



HNB

**GUVERNER**

Pursuant to Article 111 and Article 101, paragraph (2) of the Credit Institutions Act (Official Gazette 159/2013, 19/2015, 102/2015, 15/2018, 70/2019 and 47/2020) and Article 43, paragraph (2), item (10) of the Act on the Croatian National Bank (Official Gazette 75/2008, 54/2013 and 47/2020), the Governor of the Croatian National Bank hereby issues the

**Decision on outsourcing**

**I General provisions**

*Subject matter*

**Article 1**

This Decision prescribes in detail:

- 1) the term 'critical or important process, service or activity';
- 2) processes, services or activities that are not considered as outsourcing;
- 3) detailed conditions for outsourcing;
- 4) the content of information, form and maintenance of the register of outsourcing arrangements;
- 5) the time limit for submission to the Croatian National Bank of the notification of the intention to outsource critical or important processes, services or activities and the content of the documentation enclosed with the notification; and
- 6) rules for the management of other risks.

*Entities subject to the Decision*

**Article 2**

- (1) The provisions of this Decision shall apply to credit institutions with head offices in the Republic of Croatia that have been authorised by the Croatian National Bank.
- (2) The provisions of this Decision shall apply *mutatis mutandis* to branches of third-country credit institutions authorised by the Croatian National Bank to establish a branch of a third-country credit institution.
- (3) A credit institution shall apply the provisions of this Decision on an individual basis, taking also into account the provisions of Article 7 of this Decision.
- (4) A credit institution shall apply the provisions of Articles 6, 8 and 11 of this Decision on a consolidated basis in accordance with Title IV Scope of application of prudential requirements of the Credit Institutions Act.

*Definitions*

**Article 3**

The terms used in this Decision shall have the following meaning:

- 1) 'outsourcing' shall have the meaning as defined in Article 109, paragraph (1) of the Credit Institutions Act;
- 2) 'group of credit institutions' shall have the meaning as defined in Article 17 of the Credit Institutions Act;

- 3) '*senior management*' shall have the meaning as defined in Article 3, item (90) of the Credit Institutions Act;
- 4) '*Member State*' and '*third country*' shall have the meaning as defined in Article 13 of the Credit Institutions Act;
- 5) '*function*' means a service, process or activity;
- 6) '*service provider*' means a legal or natural person to which a credit institution entrusts the performance of a function or parts thereof;
- 7) '*sub-outsourcing*' means a situation where the service provider entrusts the performance of an outsourced function or parts thereof to another service provider (sub-contractor);
- 8) '*cloud services*' means services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction;
- 9) '*public cloud*' means cloud infrastructure available for open use by the general public;
- 10) '*private cloud*' means cloud infrastructure available for the exclusive use by a single institution;
- 11) '*common cloud*' means cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group;
- 12) '*hybrid cloud*' means cloud infrastructure that is composed of two or more distinct cloud infrastructures;
- 13) '*critical or important function*' shall have the meaning as set out in Article 5 of this Decision;
- 14) '*credit institution which is not a large credit institution*' means a credit institution which does not meet the conditions laid down in Article 4, paragraph (1), item (146) of Regulation (EU) No 575/2013 and whose four-year average assets reported in audited financial statements as at the last day of the preceding four business years on an individual basis do not exceed an amount equivalent to EUR 1 billion.

## **II Assessment of outsourcing arrangements**

### *Establishment of outsourcing*

#### **Article 4**

- (1) A credit institution shall establish whether the entrusting by a credit institution of the performance of processes, services or activities to a service provider falls under the definition of outsourcing.
- (2) For the purposes of this Decision, the following shall not be considered as outsourcing:
  - 1) services that are legally required to be performed by a service provider (e.g. statutory audit);
  - 2) market information services and services of interbank communication and trading services (e.g. services provided by Bloomberg, Moody's, Standard & Poor's, Fitch, Reuters);
  - 3) global electronic payment networks (e.g. Visa, MasterCard);
  - 4) clearing and settlement arrangements between clearing houses and settlement institutions and their members;
  - 5) global financial messaging infrastructures that are subject to oversight by relevant authorities (e.g. SWIFT);
  - 6) correspondent banking services;

- 7) non-financial services that would otherwise not be undertaken by the credit institution (e.g. advertising services, advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, transportation services, delivery services, receptionists, secretaries and switchboard operators, services of sending, receiving, transmitting and/or storing electronic documents or electronic invoices and trust services for electronic transactions referred to in Article 3, paragraph (16) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014);
  - 8) acquisition of goods (e.g. plastic cards, card readers, office supplies and furniture, personal computers); and
  - 9) acquisition of utilities (e.g. electricity, water, gas, telecommunication services).
- (3) A credit institution shall, proportionally to the nature, scale and complexity of its activities and the risks inherent in its business model, manage risks to which it is or might be exposed, which result from the entrusting of the performance of processes, services or activities to the service provider, regardless of whether that entrusting falls under the definition of outsourcing.

*Critical or important function*

**Article 5**

- (1) A credit institution shall consider the following as critical or important functions:
- 1) a function for which it is established that a defect or failure in its performance would materially impair:
    - a) its continuing compliance with the conditions of its authorisation or its other obligations laid down in:
      - i) the Credit institutions Act and regulations adopted under that Act; Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013) and regulations of the European Union adopted under that Regulation and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013);
      - ii) the Capital Market Act (Official Gazette 65/2018 and 17/2020), regulations adopted under that Act and regulations adopted under Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014);
      - iii) the Payment System Act (Official Gazette 66/2018), regulations adopted under that Act and regulations of the European Union adopted under Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015); and
      - iv) the Electronic Money Act (Official Gazette 64/2018), regulations adopted under the Electronic Money Act and regulations of the European Union adopted under Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit

and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009);

- b) performance; or
  - c) the soundness or continuity of its banking and/or financial services;
- 2) outsourcing of some control function tasks, unless the credit institution establishes that failures in outsourcing of such tasks would not have an adverse impact on the effectiveness of the control functions; and
  - 3) outsourcing of a function associated with the provision of banking and/or core financial services referred to in Article 10 of this Decision that would require authorisation by a competent authority.
- (2) For the purposes of this Decision, the outsourcing of functions necessary for the performance of activities within core business lines or critical functions referred to in Article 4, paragraph (2), items (33) and (34) of the Act on the Resolution of Credit Institutions and Investment Firms (Official Gazette 19/2015, 16/2019 and 47/2020) shall be considered as a critical or important outsourcing arrangement, unless the credit institution establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the operational continuity of the core business line or critical function.
- (3) When assessing whether a function is critical or important, a credit institution shall take into account, together with the outcome of the risk assessment referred to in Article 11 of this Decision, at least the following:
- 1) whether the outsourcing arrangement is directly connected to the provision of banking and/or core financial services which require authorisation of the competent authority;
  - 2) the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on its:
    - a) short- and long-term financial resilience and viability, including, if applicable, assets, capital, costs, funding, liquidity, profits or losses;
    - b) business continuity and operational resilience;
    - c) operational and reputational risks; and
    - d) where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation;
  - 3) the potential impact of the outsourcing arrangement on its ability to:
    - a) manage risks;
    - b) comply with regulatory and legal requirements; and
    - c) conduct appropriate audits regarding the outsourced function;
  - 4) the potential impact of the outsourced function on the services provided to clients;
  - 5) all outsourced functions, the credit institution's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;
  - 6) the size and complexity of any business area affected by outsourcing arrangements;
  - 7) the possibility that the proposed outsourcing arrangement might be scaled up without revising the underlying agreement;
  - 8) the ability to transfer the proposed outsourcing arrangement to another service provider;
  - 9) the ability to reintegrate the outsourced function into the credit institution; and
  - 10) the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the credit institution and its clients, including compliance with

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as 'Regulation (EU) 2016/679').

- (4) Before adopting a decision on the outsourcing of a critical or important function, a credit institution shall assess the potential effect of outsourcing arrangements at least on:
  - 1) the credit institution's risk profile;
  - 2) the ability of the credit institution and the competent authority to oversee the service provider and to manage the risks arising from outsourcing;
  - 3) the business continuity measures; and
  - 4) the quality of the performance of its business activities.
- (5) Where the risk, nature or scale of an outsourced function has materially changed, a credit institution shall reassess the criticality or importance of the outsourced function.

### **III Outsourcing management system**

#### *Organisational structure*

#### **Article 6**

- (1) A credit institution shall ensure:
  - 1) a clear, transparent and documented decision-making process on outsourcing;
  - 2) a clear allocation of powers and responsibilities of organisational units or employees responsible for documenting, managing and overseeing the process of entering into and implementing any outsourcing arrangements; and
  - 3) adequate resources to ensure compliance with the provisions of regulations and good practices governing outsourcing.
- (2) A credit institution shall establish an outsourcing function or designate a senior staff member (e.g. a person responsible for the work of a control function) responsible for overseeing the risks of outsourcing arrangements and overseeing the documentation of outsourcing arrangements.
- (3) By way of derogation from paragraph (2) of this Article, a credit institution which is not a large credit institution may assign the outsourcing function to a member of the management board.
- (4) When outsourcing, a credit institution shall at least ensure the following:
  - 1) the adoption and implementation of decisions related to its business activities and critical or important functions;
  - 2) the maintenance of the orderly conduct of its business and the provision of banking and financial services;
  - 3) adequate identification, assessment, management and mitigation of risks arising from outsourcing;
  - 4) where applicable, appropriate confidentiality arrangements regarding data and other information;
  - 5) the maintenance of an appropriate flow of relevant information with service providers;
  - 6) with regard to the outsourcing of critical or important functions, the undertaking of at least one of the following actions, within an appropriate time frame:
    - a) transfer of the function to alternative service providers;

- b) reintegration of the function into the credit institution; or
  - c) discontinuation of the business activities that are depending on the function; and
- 7) where personal data are processed by service providers located in the EU and/or third countries, data are processed in accordance with Regulation (EU) 2016/679.
- (5) A credit institution shall ensure that outsourcing does not result in the transfer of responsibilities from the responsible persons of the credit institution to the service provider.

*Outsourcing by a group of credit institutions*

**Article 7**

- (1) Where a credit institution outsources functions to service providers within the group of credit institutions to which it belongs, the management and the supervisory board of the credit institution that outsourced the activity or service in question shall, in line with their competence, be responsible also for those outsourced services and activities and shall retain full responsibility for compliance with all regulatory requirements and the effective implementation of this Decision.
- (2) Where a credit institution entrusts the performance of some control function tasks to a service provider within the group of credit institutions to which it belongs, for the monitoring and auditing of outsourcing arrangements, it shall ensure that those operational tasks are effectively performed, including through the receiving of appropriate reports.
- (3) Where the operational monitoring of a particular outsourcing arrangement is centralised within the group of credit institutions to which a credit institution belongs (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), the credit institution shall ensure that, at least for outsourced critical or important functions:
  - 1) both independent monitoring of the service provider and appropriate oversight is possible, including by receiving, at least annually and upon request from the centralised monitoring function of the group of credit institutions, reports that include, at least, a summary of the risk assessment and performance monitoring; and
  - 2) it is possible to receive from the centralised monitoring function of the group of credit institutions a summary of the relevant audit reports for critical or important outsourcing arrangements and, upon request, the full audit report.
- (4) A credit institution shall ensure that its management body will be duly notified of relevant planned changes regarding service providers that are monitored centrally within the group of credit institutions to which the credit institution belongs and of the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels.
- (5) Where a credit institution relies on an assessment of outsourcing arrangements, as referred to in Article 9 of this Decision, which is carried out centrally within the group of credit institutions to which the credit institution belongs, before entering into an arrangement with a service provider, it shall ensure that it receives a summary of the assessment and ensure that its specific structure and risks are taken into consideration within the decision-making process.
- (6) Where the register of all existing outsourcing arrangements is maintained centrally within the group of credit institutions to which a credit institution belongs, the credit institution shall ensure that it is able to obtain without delay its individual register, which contains all outsourcing arrangements with service providers, including outsourcing arrangements with service providers inside that group of credit institutions, at least to the extent laid down in Article 17 of this Decision.

- (7) Where a credit institution relies on an exit plan for a critical or important function that has been established for the group of credit institutions to which the credit institution belongs, it shall ensure that it receives a summary of the plan and be satisfied that the plan can be effectively executed.

*Outsourcing policy*

**Article 8**

- (1) In its policies, a credit institution shall lay down the principles, responsibilities and procedures in relation to outsourcing.
- (2) A credit institution's management board shall approve and regularly review the policies referred to in paragraph (1) of this Article.
- (3) The policies referred to in paragraph (1) of this Article shall contain at least the criteria and procedures related to:
- 1) the process of adopting decisions on outsourcing;
  - 2) the planning of outsourcing arrangements;
    - a) the definition of business requirements regarding outsourcing;
    - b) the definition of critical or important functions;
    - c) the definition, assessment and management of risks arising from outsourcing;
    - d) due diligence checks on prospective service providers;
    - e) the identification, assessment, management, mitigation or prevention of actual or potential conflicts of interest;
    - f) business continuity planning; and
    - g) the approval of new outsourcing arrangements;
  - 3) the implementation, monitoring and management of outsourcing arrangements, including:
    - a) the ongoing assessment of the service provider's performance;
    - b) the procedures for being notified and responding to changes to an outsourcing arrangement or service provider;
    - c) the independent review and audit of compliance with legal and regulatory requirements and policies; and
    - d) the renewal processes;
  - 4) the documentation and register maintenance; and
  - 5) the exit strategies and termination or cancellation processes, including a requirement for a documented exit plan for each critical or important function to be outsourced, where such an exit is considered possible taking into account possible service interruptions or the unexpected cancellation or termination of an outsourcing agreement with the service provider.

**IV Outsourcing process**

*Pre-outsourcing analysis*

**Article 9**

Before adopting a decision on any outsourcing arrangement, a credit institution shall:

- 1) assess if the outsourcing arrangement concerns a critical or important function, as set out in Article 5 of this Decision;
- 2) assess if the supervisory conditions for outsourcing set out in Article 10 of this Decision are met;
- 3) identify and assess all of the relevant risks arising from the outsourcing arrangement in accordance with Article 11 of this Decision;
- 4) undertake appropriate due diligence on the prospective service provider in accordance with Article 12 of this Decision; and
- 5) identify and assess conflicts of interest that the outsourcing may cause in line with Articles 17 and 18 of the Decision on governance arrangements.

#### Supervisory conditions for outsourcing

##### **Article 10**

- (1) Where a credit institution outsources a function directly connected to the provision of banking or core financial services to a service provider located in the Republic of Croatia or another Member State, one of the following conditions must be met:
  - 1) the service provider is authorised by a competent authority or entered in an appropriate register with a competent authority to perform that function; or
  - 2) the service provider is authorised to perform that function if such specific authorisation for the performance of that function is required under regulations.
- (2) Where a credit institution outsources a function directly connected to the provision of banking or core financial services to a service provider located in a third country, the following conditions must be met:
  - 1) the service provider is authorised or entered in an appropriate register with a competent authority to perform that function in the third country and is supervised by a relevant competent authority; and
  - 2) there is an appropriate cooperation agreement between the Croatian National Bank and the supervisory authority responsible for the supervision of the third-country service provider.
- (3) Regardless of outsourced functions, a credit institution shall maintain at all times sufficient substance and shall ensure that:
  - 1) it meets all the conditions of its authorisation at all times;
  - 2) its management and supervisory boards effectively carry out their responsibilities;
  - 3) it retains a clear and transparent organisational framework and structure that enables it to ensure compliance with prescribed requirements;
  - 4) where operational tasks of control functions are outsourced, it monitors and manages the risks arising from the outsourcing of critical or important functions; and
  - 5) it has sufficient resources to ensure compliance with items (1) to (4) of this paragraph.

#### *Assessment and management of risks arising from outsourcing*

##### **Article 11**

- (1) Before entering into an arrangement with a service provider and during ongoing monitoring of the service provider's performance, a credit institution shall assess risks and establish an appropriate system for managing operational and concentration risks and other risks arising from outsourcing.



- (2) Where the arrangement with a service provider includes the possibility that the service provider sub-outsources critical or important functions to other service providers, a credit institution shall when carrying out the risk assessment take into account at least the following:
  - 1) the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider; and
  - 2) the risk that long and complex chains of sub-outsourcing reduce the ability of the credit institution to oversee the outsourced critical or important function and the ability of the Croatian National Bank to effectively supervise them.
- (3) Before entering into outsourcing arrangements, a credit institution shall assess the potential impact of outsourcing arrangements on its operational risk and take into account the assessment results when deciding if the function should be outsourced to a service provider.
- (4) A credit institution shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.
- (5) Rules for the establishment and implementation of a risk management system in terms of the Credit Institutions Act and regulations adopted under that Act shall apply *mutatis mutandis* to the management of risks arising from outsourcing.
- (6) Outsourced functions must be adequately covered by a credit institution's internal control system. Rules for the establishment and implementation of the internal control system and control functions in terms of the Credit Institutions Act and regulations adopted under that Act shall apply *mutatis mutandis* to outsourced functions.

#### *Due diligence*

#### **Article 12**

- (1) Before entering into outsourcing arrangements and taking into account the assessment of operational risks related to the function to be outsourced, a credit institution shall ensure in its selection and assessment process that the service provider is suitable.
- (2) When assessing the suitability of an outsourcing service provider of a critical or important function, a credit institution shall assess whether the service provider:
  - 1) is of good repute;
  - 2) has appropriate abilities, the expertise, the resources(e.g. human, IT, financial), the organisational structure; and
  - 3) if applicable, has the authorisation to perform that function or is entered in an appropriate register with a competent authority.
- (3) When conducting due diligence on a prospective outsourcing service provider of a critical or important function, a credit institution shall also consider the following:
  - 1) the business model of the service provider, its nature, scale, complexity, financial situation, ownership structure and, where the service provider is a member of a group, the structure of the group to which it belongs;
  - 2) the long-term relationships with service providers that have already been assessed and perform services for the credit institution;
  - 3) whether the service provider is a parent undertaking or subsidiary of the credit institution and whether it is part of the accounting scope of consolidation; and
  - 4) whether or not the service provider is supervised by the competent supervisory authority.

- (4) Where outsourcing involves the processing of personal or confidential data, a credit institution shall verify that the service provider implements appropriate technical and organisational measures to protect the data.

*Contractual relationship between a credit institution and a service provider*

**Article 13**

- (1) When entering into an arrangement with a service provider, a credit institution shall ensure that the scope and content of the contractual provisions are adequate to the risks associated with outsourcing and to the scope and complexity of outsourced functions.
- (2) A credit institution shall enter into a written agreement with a service provider which shall contain at least the following:
- 1) a detailed description of the outsourced function which is the subject of the agreement;
  - 2) the start date and end date of meeting the contractual obligations;
  - 3) the parties' financial obligations;
  - 4) the provisions governing the manner in which a credit institution continuously monitors the performance of the function which is the subject of the agreement, including the types of reports to be received by the credit institution from the service provider and the frequency of their delivery;
  - 5) the obligation of the service provider to notify the credit institution in a timely manner of all facts and changes in the circumstances that have, or might have, a significant influence on meeting the contractual obligations;
  - 6) the agreed service level and quality of the performed functions, including the qualitative and, where applicable, quantitative performance targets for the outsourced function that allow for timely corrective action by the credit institution;
  - 7) where appropriate, the obligation of banking and business secrecy and the obligation and manner of protecting confidential and personal data, including provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;
  - 8) where relevant, the location(s) where the outsourced function will be provided and where relevant data will be kept, processed and stored, including a requirement to notify the credit institution if the service provider proposes to change the location(s);
  - 9) provisions on whether the sub-outsourcing of the function is permitted;
  - 10) the obligation of the service provider to provide the services in such a way that it fully complies with the existing regulations of the Republic of Croatia;
  - 11) the obligation of the service provider to ensure access and on-site inspection rights to the Croatian National Bank in the manner laid down in Article 15, paragraph (1) of this Decision;
  - 12) provisions that ensure that the data that are owned by the credit institution can be accessed in the case of dissolution or discontinuation of business operations of the service provider (e.g. bankruptcy, resolution, winding up or similar proceedings);
  - 13) provisions on the powers of the resolution authority under Articles 89 and 92 of the Act on the Resolution of Credit Institutions and Investment Firms and the powers of the resolution authority which have been delegated to a relevant authority under Articles 68 and 71 of Directive 2014/59/EU, with regard to contractual obligations of the credit institution;
  - 14) provisions on whether the service provider should take a professional indemnity insurance policy and, if applicable, the level of insurance cover requested;

- 15) the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the credit institution;
  - 16) the duration of the contractual relationship or an indication that the agreement is of indefinite duration;
  - 17) a description of the conditions for the termination and/or cancellation of the agreement with defined notice periods for the credit institution and for the service provider;
  - 18) the rights of the credit institution to terminate or cancel an agreement with the service provider, if so ordered by the Croatian National Bank;
  - 19) the selection of the applicable law; and
  - 20) the method of dispute settlement.
- (3) Where a credit institution and the service provider enter into an outsourcing agreement for critical or important functions, the agreement must, in addition to the content specified in paragraph (2), contain the following:
- 1) the obligation of the service provider to ensure access and audit rights to the credit institution in the manner laid down in Article 15, paragraph (2) of this Decision;
  - 2) provisions on the implementation and testing of business contingency plans;
  - 3) the obligations of the service provider in the case of a transfer of the outsourced function to another service provider or back to the credit institution, including the obligations regarding the treatment of data;
  - 4) setting of an appropriate transition period, during which the service provider, after the termination or cancellation of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and
  - 5) the obligation of the service provider to support the credit institution in the orderly transfer or reintegration of the function in the event of the cancellation or termination of the outsourcing agreement.
- (4) Where an outsourcing agreement for critical or important functions includes the possibility of sub-outsourcing, in addition to the content specified in paragraphs (2) and (3) of this Article, that agreement must contain at least the following:
- 1) the obligation of the service provider to notify the credit institution of any planned sub-outsourcing, or material changes thereof, within the period that would allow the credit institution to carry out a risk assessment of the proposed changes and, where necessary, to object in a timely manner to planned sub-outsourcing, or material changes thereof;
  - 2) the right to cancel/terminate the agreement where the sub-outsourcing increases the risks for the credit institution or where the service provider sub-outsources without notifying the credit institution and in other justified cases;
  - 3) where the sub-outsourcing involves the processing of personal data, the obligation of the service provider to obtain written authorisation of the credit institution referred to in Article 28 of Regulation (EU) 2016/679;
  - 4) the obligation of the service provider to oversee those services that it has sub-contracted;
  - 5) the conditions to be complied with in the case of sub-outsourcing;
  - 6) the types of functions that may not be sub-outsourced;

- 7) the obligation of the service provider to request written approval of the credit institution for any planned sub-outsourcing, or material changes thereof or the right to object to planned outsourcing; and
- 8) the obligation of the service provider to negotiate with the sub-contractor on access and audit or on-site inspection rights in the manner laid down in Article 15, paragraph (1) of this Decision.
- (5) A credit institution may permit sub-outsourcing only where the sub-contractor undertakes to act in compliance with applicable law and regulatory requirements, comply with relevant contractual obligations and ensure to the credit institution and the Croatian National Bank the same access and audit or on-site inspection rights as those granted by the service provider in accordance with Article 15 of this Decision.

*Security of data and systems*

**Article 14**

- (1) A credit institution shall ensure that service providers, where relevant, comply with appropriate IT security standards.
- (2) In the case of outsourcing to cloud service providers or other ICT outsourcing, a credit institution shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.
- (3) Before entering into an arrangement with cloud service providers or other arrangements that involve the handling or transfer of personal or confidential data, a credit institution shall assess the risks associated with data storage and data processing location(s) (i.e. country or region) and ensure that those risks are within acceptable limits.
- (4) When outsourcing, in particular to third countries, a credit institution shall take into account differences in national provisions regarding the protection of data.

*Access and audit or on-site inspection rights*

**Article 15**

- (1) A credit institution shall ensure within the outsourcing agreement with the service provider that the service provider ensures the following to the Croatian National Bank or any persons appointed by the Croatian National Bank for that purpose:
  - 1) timely and full access to business premises, including devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors; and
  - 2) the carrying out of on-site inspections of a part of the service provider's operation that relates or can be related to outsourcing, as well as on-site inspections of the performance of the functions which are the subject of the agreement with the service provider, to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.
- (2) With regard to the outsourcing of critical or important functions, a credit institution shall ensure within the outsourcing agreement with the service provider that the service provider ensures the following to the credit institution, its external auditors and other persons it appoints for that purpose and resolution authorities designated under the regulations governing the resolution of credit institutions:
  - 1) timely and full access to business premises, including devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors; and

- 2) the carrying out of audits or reviews of a part of the service provider's operation that relates or can be related to outsourcing, as well as reviews of the performance of the outsourced functions which are the subject of the agreement with the service provider, to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.
- (3) A credit institution shall ensure within the outsourcing agreement with the service provider that its internal audit function is able to review the outsourced function using a risk-based approach.
- (4) A credit institution shall exercise its access and audit rights referred to in this Article and determine the audit frequency and areas to be audited on a risk-based approach.
- (5) For the purpose of carrying out audits and reviews referred to in paragraph (2), item (2) of this Article, a credit institution may use:
  - 1) pooled audits organised jointly with other clients of the same service provider, and carried out by the credit institution and these clients or by a third party appointed by them; and
  - 2) third-party certifications and third-party or internal audit reports, made available by the service provider.
- (6) For the outsourcing of critical or important functions, a credit institution shall assess whether third-party certifications and reports as referred to in paragraph (5), item (2) of this Article are adequate and sufficient for the carrying out of appropriate audits and reviews of outsourcing arrangements and shall not rely solely on these reports over time.
- (7) Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, a credit institution shall verify:
  - 1) whether the persons referred to in paragraph (5) of this Article who carry out the audit and/or assessment have appropriate and relevant skills and knowledge to carry out relevant audits and/or assessments effectively; and
  - 2) whether the staff of the credit institution reviewing certifications and/or reports by the persons referred to in paragraph (5) of this Article have appropriate and relevant skills and knowledge to carry out relevant audits and/or reviews effectively.

#### *Exit strategies*

#### **Article 16**

- (1) In line with its outsourcing policy referred to in Article 8 of this Decision and business continuity plans referred to in Articles 38, 69, 70 and 71 of the Decision on governance arrangements, a credit institution shall for each critical or important outsourcing arrangement have a defined and documented exit strategy, taking into account at least the following possibilities:
  - 1) the cancellation or termination of outsourcing arrangements;
  - 2) the failure of the service provider;
  - 3) the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function; and
  - 4) material risks arising for the appropriate and continuous application of the function.
- (2) A credit institution shall ensure that it is able to cancel or terminate outsourcing arrangements with service providers without undue disruption to its business activities, without limiting its compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients.
- (3) To achieve the conditions referred to in paragraph (2) of this Article, a credit institution shall:

- 1) develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and
  - 2) identify alternative solutions and develop transition plans to enable the credit institution to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the credit institution or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.
- (4) When developing exit strategies, a credit institution shall:
- 1) define the objectives of the exit strategy;
  - 2) perform a business impact analysis that is commensurate with the risk of the outsourced functions, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;
  - 3) assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;
  - 4) where applicable, define success criteria for the transition of outsourced functions and data; and
  - 5) define the indicators to be used for the monitoring of the outsourcing arrangement with the service provider, including indicators based on unacceptable service levels that should trigger the exit.

## **V Maintenance of the register of outsourcing arrangements**

### *Documentation on outsourcing arrangements*

#### **Article 17**

- (1) A credit institution shall maintain and regularly update a register of all outsourcing arrangements, which shall contain the following information:
- 1) a reference number for each outsourcing arrangement with the service provider;
  - 2) the date of entering into an agreement and the date of application of the agreement where it differs from the date of entering into an agreement and, as applicable, the next contract renewal date, the end date of the contractual relationship and, where applicable, notice periods for the credit institution and for the service provider;
  - 3) a brief description of the outsourced function, including the data that are outsourced and whether or not personal data have been transferred or if their processing is outsourced to a service provider;
  - 4) a category of the outsourced function (e.g. information technology (IT), control function, etc.);
  - 5) the name of the service provider, its number in the relevant register (e.g. the business entity registration number (MBS), the legal entity identifier (LEI), where available), the head office address and other relevant contact details, and the name of its parent undertaking (if any);
  - 6) the country or countries where the service is to be performed, including the location (i.e. country or region) of the data;
  - 7) whether or not (yes/no) the outsourced function is considered critical or important and a summary of the assessment referred to in Article 9 of this Decision;

- 8) in the case of outsourcing to a cloud service provider, the cloud service and deployment models (i.e. public, private, community or hybrid), the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;
  - 9) the date of the most recent assessment of the criticality or importance of the outsourced function.
- (2) For the outsourcing of critical or important functions, in addition to the information referred to in paragraph (1) of this Article, the register shall contain at least the following additional information:
- 1) where applicable, the institutions and other firms within the scope of the prudential consolidation that make use of the outsourcing;
  - 2) whether or not the service provider or sub-contractor is part of the group within the scope of the prudential consolidation of which the credit institution is a member or is owned by that credit institution or another firm within the group;
  - 3) the date of the most recent risk assessment referred to in Article 11 of this Decision and a brief summary of the main results;
  - 4) the individual or body in the credit institution that approved the outsourcing arrangement;
  - 5) the applicable law;
  - 6) the dates of the most recent and next scheduled audits and reviews;
  - 7) where applicable, the names of any sub-contractors to which material parts of an outsourced function are sub-outsourced, including the country where the sub-contractors have their head office or domicile, the country where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;
  - 8) an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the credit institution or the impact of discontinuing the critical or important function;
  - 9) depending on the outcome of the assessment referred to in item (8) of this paragraph, identification of alternative service providers;
  - 10) whether the outsourced critical or important function supports business operations that are time-critical;
  - 11) the estimated annual budget cost.
- (3) A credit institution shall submit a register of all outsourcing arrangements as at 31 December of the previous calendar year to the Croatian National Bank by 31 January of the current year at the latest.
- (4) A credit institution shall without delay notify the Croatian National Bank of material changes and/or severe events regarding its outsourcing arrangements that could have a material impact on the operation of the credit institution.
- (5) A credit institution shall appropriately document the assessments referred to in Article 9 of this Decision and the results of the ongoing monitoring of outsourcing arrangements (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).
- (6) A credit institution shall without delay notify the Croatian National Bank where, based on the ongoing monitoring of outsourcing arrangements referred to in paragraph (5) of this Article, it establishes that the risk, nature or scale of an outsourced critical or important function has changed and/or where an outsourced function has become critical or important and shall enclose with that notification a summary of the risk assessment and a brief description of changes of the outsourced function.



## **VI Notification to the Croatian National Bank**

### *Notification of the outsourcing of a critical or important function*

#### **Article 18**

- (1) A credit institution which intends to outsource a critical or important function as set out in Article 5 of this Decision shall, within a reasonable time frame, but no later than 30 days before entering into an arrangement with a service provider, notify the Croatian National Bank thereof.
- (2) The notification referred to in paragraph (1) of this Article must contain an explanation comprising a description of critical or important functions to be outsourced and the reasons for adopting a decision on outsourcing.
- (3) The notification referred to in paragraph (1) of this Article shall be accompanied by the information referred to in Article 17, paragraphs (1) and (2) of this Decision that shall be contained in the register after entering into an outsourcing arrangement.
- (4) Where a service provider has its head office and/or operates in third countries, a credit institution shall submit evidence that the regulations of a country or countries in which the service provider operates enable the Croatian National Bank:
  - 1) in order to reach the objectives of supervision, to carry out an on-site inspection of a part of the service provider's operation that relates or can be related to outsourcing, as well as an on-site inspection of the functions which are the subject of the agreement; and
  - 2) to have timely and full access to the documentation and data related to outsourcing which are in the possession of the service provider.
- (5) In addition to the information referred to in paragraphs (3) and (4) of this Article, the Croatian National Bank may request any additional information that it deems necessary for the assessment whether the conditions for outsourcing laid down in the Credit Institutions Act and this Decision have been met.

## **VII Transitional and final provisions**

### *Entry into force and application*

#### **Article 19**

- (1) A credit institution shall bring into compliance its internal bylaws with this Decision by 31 December 2020 at the latest.
- (2) When first amending existing arrangements with service providers and by 31 December 2021 at the latest, a credit institution shall review and, where necessary, amend existing outsourcing arrangements with a view to ensuring their compliance with this Decision.
- (3) By way of derogation from paragraph (2) of this Article, where a credit institution cannot amend arrangements with service providers on the outsourcing of critical or important functions by 31 December 2021, it shall notify the Croatian National Bank in a timely manner and by 30 June 2021 at the latest of the measures planned to complete the review or the possible exit strategy.
- (4) A credit institution shall complete the register of outsourcing arrangements with information on all existing outsourcing arrangements in accordance with this Decision by 31 December 2021 at the latest.





HNB

- (5) By way of derogation from paragraph (4) of this Article, a credit institution shall on the date of the entry into force of this Decision enter into the register all outsourcing arrangements with cloud service providers.
- (6) By way of derogation from Article 17, paragraph (3) of this Decision, a credit institution shall, by 30 June 2021 at the latest, submit to the Croatian National Bank a register of all outsourcing arrangements as at 31 December 2020 that have been entered into from the date of the entry into force of this Decision.
- (7) On the date of the entry into force of this Decision, the Decision on outsourcing (Official Gazette 1/2009, 75/2009, 2/2010 and 159/2013) shall cease to have effect.
- (8) This Decision shall be published in the Official Gazette and shall enter into force on the eighth day after the day of its publication in the Official Gazette, with the exception of the provision of Article 10, paragraph (2), item (2) of this Decision, which shall enter into force on 31 December 2021.

No.: 311-020/10-20/BV  
Zagreb, 12 October 2020

Croatian National Bank  
Governor  
**Boris Vujčić**