OTP banka d.d. and OTP Group Slovenija Compliance and Anti - Corruption Policy

otpbanka

TABLE OF CONTENT

1. Introductory provisions 4
2. General provisions of Compliance Risk Management 5
2.1. Legal basis 5
2.2. Group-wide implementation 5
2.3. Definition of Compliance risk 6
2.4. Relevant compliance risk areas 6
2.5. Roles and Responsibilities 6
2.5.1. Bank management body, senior management, key function holders and other Bank management 6
2.5.2. Management body of the Bank and Banking group 7
2.5.3. Second, third and fourth management level and key function holders 8
2.5.4. Control role of stakeholders in ensuring compliance in the Bank`s processes 8
2.5.5. All employees 9
2.5.6. Compliance function (Organisation, principles, mandate and activities of compliance) 9
2.5.6.1. Bank`s Compliance office 9
2.6. Communication of compliance culture and integrity / compliance awareness ... 11
2.7. Cooperation of the Compliance function with other Internal Control functions and the Legal function 11
2.8. Reporting lines 12
3. Key Compliance areas managed by the Compliance Office 12
3.1.1. Personal data 12
3.1.2. Business secret 13
3.1.3. Classified information 13
3.1.4. Public information 13
3.1.5. Data protection 13
3.2. Regulatory compliance 13
3.3. Ethics and Integrity Compliance (Anti-corruption, conflict of interest management and reputation risk) 15
3.3.1. Giving / acceptance of gifts, business meals, entertainment and sponsored travel 15
3.3.2. Donations and sponsorships 16
3.3.3. Prohibition of funding political parties and election campaigns 16
3.3.4. Prohibition of indirect payments 17
3.3.5. Prohibited and facilitation payments 17
3.3.6. Mergers and acquisitions/joint ventures/acquisitions of minority interests 18

3.3.7. Procurement 18
3.3.8. Maintenance of books of account of business transactions 18
3.3.9. Recruitment and traineeship 19
3.3.10. Reputation management 19
3.4. ESG Compliance area 19
3.5. Corporate compliance and Fit & Proper 20
3.6. Financial instruments market and custody 21
3.7. Tax compliance (FATCA, CRS and DAC6) 23
3.8. Customer protection and anti - trust 24
3.8.1. Fair treatment of customers, consumer protection 24
3.8.2. Anti-trust 25
3.9. Compliance of product development and monitoring and license Compliance 27
3.9.1. Compliance of product development and monitoring 27
3.9.2. License Compliance 27
3.10. Management of prohibited behaviour 28
3.10.1. Prohibited behaviour management strategy / programme 29
3.10.2. Prohibited behaviour triangle 30
3.10.3. Law enforcement authorities and courts 30

1. Introductory provisions

OTP banka d.d. (here and after: the Bank) ensures the Banking Group's statutory and internal regulatory compliance, as well as the identification and management of compliance risks in accordance with legislative provisions, the guidelines of the international and European financial supervisory authorities and the OTP Bank Nyrt and their subsidiaries (here and after: OTP Group's) standards.

The Banking group and its operations are threatened by many threats arising from both the external and the internal environment, including compliance and integrity threats. The level and nature of threats change over time, and new threats arise as the Bank and the environment continue to develop and change. The likelihood that a threat will be fulfilled, including the potential harm caused by it, depends on the risks to which the Bank is exposed.

The purpose of this Policy is to determine the main direction of the independent compliance activity, which together define, foster and support compliant, legal, safe and prudent operation. The Compliance Policy defines the relevant compliance and integrity requirements, which the Bank has to consider in taking and managing compliance risks and sets the bases for achieving its objectives.

Integrity and reputation are key assets of the Banking group

The main goal of the Policy is to protect the fundamental values, integrity, ethics and reputation of the bank and its group. The Banking group achieves this goal through quality and efficient taking and management of all risks that may endanger its reputation, cause financial damage, lead to legal or regulatory sanctions or affect its employees, customers, service providers, suppliers, shareholders and any other stakeholders cooperating or wishing to cooperate with the Banking group.

The Policy is based on a series of legal regulations, decisions, resolutions, codes, recommendations, positions, good practices and OTP group standards.

The Management Body shall lead by example ("Tone at the Top principle")

The Management Body shall lead by example and shall adopt relevant actions to ensure that all business activities are compliant with applicable laws, requirements of the supervisory bodies (the Bank of Slovenia, the European Central Bank, the Securities Market Agency, etc.), rules and regulations (internal, external and OTP Group standards), arrangements, prescribed practices or ethical standards as set out in the Code of Conduct.

The management body shall be responsible for supervising the implementation of this Policy and shall ensure that all management levels, with the assistance of independent compliance function holders, competently and effectively provide for the compliance and integrity of the Bank's operations.

All staff must observe and comply with the Policy

The Policy must be complied with by all employees as well as the management body of the Banking group. It must be implemented in an agreed manner and in accordance with business, legislative and regulatory requirements.

The compliance function is a control function

The Banking group sets up and maintains an internal control system that ensures, among others, compliance, and integrity of the Banking group's operations. The compliance function is the function of compliance risk management and is part of the internal control system in the Banking group. The independent function manages compliance risk by regularly monitoring, rating, acting on and reporting on compliance risk.

2. General provisions of Compliance Risk Management

2.1. Legal basis

The main laws and regulations referred to in this Policy are:

- Banking Act (ZBan-3);
- Regulation on Internal Governance Arrangements, the Management body and the Internal Capital Adequacy Assessment Process for Banks and Savings banks;
- EBA Guidelines on internal governance under Directive 2013/36/EU;
- Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (hereinafter: GDPR);
- Directive No. 2014/65/EU of the European Parliament and the Council on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (hereinafter: MiFID2) and Regulation No. 600/2014/EU on markets in financial instruments and amending Regulation 648/2012/EU (hereinafter: MiFIR).

2.2. Group-wide implementation

The Bank is an OTP Group member. To this end, the Bank`s Compliance office shall in accordance with the instructions of OTP Bank Nyrt:

- implement relevant Compliance Internal acts and OTP Group Minimal Standards by ensuring compliance of its operations with the regulations, standards, and requirements and expectations of its regulator,
- assess semi-annually an OTP Group compliance risk assessment (CORIS) for the OTP Group purposes, and
- reports to the OTP Bank Nyrt regarding Compliance risks and Compliance activities.

Banking Group members shall appropriately implement this Policy by considering special regulations applicable to respective Banking Group members and their size, structural organization and extent and complexity of risks arising from the Banking Group member's business model and organization. The designated GCA (Group Compliance Assistant) of the Banking Group member shall report on the implementation of the Policy to the Bank's Compliance Office. The Bank's Compliance office maintains the register on internal acts relevant for Banking Group Members and the deadline for implementation.

Compliance Policy has been implemented with the Compliance Programme and the Compliance monitoring programme.

2.3. Definition of Compliance risk

Compliance risk is the potential legal / regulatory risk, the risk of supervisory or other official sanctions, of significant financial losses, or of reputational damage due to a failure to adhere to legislation or other non-legislative standards and internal rules applicable to the financial organisation and pertaining to its service activities.

Compliance risk means the existing or anticipated risk of loss arising of income, capital and reputation of the Bank due to violations or non-compliance with applicable laws, requirements of the supervisory bodies (the Bank of Slovenia, the European Central Bank, the Securities Market Agency, etc.), rules and regulations (both internal and external), arrangements, prescribed practices or ethical standards as set out in the Code of Conduct.

2.4. Relevant compliance risk areas

On the basis of generally accepted standards and good practices, this Policy outlines the requirements and guidelines for the management of the following relevant areas of Compliance Office that represent a higher level of compliance risk for the Bank (compliance risk areas):

- regulatory compliance
- Ethics and Integrity Compliance (Anti-corruption, conflict of interest management, procurement and reputation risk)
- corporate compliance risk (fit & proper, etc.)
- data protection
- consumer protection and anti-trust compliance
- product development, monitoring and licencing compliance
- markets in financial instruments
- FATCA, CRS and DAC6 and
- prohibited behaviour of employees
- ESG Compliance

Information security risk, risk of external fraud, AML/CFT and Sanctions risk are governed and defined by other policies of the bank / group and managed by other organizational units.

2.5. Roles and Responsibilities

A clear definition of the roles and responsibilities is key to effective implementation of the Compliance Policy on the one hand and to ensuring compliance in practice on the other.

2.5.1. Bank management body, senior management, key function holders and other Bank management

At the first line of defence, potential compliance risks are monitored, analysed and assessed by compliance risk owners, i.e. the Management Board, senior management and key function holders, and other employees responsible for lines of work relevant to the compliance risk assessment (these are determined by the Compliance Office in each assessment period).

To this end, the latter:

- shall assess once a year a compliance risk assessment for their respective area in accordance with the Compliance Risk Methodology[1], which shall be submitted to the Compliance office, and
- upon identifying increased compliance risk (in the event of product development or changes, legislative changes, etc.) or a compliance-related incident (hereinafter: incident or non-compliance), shall immediately inform the Compliance office thereof. An action plan shall be drawn up in relation to the identified compliance risk or incident (in cooperation with the Compliance office if needed or based on its recommendations) and the necessary actions taken, aimed at managing and minimizing the identified compliance risk, of which the Compliance office shall be informed. The Compliance office also monitors the implementation of the issued recommendations on the basis of proposed evidence in line with the Compliance programme and the Compliance monitoring programme.

2.5.2. Management body of the Bank and Banking group

The Management Body shall define and authorise the persons or organisational units in charge of independent management of individual compliance or integrity areas within the Bank and the Banking Group and the related processes.

The Management Body shall ensure that the compliance function has the appropriate authorisations and influence to carry out this independent function as well as sufficient human and financial resources for effective compliance risk identification. To this end, the appropriate communication channels shall be provided for, based on which all employees of the Bank and Banking Group at all levels may be informed of and familiarised with the requirements, which in terms of risk compliance and ensuring compliance relate to their field of work, their powers and responsibilities, especially in the case of identifying a violation of the Compliance Policy and requirements.

Furthermore, in order to provide for an independent compliance risk identification in the Bank and Banking group, the Management Body shall ensure that the Compliance Office shall perform and coordinate its tasks and activities on its own initiative, including investigations of possible violations of the Compliance Policy and other internal acts, without the Compliance Office employees being exposed to any attempts of undue influence or pressure exerted by the members of the Management body or senior management so as to impair the independence of the Compliance Office. The Management Body shall be responsible for effective management and supervision of the compliance risk management system.

To ensure compliance with the applicable legal and implementing regulations and effectiveness of the compliance function, the Management Body shall provide for consistent and timely consideration of all submitted reports, findings and proposed measures of the Compliance Office; in addition, the Management Body shall require that senior management appropriately eliminate any identified irregularities within the agreed deadlines. Failure to comply with the recommendations of the Compliance Office and any delays in the elimination of the identified irregularities with respect to the agreed deadlines shall be justified in writing by the recipient of the recommendations.

[1] Compliance Management Methodology relates only to the risks managed by the Compliance Office. In this way, the risks of money laundering and terrorist financing, true and fair accounting, information security, etc. are excluded, as these risks are managed by other OUs of the Bank.

The Management Board shall adopt and approve the reports of the Compliance Office. Moreover, the Management Board shall appoint and dismiss the head of the compliance function (i.e. the Director of Compliance Office) and shall previously notify the Supervisory Board thereof.

The Management Board shall appoint and dismiss the GCA, who is obliged to monitor, analyse, and assess compliance risk at the level of the Banking Group level, and shall notify the Supervisory Board previously thereof.

2.5.3. Second, third and fourth management level and key function holders

The second (B-1) and third management levels and Key Function holders' owners shall be in charge of compliance risk management within their respective unit/business line with the assistance of independent compliance function holders.

The second, third and fourth management levels shall be in charge of implementing the Compliance Policy in the context of the work areas and processes they manage and shall ensure that their subordinates implement this Policy.[2]

Within the scope of their powers, the third and fourth management levels shall be in charge of providing the relevant internal documents for subordinates so as to ensure Bank-wide compliance at all levels.

All management levels of the Bank shall ensure that appropriate actions are taken against any inappropriate conduct by employees in terms of compliance.

Furthermore, all management levels shall be responsible for the implementation of activities required to identify potential compliance risk within their respective fields, and in charge of adoption of activities/actions required to ensure effective compliance risk management.
All management levels shall report on the above activities and identified compliance risk to the Compliance office and, where necessary, to the Management Board.

2.5.4. Control role of stakeholders in ensuring compliance in the Bank`s processes

In defining and maintaining its business processes, the Bank places particular emphasis on their compliance, i.e. on ensuring that they comply with the applicable legal regulations and regulatory requirements.

In all areas associated with business processes, particular importance is attached to unique, reliable and definite identification and authentication, including the identification of both customers and the employees conducting each business process.

All divisions, departments and other organisational units within the Bank and Banking group shall be responsible for checking the adequacy reliability and particularly the effectiveness of implementing the internal processes and procedures, including any changes, amendments and updates proposed by an individual organisational unit for the purpose of compliance risk management/prevention/elimination, as well as general adherence to external and internal

[2] SIST ISO/IEC 27001:2013 – A.18.2.2 Compliance with security policies and standards

regulations by all stakeholders. In line with this Policy, the heads of individual organization units, DCAs and GCAs are obliged to regularly report to the Compliance Office on all the events/incidents which are or may be relevant in terms of compliance risk management. Furthermore, they are obliged to immediately report about each identified compliance risk in their respective area, as well as on any measures taken, their implementation and progress in terms of managing or eliminating the identified risk.

2.5.5. All employees

Bank employees shall be responsible for ensuring compliance in their line of work, taking into account their role and level of responsibility. In particular, they shall be obligated to undergo further training so as to become more qualified for compliance and integrity risk management, and the Bank and the Banking group shall enable them to do so in accordance with the adopted policies on ethical and professional standards.

All employees are obligated to inform the Compliance Office of any identified compliance risk or non-compliance (incident) immediately after its identification.

2.5.6. Compliance function (Organisation, principles, mandate and activities of compliance)

In line with the ECB decision, Nova KBM d.d. is considered a systemically important institution. As such, in accordance with the Banking Act, it is obligated to set up an independent Compliance Office.

The Head of the OTP Bank Compliance Directorate is also the Chief Compliance Officer both at Bank and Group levels. The director of the Banks Compliance office is also the Chief Compliance Officer in the Bank.

The Compliance office holds the compliance risk control function and acts as the second line of defence in the Bank. Compliance risk responsible in respective Banking Group members are known as Group Compliance Assistant (‘GCA’).

The Compliance office (including the Data Protection officer) and GCA shall report directly to the Bank Management Board / management body of a Banking Group member and shall have functional and organizational separation from other Banking Group member functions where there is a risk of conflict of interest vis-à-vis the compliance function. The Compliance office and GCA shall have full access to any information and data they need to meet their tasks and obligations.

As set out in this Policy, carrying out its activities at Banking Group level, on the other side the OTP Bank’s Compliance Directorate is responsible for the governance and supervision of the compliance activities of Banking Group members, and for verifying the implementation and application of OTP standards for compliance.

2.5.6.1. Bank`s Compliance office

The Compliance office shall identify the compliance risks to which the Bank and Banking group is or could be exposed in its operations due to a breach of applicable regulations or

requirements of the Bank of Slovenia or the European Central Bank, or due to the breach of valid agreements, prescribed practices or ethical standards that could impact the revenue, capital or reputation of the Bank and Banking group.

To ensure the full discharge of the compliance function, the Bank enables the employee(s) of its Compliance Office – without any specific permission required, and in order to carry out their duties – to view and request duplicates of the required documents, databases and records, to request information, and to receive the appropriate level of support from the relevant domains of the organisation for the analysis of the data and information provided or to interview the relevant employees. The Bank also enables employees of the Compliance Office authorised by means of mandate letters to enter any room of the Bank in order to carry out their work. The Compliance office is authorised to be represented in all meetings that address issues relevant to compliance.

a) Principles of operating the Compliance office

The Compliance office is operated in order to create a lawful and ethical corporate culture that ensures the prudential and ethical operation of the Bank and the Banking group in the long term.

In the course of operating the Compliance office the following principles are applied:

- independence
- integrity
- operation without interference
- objectivity
- preventive and proactive approach
- risk-based approach
- proportionality
- high level of professional care and competence
- full coverage
- efficiency, rationalisation of compliance costs

b) Compliance office responsibilities

Respective organisational units, persons in charge, DCAs and all employees report to the Compliance office on assessments taken, risks identified, non-compliance incidents and findings relating to compliance of their organizational unit/business line/line of work in accordance with Section 2.8 hereof. The Compliance office shall then monitor (conduct the Compliance monitoring programme), assess, and oversee the implementation of the potential action plan drawn up and the implementation of compliance recommendation based on proposed evidence by said persons in charge. It shall also provide guidance and advice and set priorities depending on the level of the identified risk. If necessary, depending on the specific situation and the level of compliance risk, the Compliance office may delegate the tasks, define the responsibilities, appoint the person in charge and specify any other compliance risk mitigation actions.

c) Advisory role

One of the basic tasks of the Compliance office, which is also used to manage compliance risk in the Bank, is advising the management body and senior management on compliance, including the development of regulations and standards in this field.

In practice, this is implemented as follows:

- when the Bank's / subsidiaries' management body raises doubts as to the interpretation of existing external regulations and the application of the internal regulations of the Bank, the latter can ask the Compliance office to draw up an appropriate opinion;
- for the level below the management body (i.e. B-1 and below) where the areas not within the explicit powers and responsibilities of the Compliance office are discussed, the latter provides advisory assistance and support by replying to a clearly defined and concrete question posed by an employee regarding the application of regulations for which the Compliance office is competent and the applicable external regulations in their work process. In response to the question, the person in charge shall prepare an appropriate opinion.

The advisory role shall observe the delineation of roles and responsibilities between the Compliance office and other functions in the Bank.

2.6. Communication of compliance culture and integrity / compliance awareness

Building, spreading and implementing a culture of compliance and integrity within the Bank and Banking group represents a part of preventive compliance risk management. The latter is based on the principle of fairness and honesty and zero tolerance of the Bank and banking group towards prohibited behaviour.

With the aim of achieving the goal of comprehensive employee, customers and other stakeholders' awareness of the culture of compliance and integrity, the Compliance office shall provide for clear and effective communication channels and messages through which this goal shall be achieved. In doing so, the Compliance office shall cooperate with the Corporate Communication function and the HR function in terms of training / awareness activities. This aspect should be included in regular corporate communications and training activities at least once a year by addressing all employees.

2.7. Cooperation of the Compliance function with other Internal Control functions and the Legal function

Considering the size of the Bank and Banking group and complexity of its operations, other organizational units are actively involved in the activities of the Compliance office, in particular:

- Internal Audit function,
- Legal function,
- Human resource's function,
- Strategic Risk Management function and Operational Risk function
- Information Security Governance function,
- Anti-Fraud function and
- Anti-Money Laundering function.

The above organisational functions / units shall perform these tasks within the framework of their line of work and regular work assignments; however, compliance risk monitoring based

on this policy and coordination of possible measures and activities shall be carried out centrally via the Compliance function.

This Policy shall in no way interfere with the existing tasks, duties and responsibilities of other functions / organizational units within the Bank and Banking group, as evident from the organisational structure and the corresponding internal regulations of the Bank and Banking group. This Policy shall complement this structure and organisation, both substantively and operationally, by intensifying and improving cooperation between these separate functions / organizational units. The objective of such a regulation shall be to ensure efficient and reliable implementation of the Compliance function within the Bank and Banking group. Thus, the primary responsibility of each individual function / organizational units shall be to regularly monitor and ensure compliance in its line of work, i.e. its organisational unit.

These organisational units are decentralised from the Compliance function, however, are nonetheless of particular importance in terms of realising the mission of the Compliance function, which requires their active cooperation with the Compliance office or delineation of duties between themselves and the Compliance office.

2.8. Reporting lines

Basic reporting under this Policy shall be provided by the employees of Compliance Office, including the Data protection officer and by respective decentralized compliance assisstence and GCAs within the integrated compliance function system. Reporting shall be periodic and continuous, and, in certain cases, by request (ad-hoc reporting).

3. Key Compliance areas managed by the Compliance Office

Tasks concerning the compliance areas specified in this Chapter are centralized in the Compliance Office.

An important part of compliance risk management is not only their identification but also proper integration or classification of these risks in the Bank. Apart from the centralised compliance risk, other areas of the Bank are relevant as well that are not an organizational part of the Compliance Office. In these cases, the Compliance function is decentralised so that the defined lines independently manage and are held accountable for the management of compliance risks. They report any relevant events to the Compliance Office on a regular (periodic) and ad-hoc basis (upon detecting compliance risks or incidents) according to this Policy.

3.1.1. Personal data

In order to protect the privacy and dignity of individuals in accordance with the General Data Protection Regulation (GDPR), the Banking Act, and the Personal Data Protection Act, the Bank shall define personal data, sensitive personal data and the related filing systems and their classification, set relevant responsibilities, and establish an effective personal data protection system.3

[3] SIST ISO/IEC 27001:2013 – A.18.1.4 Privacy and protection of personally identifiable information

With the purpose of effectively managing the risks relating to personal data protection, the Bank designated a Data Protection Officer within the Compliance function.
Personal data are defined in detail in a stand-alone document.

By monitoring the positions stated by national and European Unit data protection authorities and the European Data Protection Board, the Bank ensures compliance with the best practices expected by the authorities.

The placement of the Data Protection Officer within the control function ensures that data protection considerations are incorporated at a high level.

3.1.2. Business secret

Pursuant to the Banking Act and the Trade Secrets Act, the Bank defined the term business secret and its classification, set the responsibilities and established an effective system for the safeguarding of business secrets.

Business secrets are defined in detail in a stand-alone document.

3.1.3. Classified information

The Bank treats and manages classified information in accordance with the Classified Information Act.

3.1.4. Public information

The Bank may publish any information it classifies or defines as public information. This shall include information intended for both the internal and external users without any restrictions. The Bank shall make public all information that falls within the scope of public information pursuant to the Public Information Access Act.

3.1.5. Data protection

The Bank shall ensure the protection of data or records, which shall include cryptographic controls[4] in line with the requirements provided by applicable legislation, relevant provisions of agreements entered into, and in accordance with the business requirements of the Bank regarding confidentiality, availability and integrity of information and material records.[5]

3.2. Regulatory compliance

[4] SIST ISO/IEC 27001:2013 – A.18.1.5 Use of cryptographic controls
[5] SIST ISO/IEC 27001:2013 – A.18.1.3 Protection of records

Compliance risk in the Bank is managed through regular monitoring and assessment of both the existing and new statutory (adoption of new laws or amendment to existing) and executive regulations that may be relevant for the operations of the Bank as a financial institution. The Compliance Office staff includes designated Regulatory Compliance Officers.

The primary objective of the Bank is its commitment to operate in compliance with applicable regulations. In order to achieve this objective, it is necessary to continuously manage compliance risk by, on the one hand, regularly monitoring all the changes and amendments to applicable legislation and, on the other hand, ensuring their implementation in internal regulations and processes of the Bank.

To this end, the Compliance Office shall in particular:

- Continuously monitor new or amended regulations and rules, and report thereon to the competent persons in the Bank as soon as possible. Via the contact addresses and previously agreed communication channel, the Compliance Office shall send to the stakeholders a notice highlighting the changes to regulations, including a hyperlink, and invite the addressees to inform the Compliance Office within defined business days whether further activities are required due to the changes/amendments, the action owner, the implementation deadline, etc. The regulatory change management process is further specified in the instructions.

Based on the previous point of this paragraph, cooperate in the compliance risk assessment with respect to applicable regulations and any changes/amendments, considering in particular the impact on Bank performance, its processes, products and other services;
Based on the previous two points of this paragraph, draw up an action plan, if necessary, to mitigate and eliminate the identified risk or make other recommendations aimed at implementing the necessary changes in the Bank (introduction of good practices);
approve internal documents at levels 1 and 2 prior to their approval by the competent body;
Analyse compliance risk by being proactively involved in examining whether the launch of new products complies with applicable regulations, standards and internal documents of the Bank.

a) External regulations

If a compliance risk is identified within the regulatory compliance monitoring process, all the actions or measures necessary to mitigate such a risk need to be adopted without undue delay. It is crucial to immediately create an action plan, which should contain the following in particular: actual state of affairs, necessary activities classified by priority along with individual deadlines for their realisation, compliance risk assessment, likelihood of breach and impact of potential breach for the Bank. Where possible within the nature of the case, the action plan shall include the target post-recovery state that serves as a dashboard for the Compliance Office.

b) Internal acts of the Bank

The Compliance Office shall examine and approve internal acts at levels 1 and 2, both in terms of legal compliance and in terms of workstream compliance, before the adoption of the document or a part of the document (in the case of amendment) by the relevant approval body. The internal act shall not be submitted for adoption and publication to the person or body in charge without the approval of the Compliance Office.

Internal acts shall be reviewed and updated as necessary case of business or legal changes or at least once a year.

Once a year, the owners of level 1 and 2 acts shall report on the status of compliance of the business function with the relevant internal regulations and legislation.

The rules and procedures of internal act management are laid down in a stand-alone document.

3.3. Ethics and Integrity Compliance (Anti-corruption, conflict of interest management and reputation risk)

The Bank is committed to following the law and other regulations and rules on combating bribery in all countries in which it operates, and prohibits all improper payments, including improper payments to public employees, employees, customers, vendors and competitors. These rules apply to all employees, members of the Bank's management body, external service providers / vendors, and individuals and entities acting on behalf of the Bank.
All acts of corruption are unacceptable.

Corruption shall mean any breach of due conduct of the employees of the Bank, as well as the conduct of persons initiating such violations or persons benefiting from it, for the purpose of undue benefit promised, offered or given directly or indirectly, or for the purpose of undue benefit demanded, accepted or expected for one's own advantage or to the advantage of any other person. The acts of corruption shall include facilitation payments, unlawful acceptance and giving of gifts, funding of political parties, illegal donations, charitable contributions and sponsorships.

The Compliance Office is the owner of and responsible for managing the risk of corruption and conflict of interest and has designated for this purpose an Ethical Compliance function.
In order to protect its reputation, ensure fairness and transparency of operations, prevent, both in fact and appearance, the private interests of employees influencing their impartial and objective performance of their duties and tasks, and to avoid damage to the Bank or its stakeholders, the Bank defined the roles and responsibilities and introduced an effective system for the management and prevention of conflict of interest and similar influences in accordance with the Integrity and Prevention of Corruption Act, the Companies Act and the Banking Act.

The Bank ensures appropriate delineation of responsibilities, duties and tasks so that no employee is able to perform mutually incompatible tasks which may give rise to conflict of interest.

With the aim of preventing conflicts of interest, the Bank limited the acceptance and giving of gifts, sponsored travel, donations and sponsorships and performing compliance due diligence of employees and suppliers.

Conflict of interest prevention and Anti – corruption risk is defined in detail in a stand-alone document.

3.3.1. Giving / acceptance of gifts, business meals, entertainment and sponsored travel

Prohibited acceptance of gifts shall be understood as the facilitation or acceptance of unlawful reward, invitation, gift or any other benefit for oneself or another party or facilitation or acceptance of an offer of such a benefit that may impact the impartiality of the gift-taker and the business relationship as a whole.

Employees are prohibited from accepting any personal discounts from business partners and service providers/vendors of the Bank if offered in relation to their work at the Bank, unless the discounts are offered to all or a greater number of Bank employees.

Bank employees are also prohibited from facilitating or accepting improper payments.
Gifts, business lunches, business dinners and hospitality play an important role in the business protocol and tradition in many countries. However, when they are given or received in an inappropriate manner, they are in violation of one or several laws. That is why the applicable legislation and policies and instructions of the Bank need to be followed.

Gifts, business lunches and dinners, hospitality and sponsored travel:

- shall not be offered or accepted with the purpose of obtaining an improper advantage or affecting an official action;
- must be allowed by the local legislation or the applicable regulations of a concrete agency or other competent body;
- shall have a nominal value and shall be appropriate in relation to the position of the recipient, the circumstances and opportunities in order to prevent creating the appearance of unfairness or inappropriateness and that neither the recipient nor any other person cannot reasonably misunderstand them as a bribe;
- shall be such that the value and frequency of previous gifts and hospitality do not create the impression of improper conduct to the same recipient;
- shall be fairly and accurately recorded in the records of the Bank.

Details on the matter are provided by a stand – alone document.

3.3.2. Donations and sponsorships

Although donations to charitable organisations are usually considered in terms of corporate social responsibility, donations to organisations with which public employees or employees of the buyer or supplier are associated raise doubts connected to corruption, especially if it involves an expectation of a favour for a favour or benefit for the Bank.

With respect to donations and charitable contributions, the following shall be assessed before making a commitment or contribution:

- the purpose of payment;
- whether the payment is being made at the request of a public employee or employee of the customer or supplier;
- whether the public employee or employee of the customer or supplier is associated with the charity organization and whether the public employee or employee of the customer or supplier takes decisions relating to the business of the Banking Group;
- whether the acquisition of business or other benefits depends, directly or indirectly, on the payment.

Details on the matter are provided by a stand – alone document.

3.3.3. Prohibition of funding political parties and election campaigns

The prohibition of funding political parties and election campaigns shall mean that it is not allowed to provide any benefits to political parties or politically exposed persons.

Illegal donations, charitable contributions and sponsorships shall mean that the benefits in the form of expenses, donations, charitable contributions and sponsorships may not be provided by circumventing the rules regarding the acceptance and giving of gifts and bribes and in relation to the benefits provided to political parties and politically exposed persons and benefits provided to political parties, election candidates and political campaigns.

3.3.4. Prohibition of indirect payments

Indirect payments through a third person are prohibited. This includes giving anything of value to a third party, if it is known that the object of a certain value will be given to a public employee or an individual in the private sector for improper purposes. Because of the risk involved in cooperating with such intermediaries, it is very important that the employees of the Bank who cooperate with external service providers/vendors follow the procedure laid down in a stand – alone document.

3.3.5. Prohibited and facilitation payments

None of the employees of the Bank and of persons acting on its behalf shall execute, offer or promise a payment (regardless of whether the payment is actually executed) or directly or indirectly give anything of value to a public employee or an individual in the private sector so as to help the Bank obtain or retain an improper business advantage regardless of whether it benefits from it or not.

Prohibited payments include in particular:

- payments to obtain an improper advantage, including the decision to select the Bank as the provider of products or services or to ensure more favourable conditions for the Bank, including the provision of confidential or protected information and data on competitors, which could provide an improper advantage to the Bank;
- payments the purpose of which is to influence the action or decision of a public employee in the performance of their official duties;
- payments the purpose of which is to influence a public employee to use their influence in order to obtain personal benefits;
- payments the purpose of which is to induce a public employee to act or refrain from acting;
- payments the purpose of which is to induce a public employee to use their influence in the government or a governmental agency in order to influence the action or decision of the government or its agency.

The Bank does not allow “small bribes”. Facilitation payments are almost always illegal in accordance with the local legislation and the applicable regulations of the competent agencies in the countries where these occur.

The only exceptions from the prohibition of making facilitation payments shall be:

- when it concerns urgent medical treatment or an emergency security situation, which requires government agencies to ensure the safety of the Bank`s employees (e.g. medical evacuation, police protection or protection against fire); or
- where there is a reasonable belief that an employee of the Bank is in imminent danger of a serious injury and there is no other reasonable possibility to provide assistance.

If an employee of the Bank carries out a facilitation payment in accordance with the above exceptions relating to security, they shall immediately notify thereof the Director of the Compliance Office and specify the circumstances, the amount, the recipient and other relevant information. The security exceptions for making facilitation payments shall be used only rarely.

When faced with an application or request for an improper payment or breach of the provisions of this Policy, this should be reported as a suspicion of prohibited behaviour.

3.3.6. Mergers and acquisitions/joint ventures/acquisitions of minority interests

Acquisitions, joint ventures, consortia and disposals of minority interests may pose a significant risk of corruption and bribery. When the Bank undertakes to perform such activities, it is important to ensure the following in consultation with a legal advisor:

- a thorough due diligence of compliance of operations and the reputation of potential acquisition or investment objective, joint venture/partners in the joint venture or consortium or partner/partners in the consortium based on risks;
- the application of the Code of Conduct, the Compliance Policy with the Anti-Corruption Policy and/or subordinate documents of Bank in the acquired entity as well as, to the extent possible, in the joint venture, the consortium or investment objective;
- training in combating corruption and ensuring that such training is held;
- planning and execution of an audit of the acquired entity, which is focused on corruption, within the shortest possible time and making every effort to carry out such a review in the event of joint ventures, consortia and purchase of a minority interest.

3.3.7. Procurement

In certain cases, the Compliance Office will carry out vendor due diligence to reduce the risk of corruption in vendor relationships. Of the Compliance Office does not sign off on a vendor relationship, the Bank shall not engage with that vendor.

Furthermore, vendors are obligated to deliver to the Bank a signed and executed copy of the Compliance Declaration.

This Section shall be executed with observance of a stand – alone document.

3.3.8. Maintenance of books of account of business transactions

The Bank shall establish and keep the books, records and accounts, which, in adequate detail, accurately and fairly reflect the nature of business transactions and assets of the Bank. Nothing shall be kept off-the-books in order to facilitate or conceal an improper payment or

for any other reason. All expenses, gifts, hospitality and any other payments shall be precisely and accurately reported and recorded. All accounting records, expense reports, invoices, gift certificates and other business records shall be accurately and fully completed and properly kept. They shall be duly reported upon and recorded. Assets, accounts or payments undisclosed or unrecorded for whatever reason shall not be made or kept. It shall be prohibited to avoid or attempt to avoid internal accounting controls of the Bank or to circumvent them.

3.3.9. Recruitment and traineeship

Public employees or employees of the Bank's business partners may sometimes ask the Bank to ensure traineeship or employment for specific individuals, or these public employees or employees themselves may request to be recruited by the Bank. Depending on the circumstances, the offer of employment or traineeship may constitute a bribe, especially if the public employee or employee of a business partner may have an influence on the business interests of the Bank. Each Bank employee shall consult the Compliance Office of the Bank when a public employee or employee of a business partner who may have an influence on the business interests of the Bank (i) asks to be considered as a candidate for employment, or (ii) asks that a person related to them be considered as a candidate for employment or traineeship.

Compliance Office carries out a Know Your Employee check of candidates before the actual employment takes place.

3.3.10. Reputation management

Reputation risk means the risk of loss arising from the negative image of the bank held by its customers, business partners, owners and investors or supervisors.

Effective risk event management acts as a means of strengthening the Bank`s reputation.
The Compliance Office monitors monthly announcements in the media and monthly clippings and analyses negative announcements, monitors customer advertising and, if necessary, issues appropriate measures that are necessary to prevent or minimize reputation risk (carrying out interviews with involved parties, involving Legal Office for the purpose of filing legal remedies, putting legal entities and natural persons, which are damaging the bank`s reputation on the stop list, etc.).

The Compliance Office keeps records of all negative announcements in the adopted measures and reports to the managing body.

3.4. ESG Compliance area

In accordance with the sustainability (ESG) criteria, the Bank assesses and evaluates its activity from the aspect of the activity's environmental impact (E), social fairness (S) and the related corporate governance issues (G) and ensures its compliance with the relevant legislative requirements.

The Bank has taken a comprehensive approach to the ESG by establishing the Climate Change & Sustainability Committee, which is responsible for the comprehensive and effective

implementation of the ESG strategy in order to manage the risks and opportunities in this area.

Among other things, the Committee decides on involvement in various initiatives, sets and monitors climate risk objectives and performance, monitors the work of the internal working group, monitors the preparation and approval of the sustainability report, adopts activity reports of relevant organizational units and reports to the Supervisory Board. The member of the Committee is the director of the Compliance Office.

Within the Committee, the Director of the Compliance Office is responsible for supervising and coordinating the Bank's activities aimed at ensuring compliance with relevant and applicable ESG requirements and regulations and supervising the implementation of the entire ESG strategy.

The ESG strategy consists of 10 pillars, one of the key ones being ensuring compliance.
The Compliance Office monitors the relevant legislation and requirements of the regulator in the field of ESG and coordinates the implementation of legislative requirements and requirements or expectations of regulators.

The Compliance Office included an ESG questionnaire in the process of due diligence of external contractors / suppliers, on the basis of which it assesses the acceptability or unacceptability of the external contractor / supplier also from the point of view of ESG risk management.

3.5. Corporate compliance and Fit & Proper

In the spirit of responsible corporate governance, the OTP bank Nyrt has guidelines in place ensuring that, as a publicly traded company, its operations comply with the internationally recognised rules and standards of responsible corporate governance, and that the public disclosure of information on its governance and operations makes it a transparent and verifiable company.

In its business practices, the Bank takes into account the interests of the OTP`s shareholders, customers and business partners on the one hand and ensuring compliance of its operations with the regulations, standards, and requirements and expectations of its regulator on the other hand.

At all times, the Bank has a governance system in place, and operates bodies and boards, which support and assist the organisation in monitoring the enforcement of customer and counterparty interests, and variations in business needs, and in adjusting its business policy and its relations with customers and business partners accordingly, by taking into account the relevant regulations, standards, and requirements and expectations of its regulator.

The Policy on the Assessment of Suitability of Members of the Management Bodies and Key Function Holders defines the selection strategy and procedural aspects for the assessment of suitability of members of the Management Board, Supervisory Board and Key Function Holders of the Bank. The Fit & Proper Policy is aligned with the Bank’s strategy, values and long-term vision, and includes criteria for the assessment of individual and collective suitability, sets out documents underlying the assessment, procedures to ensure suitability and, where applicable, the reassessment process. The Policy also outlines procedures and action in cases where the candidate is assessed as not suitable for a particular position or function.

The Compliance Office providers relevant support to the Fit & Proper Committee.

3.6. Financial instruments market and custody

The Compliance Office holds an important role in ensuring compliance in trading in financial instruments and custody.

For purposes of protecting the Bank's reputation and ensuring compliance with regulations governing financial instruments and custody, the Compliance Office monitors and assesses established processes and procedures the Bank carries out to meet statutory requirements. The Compliance Office also advises on and assists employees involved in the business line to meet statutory requirements. The Compliance Office employs a designated Financial Market Compliance function.
Bank takes all of the measures required to ensure that orders are carried out in the best interest of customers.

Per the MiFID II EU regulatory framework, the Bank is obligated to set up and maintain a permanent compliance function that operates independently and entrusted, among others, with the following tasks and responsibilities:

- Permanently monitors and regularly assesses the adequacy and effectiveness of the measures, policies, and procedures relating to investment services as well actions the Bank adopts to eliminate any weakness / compliance deficiencies in the performance of its obligations.
- Advise and assist persons responsible for investment services and activities on relevant legislation.
- Report to the Management Board at least annually on the implementation and effectiveness of the overall control landscape, the risks detected and on the reporting of complaint resolutions, as well as on actions taken or to be taken. As part of the annual reporting, the Compliance office also informs the Management Board about the product management process in the company.
- Monitor the performance of the complaint resolution process and consider complaints as a relevant source of information.
- In order to protect the clients` financial instruments, a responsible person is appointed within the Compliance office for matters related to how the bank fulfils its obligations regarding the protection of clients' assets. As part of the function, the person reviews the existing processes related to the subject area, participates in the educational process of persons providing clients with information about financial instruments and services, and participates in the implementation of new requirements as needed.

In order for the Compliance Office to ascertain that the level of compliance within the financial instruments market and custody is sufficient, a compliance monitoring program for this area shall be established. The program is based on a risk assessment carried out by the Compliance Office in accordance with a defined internal methodology.

To ensure Compliance with restrictions on information flows between financial and investment service activities the Bank puts in place an internal organisational, operational and procedural mechanism to ensure that the data and information flows among the organisational units in charge of financial services, ancillary financial services and investment services comply with the applicable legal provisions and recommendations.

The organisational units of the Bank may only disclose confidential banking and securities information to one another as provided for in the applicable internal regulation of the Bank.

Additionally, the Bank ensures that any person may only access bank secrets and securities secrets on a need-to-know basis.

Market abuse prevention actions also play a key role in ensuring compliance in the financial instruments trading line. As a prominent issuer of the Budapest Stock Exchange, the OTP Bank, in its capacity as issuer, investment service provider and credit institution, is highly committed to the maintenance of transparency and efficiency in the capital market, and to compliance with all applicable legal obligations.

Within the meaning of applicable law and of its own regulation, the Bank prohibits insider dealing and attempted insider of any financial instruments. The Bank counters all forms of inside dealing, carrying out analyses and examinations of such incidents, and taking action to prevent such incidents, or address incidents that have occurred.

The Bank counters all forms of conduct that involves a potential for market manipulation, or is inconsistent with generally accepted professional principles, or discloses unfounded, false or potentially deceptive information and gives signals of that character about the price of a specific financial instrument, or artificially keeps the price of an instrument at an abnormal level.

The Bank has undertaken a commitment to safeguard the interests of capital market participants, investors and customers, to maintain fair competition, and to prevent market abuse and conflicts of interest. To that end, it regulates the conclusion, notification and registration of any transactions by the persons concerned that are linked to investment service activities or the provision of ancillary services.

The Bank remains mindful of developing an internal regulatory environment that is suitable for preventing persons involved in activities leading to potential conflicts of interest from concluding transactions that are prohibited by the law or involve the illicit use of confidential information or would result in conflicts of interest, by having access to insider information as a result of their activity or to confidential information as a result of their relationship with customers.

The Bank has in place a system for the prevention of abuses of this type, which is defined by precise rules in statute and reporting obligations of respective employees. For purposes of mitigating the risk of market abuse, the Compliance Office maintains an internal Restricted List, which is a document, published and made available internally, comprising sensitive financial instruments issuers. Relevant persons are prohibited from trading in these instruments, as there is a potential risk of these Bank employees taking knowledge of inside information on the financial instrument issuer. Aside from the Restricted List, the Compliance Office is also the owner of the Watch list and thus further monitors transactions with potentially sensitive financial instruments.

Persons involved in trading in financial instruments shall be understood as persons who may detect or take note of any trading characteristic based on inside information or market manipulation. Whenever this type of trading is detected at the Bank, the Compliance Office shall examine an additional review and if needed report to the Securities Market Agency. The directors of the areas of investment banking, treasury and back-office services shall assist in this.

In addition, the Compliance office periodically conducts an independent review of the turnover generated in the field of trading in financial instruments in order to identify potential market abuse.

The Compliance Office regularly reports to the Bank Management Board on actions taken to ensure compliance in the financial instruments line and custody and oversees all correspondence between the Bank and the Securities Market Agency.

Representative of the Office is also a member of the Investment Product Governance Committee. The main committee's task and responsibilities are definition/review of investment products' target markets, providing protection of the clients and detection/management of potential conflict of interests from the investments point of view.

More specifically, the tasks and responsibilities of the Compliance office in the area of financial instruments operations are defined a stand – alone document.

Following the fact that NKBM is the issuer of the financial instruments, listed on MTF of Luxebourg Stock Exchange, the Bank is obliged to comply with requirements of Regulation 596/2014 (MAR). With this purpose Compliance office maintains and updates Insider list and reports the list based on the request to the ATVP. The details on the provisions in this relation are defined in a stand – alone document.

3.7. Tax compliance (FATCA, CRS and DAC6)

In order to protect the reputation of the Bank and prevent tax evasion, the Bank adheres to and implements the following:

- Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the United States of America to Improve International Tax Compliance and to Implement FATCA,
- Standard for Automatic Exchange of Financial Account Information developed by the Organisation for Economic Cooperation and Development (OECD), Council Directive 2014/107/EU, and
- tax laws (particularly the Tax Procedure Act) and DAC6 on tax avoidance and profit spill overs of a more taxable jurisdiction.

For this purpose, the Bank, as a reporting financial institution, is obligated to set up a tax compliance assurance process, which entails in particular:

- identifying of clients and beneficial holders of banking services (individuals and legal entities and their ultimate beneficial owners),
- collecting mandatory data and documentation that the Bank can determine and verify the clients' citizenship and/or tax residence,
- correctly recording collected data into the Bank's information system,
- properly managing collected data and monitoring any changes,
- identifying potentially aggressive cross-border tax planning arrangements using t.i. recognizable features that potentially indicate aggressive tax planning.

The information will be exchanged between the tax authorities automatically. The requirements regarding DAC6 have been regulated in Chapter no. 4 of Rules on the Implementation of FATCA, CRS and DAC6, Pr55.
The Bank is obliged to annually communicate the following information to the Financial Administration of the Republic of Slovenia (FURS). In this regard the Compliance office is responsible for coordinating the preparation and mediation of the reports for:

- financial accounts of tax non-residents,
- financial accounts of clients who declared as U.S. citizens or tax residents and
- potentially aggressive cross-border tax planning arrangements.

In addition to the Accounting Department, tax evasion shall be dealt with by the Compliance office. In the Compliance office, the designated Tax Compliance Officer shall be responsible for the management of this risk.

The responsibilities are defined in a stand – alone documents.

3.8. Customer protection and anti - trust

3.8.1. Fair treatment of customers, consumer protection

The Bank is committed to the enforcement of consumers' interests. In this context, it follows consumer protection principles that are consistent in their approach and takes into account changes in consumer habits and interests.

In order to ensure compliance with a dynamically changing legal environment, the Bank provides for the development and, where appropriate, redesign of products in accordance with the criteria set out in internal regulations, legal regulations, and regulatory requirements. In this regard it continuously monitors changes in national and international law, newly issued supervisory recommendations, and other requirements at the national and EU levels.

The Bank ensures the appropriate enforcement of consumer protection considerations during product development and the consumer protection and competition law compliance of all commercial communication.

The Bank shall respect and protect the rights of its customers.
In order to ensure regular and quality provision of services to its customers, the Bank shall continuously develop and increase the quality of its services. For this purpose, the Bank shall establish a customer complaint resolving procedure, the aim of which shall be to effectively resolve any customer complaint to the satisfaction of both the customer and the Bank by also including its employees.

The Bank shall respond to the customer's complaint within the statutory time limit. Complaints received, and their handling, shall be documented; resolved complaints shall applied as lessons learned to optimise the Bank's organisation, business processes and improve internal controls.

Banking Operations, the Call Centre and the Bank's front office act as the central hubs for monitoring and managing the records of customer complaints and for proactive and reactive response actions aimed at customer retention. The Compliance Office shall monitor complaints in terms of compliance risk and shall take appropriate action should an increased compliance risk or non-compliance be detected.

Prior to the launch of a new advertising campaign, the Marketing and communication unit shall notify the Compliance office thereof and deliver to it all relevant advertising material so as to check whether it complies with the applicable sector-specific legislation (e.g. the Consumer Credit Act) or the general consumer protection legislation advertising or in order to prevent any misleading (e.g. the Consumer Protection Act).

In order to strengthen consumer protection in all banking areas, the Bank adopted a Consumer Protection Policy, which identifies the most important consumer protection areas.

3.8.2. Anti-trust

By this Policy, the Bank defines in detail the prohibition of the employees' behaviour that may constitute a restriction of competition.

Any agreements (unless they are of minor importance) between banks or other financial institutions or undertakings, decisions by associations in which the Bank participates (e.g. the Bank Association of Slovenia) and concerted practices of banks or other financial institutions or undertakings (hereinafter: agreements), which have as their object or effect the prevention, restriction or distortion of competition, shall be prohibited and shall be null and void.

The prohibition shall apply in particular to:

- direct or indirect fixing of purchase or sales prices or other trading conditions;
- limiting or controlling production, sales, technical progress or investments;
- applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
- making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, no connection to the subject of their contracts;
- sharing markets or sources of supply.

The prohibition referred to in the previous paragraph shall not apply if these agreements contribute to improving the production or distribution of goods or to promoting technical and economic progress, while allowing consumers a fair share of the resulting benefit. These agreements shall not:

- impose on the undertakings involved any restrictions that are not indispensable to the attainment of these objectives, and
- confer upon these undertakings the option of eliminating the competition in respect of a substantial part of the products or services that are the subject of the agreement.

Abuse of a dominant position in the market by one or more banks or undertakings shall be prohibited. An undertaking or a bank or several undertakings or banks shall be deemed to have a dominant position when they can, to a significant degree, act independently of competitors, customers or consumers (in determining the latter, the following criteria shall be taken into consideration in particular: market share, funding options, legal or actual entry barriers, access to suppliers or the market and existing or potential competition).

The abuse of a dominant position shall constitute in particular:

- directly or indirectly imposing unfair purchase or sales prices or other unfair trading conditions;
- limiting production, markets or technical development to the prejudice of consumers;
- applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
- making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection to the subject of their contracts.

An undertaking or a bank shall be deemed to have a dominant position if its share on the market of the Republic of Slovenia exceeds the 40 percent threshold. Two or more banks or undertakings shall be deemed to have a dominant position if their share on the market of the Republic of Slovenia exceeds 60 percent.

Concentrations that would significantly impede effective competition on the territory of the Republic of Slovenia or on a substantial part of it, especially as a result of the creation or strengthening of a dominant position, shall be prohibited.

The concentration assessment criteria shall include in particular the following: market position of the undertakings or banks involved in the concentration, their financial options, market structure, alternatives available to suppliers and users, their access to sources of supply or markets, any legal or other barriers to entry, supply and demand trends for the relevant markets, the interests of intermediate and ultimate consumers and the development of technical and economic progress provided that it is to consumers' advantage and does not form an obstacle to competition.

A concentration shall be deemed to arise where a change of control on a lasting basis results from:

- the merger of two or more previously independent undertakings or banks or parts of undertakings or banks, or
- the acquisition, by one or more natural persons already controlling at least one undertaking or bank, or by one or more undertakings or banks, whether by purchase of securities or assets, by contract or by any other means, of direct or indirect control of the whole or parts of one or more other undertakings or banks, or
- the creation of a joint venture or bank by two or more independent undertakings or banks, performing on a lasting basis all the functions of an autonomous economic entity.

Control of a whole undertaking or bank or a part of it within the meaning of the preceding paragraph shall be constituted by rights, contracts or any other means that, either separately or in combination and having regard to the considerations of facts or regulations involved, confer the possibility of exercising decisive influence on such an undertaking or bank or part of undertaking or bank, in particular:
ownership or the right to use all or part of the assets of an undertaking or bank;
rights or contracts that confer a decisive influence on the composition, voting or orders of the bodies of an undertaking or bank.

Control is acquired by persons or undertakings or banks that:

- are holders of rights or entitled to rights under the contracts concerned, or
- while not being holders of such rights or entitled to rights under such contracts, have the power to exercise the rights deriving from contracts.

A concentration shall not be deemed to arise when banks or other financial institutions, the normal activities of which include transactions and dealing in securities for their own account or for the account of others, hold on a temporary basis business assets that they have acquired in an undertaking with a view to reselling them, provided that they do not exercise voting rights in respect of those business assets with a view to determining the competitive behaviour of that undertaking or provided that they exercise such voting rights only with a view to preparing the disposal of these business assets and that any such disposal takes place within one year of the date of acquisition of these business assets. The period of one year may be extended by order of the Agency by request of the undertaking where the undertaking can show that the disposal was not reasonably possible within the prescribed period.

3.9. Compliance of product development and monitoring and license Compliance

3.9.1. Compliance of product development and monitoring

In developing its products and granting access to its services, the Bank complies with the principles and standards of ethics, consumer protection, and relevant legal requirements whereby it is ensured that the services provided are modern, high-quality and fair, and meet customers' needs.

In designing its products and services, the Bank pays special attention to the enforcement of consumer protection principles, and to reducing information asymmetry between the and customers.

The terms of contracting, contract amendments, account opening and account termination are specified by the Bank in such a manner that they are consistent with the principles of compliance and risk exposure, and ensure the prudential operation of the organisation.
In the establishment and maintenance of its customer relations, the Bank has regulations in place to ensure that exposures, commitments and services are well-found and transparent, risks are assessed, assessment is controlled, and risks are mitigated.
Product Development and Segments of Retail Banking Sector is the holder of the compliance function with respect to the Bank's products, as set out in greater detail in a stand – alone document.

Should the Product Development and Segments of Retail Banking Sector identify a compliance risk in its line of work, it shall inform the Compliance Office thereof.

Prior to the launch of a new or change of a pre-existing banking product, technology, service, system, model, entry into new markets, etc., Product Development and Segments of Retail and Corporate Banking shall inform the Compliance office thereof, so that the Compliance office can actively participate in the verification whether such a launch or change complies with applicable regulations, standards and internal regulations of the Bank.

3.9.2. License Compliance

The Bank shall protect its and its stakeholders' intellectual property in accordance with legal requirements, regulations and agreements relating to intellectual property rights and the use of proprietary software products.

Intellectual property comprises copyrights, design rights, trademarks, patents and source code licenses.

In order to protect its intellectual property, the Bank shall introduce appropriate procedures and responsibilities for ensuring compliance with legal and contractual requirements and the requirements arising from other regulations which require that intellectual property protection be observed.6

[6] SIST ISO/IEC 27001:2013 – A.18.1.2 Intellectual Property Rights

Compliance office cooperates within the notification process regarding Bank`s licences to the Regulator.

3.10. Management of prohibited behaviour

With the aim of protecting the Bank's core values, integrity and reputation and preventing damage to the Bank or its stakeholders, the Bank shall define integrity and core values and set up roles, responsibilities and an effective system for ensuring core values and integrity on all business levels.

With the same aim as referred to above, the Bank shall define prohibited behaviour and introduce an effective system for the detection, prevention, management and, in particular, mitigation of prohibited behaviour. The Bank has a zero-tolerance policy towards prohibited behaviour.

The Bank set up a neutral channel that Bank employees can use to anonymously report any prohibited behaviour (whistleblowing) without being exposed to risk of retaliation or any other risk. By setting up a whistleblowing channel, the Bank encourages and promotes the detection, prevention and elimination of prohibited behaviour, and introduces a trustworthy and safe work environment that allows for unimpeded cooperation of all employees.

All Bank employees have the duty and responsibility to prevent prohibited behaviour.

Within the process of managing prohibited behaviour of employees management and prohibited behaviour-related the Compliance office is responsible for strategic planning and management of the system for the prevention of prohibited behaviour of employees, identifying and detecting suspicions of prohibited behaviour of employees, receiving reports on suspicions of prohibited behaviour of employees in accordance with provisions governing the receipt of reports, dealing with suspicions of prohibited behaviour of employees in accordance with the provisions governing the treatment of prohibited behaviour of employees, proposing measures to correct the irregularities within the framework of treatment of prohibited behaviour of employees, assessing risks of prohibited behaviour of employees and the soundness of internal controls in terms of managing prohibited behaviour of employees and making recommendations for improving internal controls, monitoring if implementation of compliance recommendation based on proposed proofs, reporting to the Management Board and other functions of the Bank, as specified in detail by relevant rulebooks, and training / communication on prohibited behaviour of employees. The Compliance office is also responsible for reporting and lodging of criminal reports and charges with competent state authorities, cooperating with competent law enforcement authorities, reporting to the Management Board and other bodies of the Bank.

The Fraud Management unit is responsible for strategic planning and fraud management, strategic planning and management of the system for the prevention of prohibited behaviour of third parties, detection and identification of prohibited behaviour of third parties, management of the automated prohibited behaviour warning system, receiving reports on suspicions of prohibited behaviour of third parties in accordance with the provisions of applicable internal acts, treatment of suspicions of prohibited behaviour of third parties in accordance with applicable internal acts, proposing measures to eliminate the irregularities within the framework of the treatment of prohibited behaviour of third parties, assessing risks of prohibited behaviour of third parties and the soundness of internal controls in terms of managing prohibited behaviour of third parties and making recommendations for improving the internal controls, reporting to the Management Board and other bodies of the Bank, training / communication on prohibited behaviour of third parties.

Prevention of prohibited behaviour is further defined by a stand – alone document.

3.10.1. Prohibited behaviour management strategy / programme

The Bank places great emphasis on the management of prohibited behaviour for purposes of optimizing risks associated with prohibited behaviour, i.e. for purposes of achieving optimal balance between losses incurred due to prohibited behaviour and costs associated with the management and prevention of prohibited behaviour.

The overarching objective is to control losses incurred due to prohibited behaviour by focusing on the prevention of said practices. With respect to prevention and management of prohibited behaviour, the Bank ensures adequacy and compliance of Bank operations by preventing violations of provisions laid down in this Policy. By acting in this manner, the Bank not only protects its reputation and financial interests, but also its employees, clients, shareholders, suppliers and vendors. On a broader scale, actions of the Bank also protect the reputation of financial centres the Bank operates in, as well as the interests of the civil society.

A permanent task with respect to the management and prevention of prohibited behaviour are preventive activities and warnings issued regarding negative consequences that may result from prohibited behaviour. Preventive activities include the system for anonymous reporting of suspicion of prohibited behaviour (whistle-blower system), system for automated detection of prohibited behaviour, and continuous raising of awareness of employees on the importance to adhere to applicable rules and regulations. Another task with respect to the management and prevention of prohibited behaviour is regular monitoring of the compliance of conduct of employees taken as part of predetermined and implemented controls, audits and standard processes, as well as the detection of violations and issuance of recommendations on remedial actions and monitoring of implementation of issued recommendation. The aforementioned measures are material to the protection of the Bank's goodwill and reputation.

As a result of preventive activities, the Bank integrates relevant controls and control points in all business processes sensitive to prohibited behaviour, so as to ensure quick detection and prevention of (attempted) prohibited behaviour.

The management of risks associated with suspected prohibited behaviour in the Bank is a material element of the Bank's strategy on the management and prevention of prohibited behaviour, and entails a detailed investigation of relevant circumstances.

Immediately after determining that prohibited behaviour occurred, the Bank shall undertake all measures necessary to terminate contractual or business relationships with natural persons and / or legal entities that either engaged in or attempted to engage in prohibited behaviour.

The Programme of management and prevention of prohibited behaviour, which is a part of Compliance Strategy / Programme and Compliance monitoring programme, as a whole entails in particular the following activities:

- Follow-up on current state of affairs (including prohibited behaviour identified, efficiency and success rate of prohibited behaviour prevention processes, current risk mitigation measures, investigations and cooperation between stakeholders, and results of the last risk assessment).
- Define key objectives – changes to be implemented during the period concerned.

- Produce action plan for implementation.

3.10.2. Prohibited behaviour triangle

The prohibited behaviour triangle is a model applied to interpret the factors of prohibited behaviour. The model can be applied to identify the risk of prohibited behaviour occurring, and to define the manner of prevention and deterrence of prohibited behaviour in the Bank.
The model consists of three components that commonly appear simultaneously and lead to prohibited behaviour:

- persons need to be encouraged or coerced into engaging in prohibited behaviour, e.g. coercion to realize financial objective, victim of intimidation, concern about job, attempt to hide an error, personal financial distress or addiction, desire for power or desire to beat the system;
- opportunity (lack of controls, inefficient controls, opportunity to evade controls, poor supervision or lack of supervision, opportunity for conspiracy);
- persons do not see themselves as perpetrators and therefore need to rationalize or justify their actions (conviction that this is common practice, job or wage dissatisfaction – “I’ll take what they owe me”, denial with regard to consequences or conviction that they will not be caught).

The management and prevention of prohibited behaviour in the Bank should affect all three components referred to above. The overarching objective is to reduce the volume of prohibited behaviour and reduce the volume of opportunities to engage in prohibited behaviour (risk).

3.10.3. Law enforcement authorities and courts

The Bank shall cooperate with law enforcement authorities in criminal complaints, investigations and prosecutions and shall provide information in line with the applicable legislation to the law enforcement authorities and courts at their request. Furthermore, the Bank shall perform the main supervision of data transmission to law enforcement authorities and courts and shall file reports and make statements.

Relations with law enforcement authorities and courts are managed by the Compliance Office.