate the identified information-communication system risks.

10. The service provider shall manage the information-communication system risk in such a way as to ensure unhindered management of the system's security and management of its business continuity.

The management of the information-communication system risk must include the overall information-communication system of the service provider and be integrated in all the phases of development of that system.

11. The service provider shall adequately manage the risks arising from contractual relations with legal and natural persons whose activities relate to its information-communication system.

The service provider shall continuously supervise the manner and quality of implementation of agreed activities referred to in paragraph 1 hereof.

12. The provisions of the regulations governing general terms and manner of managing risks in the operations of the service provider shall also apply to the management of the information-communication system risk.

IV. INTERNAL AUDIT OF THE INFORMATION-COMMUNICATION SYSTEM

13. The service provider shall cover, by internal audit methodology, the criteria, manner and procedures of risk-based internal audit of the information-communication system.

14. Internal audit of the information-communication system is carried out in accordance with the regulations governing the service provider's operations.

V. SECURITY OF THE INFORMATION-COMMUNICATION SYSTEM

15. The service provider shall adopt a general internal regulation setting up a framework for managing the information-communication system security (hereinafter: security policy).

The security policy shall regulate in particular the principles, manner and procedures of achieving and maintaining an adequate level of the information-communication system security, as well as the authorisations and responsibilities related to that security and the system's resources.

The service provider shall align the security policy with the changes in the environment and in the information-communication system itself.

16. The service provider shall set up the process of managing the information-communication system security as a continuous process of identifying the need for this security and achieving and maintaining an adequate level of that security, based, as a minimum, on the assessment of risks in the system and the obligations arising from the regulations, general internal regulations, contractual relations etc.

17. In order to achieve and maintain an adequate level of information-communication system security, the service provider shall set up appropriate controls.

18. The service provider shall conduct an appropriate control of access to information-communication system resources and set up an adequate system of managing user access rights.

The system of managing user access rights shall in particular include the processes of recording the users of the information-communication system, authorisation, identification and authentication, as well as the oversight over user access rights.

The service provider shall ensure that the authorisation of information-communication system users is based on the principle of granting minimum possible rights of access to the system's resources which enable efficient performance of tasks.

The service provider shall, periodically and on as needed basis, but at least once a year, update user access rights.

In managing user access rights, the service provider shall regulate in particular the privileged and remote access to the information-communication system.

19. Based on the assessment of the information-communication system risk, the service provider shall set up an adequate system of oversight of the system and generation of operational and system records, as well as ensure an appropriate protection of those records and determine the period of keeping and the frequency, scope and manner of monitoring those records.

The records referred to in paragraph 1 hereof must contain sufficient quantity of information for problem detection, event reconstruction and detection of unauthorised access and activities on information-communication system resources, as well as for determining responsibility in that regard.

20. By applying appropriate controls, the service provider shall protect the resources of the information-communication system and other systems supporting the information-communication system functioning from unauthorised physical access, theft and physical damage or destruction caused by a human or natural factor.

In case of renting a computer centre, the service provider shall make sure that the appropriate controls referred to in paragraph 1 hereof have been applied.

21. The service provider shall in particular ensure the integrity of data about virtual currency transactions executed based on the orders of virtual currency users, as well as in their processing, keeping and undertaking all other actions related to such data.

22. The service provider shall apply appropriate controls and technical solutions to protect the information-communication system resources from malicious software and cyber-attacks.

VI. BUSINESS CONTINUITY AND DISASTER RECOVERY

23. For the sake of ensuring unhindered and continuous functioning of all of its important systems and processes and limiting losses in emergency situations, the service provider shall set up the process of managing business continuity.

24. The service provider shall ensure that business continuity management is based on the business impact analysis and risk assessment.

The business impact analysis shall in particular include:

1) identifying resources and systems needed for the implementation of individual business processes and their interdependencies and interconnectedness;
2) assessment of the risks related to individual business processes, including the probability of occurrence of undesirable events and their potential impact on business continuity, financial status and reputation of the service provider;
3) establishing acceptable levels of risk and techniques for mitigating the risks identified;
4) establishing critical/key business processes and activities;
5) establishing the maximum acceptable outage (MAO) of individual business processes.

25. Based on the activities undertaken in accordance with Section 24 of this Decision, the responsible body in the service provider shall adopt a business continuity plan and a disaster recovery plan which primarily regulate the creation of conditions for the recovery and availability of information-communication system resources necessary for the implementation of critical/key business processes.

The business continuity plan shall contain in particular:

1) description of procedures in case of business interruption;
2) updated list of all resources needed to re-establish business continuity;
3) data about teams which will be responsible for re-establishing business continuity in case of occurrence of unforeseen events and the designated members of those teams, including their clearly defined duties and responsibilities and the plan of internal and external lines of communication;
4) backup location – in case of business interruption and inability to re-establish business processes at the primary location.

The disaster recovery plan shall contain in particular:

1) procedures for the disaster recovery of the information-communication system;
2) priorities of the recovery of information-communication system resources;
3) data about the teams which will be responsible for the information-communication system recovery and designated members of those teams, including their clearly defined duties and responsibilities;

4) backup location for the information-communication system recovery, i.e. the location of the backup computer centre.

For the sake of efficient implementation of plans referred to in paragraph 1 hereof, the service provider shall ensure that all employees are acquainted with their roles and responsibilities in case of emergency.

The service provider shall take all the necessary activities in order to align the plans referred to in paragraph 1 hereof with the business changes, including changes in products, activities, processes and systems, changes in the environment, as well as the business policy and strategy.

The service provider shall test the plans referred to in paragraph 1 hereof periodically and after the occurrence of significant changes, but at least once a year, and shall document the results of those tests and ensure that they are included in the reporting to the competent body of the service provider.

The competent body of the service provider shall be responsible for the implementation of plans referred to in paragraph 1 hereof.

26. In managing business continuity, the service provider shall consider outsourced activities and the dependence on services provided by third parties.

27. In case of circumstances which require the implementation of business continuity and disaster recovery plans, the service provider shall inform the National Bank of Serbia thereof, no later than the next day after such circumstances occur. The National Bank of Serbia may request additional documents relating to the relevant facts about these circumstances and set a deadline for the submission of those documents.

28. The service provider shall set up an incident management process ensuring a timely and efficient response in the case of any threats to the security or functionality of information-communication system resources.

The service provider shall inform the National Bank of Serbia about the incident which seriously jeopardised or undermined its operations, and/or which could seriously jeopardise or undermine its operations, namely:

1) if it occurred due to the undermined functionality of information-communication system resources – immediately upon establishing the circumstances of the occurrence of such incident;

2) if it occurred due to the undermined security of the information-communication system – immediately upon learning about the incident;

3) if it occurred in a third party within the meaning of Section 37, paragraph 5 of this Decision and had or could have had a significant impact on the service provider's information-communication system – immediately upon establishing the circumstances of the occurrence of such incident, and/or upon learning about such incident.

Upon the notification referred to in paragraph 2 hereof, if the incident is ongoing, the service provider shall continuously inform the National Bank of Serbia about the important events and other relevant information related to the incident from that paragraph (incident status), and the activities taken to mitigate the incident and its consequences. The notification shall contain also a detailed description of the incident, information about the number of users of virtual currencies which were affected by the incident, the roughly estimated time needed to resolve the incident, potential impact on other service providers, as well as the relevant events and other relevant information since the incident occurrence (e.g. information on whether the incident escalated, whether new causes were discovered and about the efficiency of the applied activities).

The service provider shall submit to the National Bank of Serbia the final report on the incident from paragraph 2 hereof within 15 days since the cessation of the incident, i.e. since the day it has estimated that its regular operations and stable work of the information-communication system have been established. The report shall contain final information about the incident – start and end dates, duration, type (inaccessibility of hardware components, problems in operation of software components or a security incident), description of the incident, causes of occurrence and consequences of the incident, activities implemented during the incident, plan of preventative actions precluding repeated occurrences of the same incident, the number of users of virtual currencies affected by the incident, financial costs incurred in relation to the incident, impact on other service providers and other relevant information as needed.

In accordance with paragraphs 1 and 2 hereof, the service provider shall inform the National Bank of Serbia about the incidents relating to the abuse of sensitive data of virtual currency users, unauthorised virtual currency transactions, technical manipulations on crypto ATMs, fraudulent actions and abuses of virtual currency users, abuses of authentication factors and system etc. which had no direct impact on its information-communication system.

The National Bank of Serbia may request additional documents in relation to the relevant facts about the circumstances and consequences of the incident that occurred and set a deadline for the submission of those documents.

29. The service provider shall set up the process of backup management and establish detailed procedures and responsibilities for that purpose.

Backup management must include the procedures of preparing, keeping and testing backup copies and recovering data and software components, in order to enable the re-establishment of business processes.

The service provider shall ensure that backup data copies are updated and adequately protected and that the recovery procedures are tested and effective.

Minimum one updated and complete backup data copy must be adequately stored in a remote and safe location.

VII. DEVELOPMENT AND MAINTENANCE OF THE INFORMATION-COMMUNICATION SYSTEM

30. The service provider shall implement the process of development of the information-communication system in accordance with the information-communication system development strategy, considering the functional requirements and security needs.

In the course of independent development of the information-communication system, the service provider shall set up and document that development process, including the analysis and design, programming, testing and transfer to production.

The service provider shall set up and appropriately separate test and production environments.

In case of an independent development of the information-communication system, apart from the environments referred to in paragraph 3 hereof, the service provider shall also set up a development environment.

31. The service provider shall set up a process of management of hardware and software components in all phases of their lifecycle – from procurement or development to withdrawal from use.

32. The service provider shall ensure adequate maintenance of hardware and software components of the information-communication system according to manufacturer's recommendations and keep the records on that maintenance, as well as take care not to jeopardise the system's security or functionality during maintenance.

In accordance with paragraph 1 hereof, the service provider shall adequately supervise the outsourced activities relating to the maintenance of hardware and software components of the information-communication system.

33. The service provider shall establish the process of managing changes in hardware and software components of the information-communication system, in order to prevent these changes from causing unexpected or undesirable system behaviour and/or undermining system security or functionality.

The service provider shall ensure that all changes in hardware and software components, including new components and systems are tested and approved prior to release to production, as well as set up a rollback plan.

The service provider shall regulate by a general internal regulation the process of managing emergency changes in hardware and software components of the information-communication system.

34. The service provider planning data migration to the new virtual currency trading platform, introduction of a new virtual currency trading platform or data migration to another computer centre, and/or which changes the computer centre location, shall notify the National Bank of Serbia thereof minimum 30 days prior to the beginning of testing related to that migration.

The notification from paragraph 1 hereof shall contain in particular:

1) detailed description of systems between which the data are transferred, and/or description of a new virtual currency trading platform;
2) plan, dynamics and description of activities related to switching to a new virtual currency trading platform, or to another computer centre;
3) results of risk assessment and description of controls to be applied in the course of data migration with a view to preserving data confidentiality, integrity and availability;
4) the rollback plan to the status prior to data migration, including the dynamics of the rollback and description of activities, as well as the criteria for making the decision to apply that plan.

Notwithstanding paragraph 1 hereof, the service provider which plans data migration due to the status change for which it is obliged to obtain approval, and/or licence of the National Bank of Serbia shall, simultaneously with applying for such approval and/or licence, submit to the National Bank of Serbia the notification with the data from paragraph 2 hereof.

The National Bank of Serbia may request additional documents in relation to the relevant facts and circumstances of migration referred to in paragraphs 1 and 3 hereof.

35. The service provider shall ensure the preparation, keeping and regular updating of the documents relating to the information-communication system, so that such documents are accurate, complete and up-to-date at all times.

The service provider shall ensure access to appropriate documents in accordance with business needs to all users of the information-communication system.

36. The service provider shall ensure adequate and continuous professional training for employees in terms of using the information-communication system and safeguarding its security and functionality.

VIII. OUTSOURCING OF ACTIVITIES RELATED TO THE INFORMATION-COMMUNICATION SYSTEM

37. Outsourcing of the activities related to the information-communication system to third parties (hereinafter: outsourcing) shall be done in accordance with the regulations governing the operations of the service provider and this Decision.

The activities referred to in paragraph 1 hereof shall be all activities including processing, keeping and/or accessing data available to the service provider which pertain to its operations, as well as activities of development and/or maintenance of key business applications and platforms for trading in virtual currencies.

Outsourcing shall include also the outsourcing to persons connected with the service provider by property and management links (persons with a holding, members of the group of companies to which that service provider belongs etc.) operating in the Republic of Serbia or abroad.

The use of standardised services or telecommunications services or purchase of off-the-shelf solutions shall not be considered to be outsourcing etc.

Outsourcing is based on a contract concluded between the service provider and a third party to which the activities are outsourced (hereinafter: third party).

Within the meaning of this Decision, outsourcing shall not pertain to the service provider's activities directly relating to the provision of virtual currency services referred to in Article 3, paragraph 1 of the Law on Digital Assets.

38. A service provider intending to outsource certain activities shall regulate:

1) the process of deciding about the outsourcing and the criteria for making such decision;
2) the manner of inclusion of those activities in the risk management process and the system of internal reporting about the risks;
3) the manner in which it shall ensure the continuity of performance of outsourced activities and the measures to be taken in the case of termination of the contractual relation with third parties, as well as in the case of a temporary halt or cessation of service provision by third parties;
4) the manner of supervising outsourced activities, including the supervision of compliance of outsourced activities with the regulations, good business practices and generally accepted standards in the relevant area.

39. The service provider shall ensure that the third party provides a timely and unlimited access to the documents and data relating to outsourced activities to the service provider, external auditor and the National Bank of Serbia.

The service provider shall ensure that each contract concluded with a third party contains a provision whereby the third party is obliged to fulfil the obligation from paragraph 1 hereof, as well as the provision enabling the service provider to unilaterally terminate that contract if so ordered by the National Bank of Serbia and in accordance with that order.

The service provider shall also ensure that the National Bank of Serbia may perform unhindered on-site supervision of outsourced activities at the third party's premises, and/or at the location where the outsourced activities are carried out.

40. The service provider shall ensure that the outsourcing of activities does not jeopardise security or functionality of the information-communication system and that the data remain in its possession.

The service provider shall ensure that the third party carries out the outsourced activities in accordance with the service provider's security policy, as well as with the regulations and professional standards governing the security of its information-communication system.

In the outsourcing of activities and/or performing of outsourced activities the service provider and a third party shall act in accordance with the law governing personal data protection and other regulations governing the keeping of a secret which occurred in service provider's operations.

41. The service provider may outsource certain activities and/or replace a third party only if it has notified the National Bank of Serbia thereof no later than 30 days prior to concluding the outsourcing contract.

If the contract from paragraph 1 hereof is changed without changing the outsourced activity, and/or the scope of outsourced activities (adding new functionalities, modules etc.) or without changing the third party – the service provider shall, no later than 15 days prior to concluding the annex to the contract, notify the National Bank of Serbia thereof and send to it the draft annex.

The notification from paragraph 1 hereof shall contain in particular:

1) decision of the service provider's responsible body about the outsourcing of an activity and/or change of the third party;

2) description of activities that the service provider intends to outsource, obligations and conditions that the third party is required to fulfil and the period of outsourcing;

3) basic data about the third party (business name, head office, registration number and TIN and/or other appropriate data for a foreign person);

4) draft outsourcing contract;

5) results of the analysis of a potential third party relating to its ability to provide services, financial status and business reputation;

6) exit strategy whereby the service provider estimated the potential difficulties and the time needed for the selection of a new third party or the possibility of continued independent performance of these activities in the case of termination of provision of agreed services, which must include a list of measures and activities that need to be taken and the timeframe of their implementation from the moment of termination of provision of agreed

services until the selection of a new third party or the full establishment of an independent process of performance of those activities;

7) results of the assessment of the impact of outsourcing on business continuity, reputation, costs, financial result and risk profile of the service provider;

8) evidence that the regulations of the country and/or the country in which the third party operates allow the National Bank of Serbia to perform unhindered on-site supervision of operations in the part relating to the implementation of outsourced activities or in connection with them – if the third party is headquartered outside of the Republic of Serbia or it is agreed that it should perform the outsourced activities outside of the Republic of Serbia.

The deadline from paragraph 1 hereof shall run from the date of submission of duly completed documents referred to in this Section.

42. A third party may outsource to another party the activities that were outsourced to it by the service provider or other tasks connected to those activities only with the prior consent of the service provider, which shall be granted in each individual case applying accordingly the provisions of Sections 38 to 40 of this Decision.

The service provider may give the consent from paragraph 1 hereof only if it has notified the National Bank of Serbia about the intended outsourcing of activities or tasks from that paragraph at least 30 days in advance.

The notification referred to in paragraph 2 hereof shall contain in particular:

1) draft decision of the responsible body in the service provider on granting consent referred to in paragraph 1 hereof;

2) description of activities which the third party intends to outsource and the obligations and conditions which another person referred to in paragraph 1 hereof is required to fulfil;

3) basic data about another person from paragraph 1 hereof (business name, head office, registration number and TIN, and/or other relevant data for a foreign person);

4) draft contract between the third party and another party referred to in paragraph 1 hereof on the outsourcing of activities from that paragraph;

5) results of the analysis of a potential another person from paragraph 1 hereof relating to its ability to provide services, financial status and business reputation;

6) revised exit strategy whereby the service provider covered also another person from paragraph 1 hereof;

7) results of the analysis of the impact of outsourcing referred to in paragraph 1 hereof on business continuity, reputation, costs, financial result and risk profile of the service provider;

8) evidence that regulations of the country and/or the country in which another person referred to in paragraph 1 hereof operates enable the National Bank of Serbia to perform unhindered on-site supervision in the part relating to the implementation of outsourced activities or in connection with them – if that person is headquartered outside of Serbia or it is agreed that it should perform the outsourced activities outside of Serbia.

The deadline from paragraph 2 hereof shall run from the day of submission of duly completed documents referred to in this Section.

43. The service provider shall be fully responsible for the outsourced activities.

The service provider shall continuously supervise the provided services and perform quality assurance of provided services in relation to outsourced activities, especially in the part pertaining to the information-communication system security.

If it has established in the supervision procedure that the service provider, due to the omissions in the work of a third party or another person from Section 42 of this Decision, has not acted in accordance with this Decision and other regulations, the National Bank of Serbia may order the service provider to terminate the outsourcing contract concluded with the third party and take other measures in the procedure of supervision over the service provider’s operations.

44. The service provider shall submit to the National Bank of Serbia the contract referred to in Section 37, paragraph 5 of this Decision, including any annexes to the contract – within 15 days from concluding the contract and/or annex.

In the case of termination of the contract referred to in paragraph 1 hereof, the service provider shall immediately inform the National Bank of Serbia thereof.

IX. ELECTRONIC SERVICES

45. The service provider providing electronic services (hereinafter: electronic service provider) shall, as an integral part of managing the

information-communication system risk, set up a process of managing risks arising from electronic service provision.

46. In electronic service provision, the electronic service provider shall apply safe and efficient methods for verifying and confirming the identity and authorisations of persons, processes and systems.

In electronic service usage, the electronic service provider shall ensure to virtual currency users the authentication including the combination of at least two mutually independent elements for confirming user identity.

Notwithstanding paragraph 2 hereof, the electronic service provider may apply the authentication of virtual currency users which is performed by using one element for confirming user identity in case of services which were assessed, based on the risk analysis, to be low risk services.

The electronic service provider may apply the authentication of virtual currency users from paragraph 3 hereof only if it has notified the National Bank of Serbia thereof at least 30 days prior to the beginning of provision of the service from that paragraph, and submitted, together with such notification, a comprehensive and detailed analysis of risks and manner of risk management.

The deadline referred to in paragraph 4 hereof shall run from the day of submission of duly completed documents from that paragraph.

47. An electronic service provider shall adopt and apply rules which in appropriate manner, in accordance with the risk assessment and the accepted standards, limit the number of attempted log-ins to the electronic service provision system, and/or authentication attempts, determine the longest possible idle time of the virtual currency user after logging in to such system and determine the deadlines for the validity of authentication parameters.

In the use of one-off authentication passwords (e.g. One Time Password – OTP), the electronic service provider shall ensure that the time of validity of that password is limited to the period needed to perform the authentication.

The electronic service provider shall determine the greatest possible number of unsuccessful attempts of logging in to the system for electronic service provision after which the system becomes permanently or temporarily blocked, and establish procedures for safe system re-activation.

The electronic service provider shall determine the longest possible idle time of a virtual currency user on the system for electronic service provision upon logging in after which the user is automatically logged off from the system (the so-called end of session).

The electronic service provider shall ensure an appropriate confirmation of its identity on a distributive channel for electronic service provision, so that the users are able to verify the electronic service provider.

The electronic service provider shall ensure the existence of operational and system records in order to ensure, to an appropriate extent, the non-repudiation and accountability of actions relating to electronic service provision.

X. FINAL PROVISION

48. This decision shall enter into force on the eighth day following its publication in the RS Official Gazette and shall apply as of 29 June 2021.

Decision No 12
13 May 2021
B e l g r a d e

G o v e r n o r
National Bank of Serbia

Dr JorgovankaTabaković, sign.