PERSONAL DATA PROTECTION POLICY

2024

Contents

1. INTRODUCTION

Pursuant to 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 (hereinafter: **General Data Protection Regulation**), the Management Board of KentBank d.d. (hereinafter: "the **Bank**") adopted this Personal Data Protection Policy (hereinafter: "the **Policy**") at its session held on 19 March 2021.

2. PURPOSE

The protection of personal data is a fundamental human right. The Bank is aware of the importance of secure, reliable and transparent processing of personal data of its clients, employees and other natural persons whose personal data it collects and further processes.

This Policy stipulates the basic rules and principles on the basis of which the Bank processes personal data of clients, consumers, suppliers, business partners, employees and other individuals and indicates the responsibility of business units and employees when processing personal data. The Bank achieves protection of personal data primarily in the following ways:

- by adoption of this Policy,
- by adoption of additional internal acts that stipulate the processing of personal data in more detail,
- by implementing organizational and technical measures of protection of personal data,
- by keeping up-to-date the records of personal data processing activities,
- by continuously educating employees on the importance of personal data protection, and
- by designation of a personal data protection officer.

3. REFERENCE DOCUMENTS

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.

4. DEFINITIONS

The terms used in this Policy have the same meaning as in the General Data Protection Regulation. For the reasons of transparency, the most important are listed below:

‘**personal data’** means any information relating to an identified or identifiable natural person (‘**data subject’**);

„**special categories of personal data**“ - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

‘**processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘**controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; For the purpose of this Policy, the Controller is the Bank;

‘**processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

‘**recipient**’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed;

‘**personal data breach**’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

‘**supervisory authority’** means an independent public authority which is established by a Member State pursuant to Article 51 of the General Data Protection Regulation; in the Republic of Croatia it is the Personal Data Protection Agency (AZOP)

'**officer'** - data protection officer.

5. SCOPE OF APPLICATION

This Policy is the fundamental act of the Bank applicable to all personal data processing activities carried out by the Bank, which in particular include:

- processing of personal data of clients when concluding, executing and processing various agreements on loans, transaction accounts, deposits and other products of the Bank,
- processing of personal data for contacting potential employees in selection procedures before making a decision on employment, as well as of employees when concluding, executing and processing employment contracts,
- processing of personal data of natural persons engaged by the Bank on the basis of service contracts, author's contracts and similar contracts,
- processing of personal data of employees who are employed with the Bank's suppliers,
- processing of personal data of students who are on vocational professional practice at the Bank or on occasional student work,
- processing of personal data of family members of the Bank employees to the extent necessary for the implementation of legal obligations or the exercise of a legal right or a right provided for by an internal act of the Bank (e.g. exercising the right to a tax deduction, paid leave, the right to a special gift for a child and similar),
- processing of personal data of the Bank's shareholders,
- processing of personal data for marketing purposes,
- all other personal data processing activities that the Bank performs or might perform in the future, either temporarily and/or continuously.

This Policy is binding to all organizational units of the Bank.

5.1. RELATION OF THE POLICY TO OTHER BINDING ACTS AND INTERNAL RULES OF THE BANK

The provisions of the Personal Data Protection Policy are intended to ensure a high and uniform level of protection of personal data in the Bank. This Personal Data Protection Policy does not affect the existing or future obligations established by laws and other regulations that the Bank must comply with in terms of the processing and use of personal data, which are broader in scope than the principles set out in this Policy.

The provisions of this Policy do not affect the applicability of national legislation adopted in connection with national security, defense or public safety or for the prevention and investigation of criminal offenses and the prosecution of perpetrators of criminal offenses.

The rules applicable to individual areas of personal data processing in the Bank will be regulated in more detail by individual rules that must be in accordance with all relevant regulations in the area of personal data protection and this Policy.

The Bank has adopted additional internal acts for this area and may adopt other internal acts in the future in order to achieve a higher level of personal data protection in a particular area of business, whereby such internal acts shall supplement the provisions of this Policy and cannot contradict the Policy.

6. PRINCIPLES AND LEGAL BASIS OF PROCESSING OF PERSONAL DATA

When collecting, processing, using, keeping and storing personal data, the Bank is obliged to adhere to the basic principles set out in the General Data Protection Regulation, such as:

a) Lawfulness, fairness and transparency - personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
b) Purpose limitation - personal data shall be collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) Data minimization - personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The Bank is obliged to apply anonymization and pseudonymization to personal data if possible in order to reduce the risks for data subjects.
d) Accuracy - personal data must be accurate and kept up to date; every reasonable step must be taken by the Bank to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
e) Storage limitation - personal data can not be kept for longer than is necessary for the purposes for which the personal data are processed
f) Integrity and confidentiality - personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The Bank must organize its operations in such a way that personal data are available only to authorized persons and only to the extent necessary for the performance of their work tasks.

The Bank shall apply appropriate managerial, logical and physical protection measures taking into account technological developments, implementation costs, nature, scope, context and purposes of processing and the risk of personal data breaches.

Such measures include, but are not limited to:

a) preventing the possibility of unauthorized persons entering the data processing systems where personal data are processed or used (physical access control),
b) preventing the possibility of using the data processing system by unauthorized persons, i.e. ensuring that persons authorized to use data processing systems can only access data to which they have authorized access and ensuring that unauthorized persons cannot read, copy, alter or remove personal data during their processing or use or after their recording/saving (controls of segregation of duties, essential business needs, user authentication and authorization of activities),
c) ensuring the protection of personal data against accidental destruction or loss (integrity and availability controls),
d) ensuring that unauthorized persons cannot read, copy, alter or remove personal data during physical or electronic transmission or recording on a data carrier and ensuring the possibility of verifying and establishing the identity of the recipient of personal data (data transfer control),
e) ensuring the possibility of retroactive examination and determination of whether personal data were entered into the data processing systems, altered or removed and who entered, changed or removed them (controls of non-repudiation and provability),
f) ensuring that the personal data being processed can only be processed for the purposes for which they were collected, i.e. the possibility of separating the processing of data collected for different purposes (segregation rule).

6.1. LEGAL BASIS FOR PROCESSING OF PERSONAL DATA

The Bank may process personal data only if at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special categories of personal data may only be processed if there is one of the legal bases listed in Article 9 of the General Data Protection Regulation.

6.1.1. DATA SUBJECT'S CONSENT

Processing of personal data can be based on the data subject's consent. If the collection and processing of data is based on the consent of the data subject, the Bank must be able to demonstrate that the data subject has consented to processing of his or her personal data.

The data subject gives consent by a clear affirmative action expressing the data subject's voluntary, specific, informed and unambiguous consent to the processing of personal data relating to him or her for specific purposes.

The request for consent shall be presented to the data subject in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the Bank shall inform the data subject thereof. It shall be as easy to withdraw as to give consent.

Given that the data subject may withdraw consent at any time, the Bank will rely on consent only if there is no other, more appropriate legal basis for the processing of personal data. Consent can constitute an adequate legal basis for the processing of personal data only if its provision is truly voluntary and if the data subject can withhold it without suffering any adverse consequences.

6.1.2. OBTAINING PERSONAL DATA BASED ON A LEGITIMATE INTEREST OF THE BANK

In the case when the Bank processes personal data on the basis of its legitimate interest, the nature of its legitimate interest and the circumstances on the basis of which the Bank concluded that its legitimate interest overrides the interests, rights and freedoms of the respondents shall be stated in the record of processing activities.

In cases where the legitimate interest is not obvious but requires the application of a more detailed proportionality test and more thorough analysis, the Bank shall document in writing in more detail the reasons on the basis of which it has determined that the legitimate interest are overridden by the Bank.

6.1.3. PROCESSING OF PERSONAL DATA FOR DIRECT MARKETING PURPOSES

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the Bank.

This must be personal data that the Bank has previously lawfully collected. The use of the data for direct marketing purposes must be within the scope of what the data subject can reasonably expect based on his or her relationship with the Bank as the controller. Otherwise, the processing of personal data for the purposes of direct marketing and sales must be based on the consent of the data subject (for example, the use of automated calling and communication systems without human intervention, fax machines or electronic mail, including SMS and MMS messages).

If the Bank processes personal data for direct marketing purposes, the data subject shall have the right to object to such processing at any time. At the time of the first communication with the data subject at the latest, the data subject shall be informed of this right in a clear and transparent manner, separately from any other information.

If the data subject objects to the processing for direct marketing purposes, the Bank shall no longer process his or her personal data for such purposes.

7. RIGHTS OF THE DATA SUBJECT

7.1. RIGHTS OF THE DATA SUBJECT IN GENERAL

The data subject has the following rights regarding the processing of personal data:

- the right of access to personal data
- the right to rectification of personal data
- the right to erasure of personal data
- the right to restriction of processing
- the right to data portability
- the right to object to processing of personal data concerning him or her as well as processing of personal data concerning him or her for direct marketing purposes, including profiling to the extent that it is related to such direct marketing
- the right not to be subject to a decision based solely on automated decision-making, including profiling
- the right to lodge a complaint with a supervisory authority.

7.2. RIGHT OF ACCESS TO PERSONAL DATA

The data subject shall have the right to obtain from the Bank confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing,
b) the categories of personal data concerned,
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations. If personal data are transferred to a third country or an international organization, the data subject will be informed of the appropriate safeguards that have been implemented,
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the Bank rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Upon receipt of a request for access to personal data, the Bank will provide the data subject with the above information, or the information requested by the data subject, in writing.

The Bank shall provide a copy of the personal data undergoing processing. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

7.3. RIGHT TO RECTIFICATION OF PERSONAL DATA

The data subject shall have the right to obtain from the Bank without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed.

Where appropriate in the circumstances, the Bank will require the data subject to substantiate their claim by providing credible evidence.

7.4. RIGHT TO ERASURE OF PERSONAL DATA

The data subject shall have the right to obtain from the Bank the erasure of personal data concerning him or her without undue delay and the Bank shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent (where the processing is based on consent) and where there is no other legal ground for the processing;
c) the data subject objects to the processing of personal data based on a legitimate interest or for the purposes of direct marketing and there are no overriding legitimate grounds for the processing
d) the personal data have been unlawfully processed;
e) in other cases as referred to in Article 17 of General Data Protection Regulation

The Bank shall consider all the circumstances in each individual case and then decide on the data subject's request. When deciding on the request, the Bank shall take into account the legal grounds that prevent it from erasure of certain personal data.

7.5. RIGHT TO RESTRICTION OF PROCESSING

The data subject shall have the right to obtain from the Bank restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the Bank to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the Bank no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing pursuant to General Data Protection Regulation pending the verification whether the legitimate grounds of the Bank override those of the data subject.

Data subject who has obtained restriction of processing shall be informed by the Bank before the restriction of processing is lifted.

The Bank shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Bank shall inform the data subject about those recipients if the data subject requests it.

7.6. RIGHT TO DATA PORTABILITY

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Bank,

where:

(a) the processing is based on consent by the data subject or the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(b) the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from the Bank to another controller, where technically feasible.

7.7. RIGHT TO OBJECT TO PROCESSING OF PERSONAL DATA

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her if the processing is necessary for the performance of a task carried out in the public interest or a legitimate interest of the Bank or a third party, including profiling based on those provisions.

The Bank shall no longer process the personal data unless the Bank demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Proving the circumstances that allow the Bank to proceed with further processing must be documented in writing.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed by the Bank for such purposes.

7.8. AUTOMATED INDIVIDUAL DECISION - MAKING, INCLUDING PROFILING

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

For the avoidance of any doubt, the Bank does not apply automated individual decision-making but rather makes all decisions that produce legal effects concerning the data subject or similarly significantly affect him or her with human intervention.

7.9. RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY

The data subject shall have the right to lodge a complaint with a supervisory authority relating to processing personal data by the Bank at any time. The supervisory authority is Personal Data Protection Agency (AZOP) http://azop.hr/

7.10. EXERCISE OF THE RIGHTS

The data subject shall have the right to request the exercise of any of the above rights at any time.

In the event that a request for exercising rights is submitted by a person who is not physically present, the Bank may, before acting on the request, request the applicant to provide additional information in order to verify his or her identity.

The Bank shall take appropriate measures and actions to provide any information relating to processing the personal data of the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The communication with the data subject shall be carried out in line with the requests of the data subject whenever it is possible (by e-mail, fax or in writing by post mail).

The Bank shall not refuse to act on the request of the data subject for exercising his or her rights. The Bank shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Bank shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the Bank does not take action on the request of the data subject, the Bank shall, without delay, and no later than one month from receipt of the request, inform the data subject of the reasons for not acting upon the request and of the possibility of submitting a complaint to the supervisory authority and seeking legal remedy.

Information provided by the Bank shall be free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Bank may either:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, in which case the Bank will notify the data subject of the cost amount and act on the request only after the data subject agrees to bear the cost; or
- refuse to act on the request.

7.11. RECORDS OF THE RECEIVED REQUESTS BY DATA SUBJECTS

The Personal Data Protection Officer shall keep records that must summarize all requests received from the data subject, responses to requests, if necessary, internal reports on investigations conducted and similar documentation related to each request by the Data Subject.

These records shall be kept in electronic form. The records shall be kept chronologically, in such a way that each request received from the data subject may be accompanied by a response to it and other supporting documentation. The records shall demonstrate that the deadlines for processing the request are being met.

These records shall be available to the supervisory authority upon request.

8. VIDEO SURVEILLANCE

For the purpose of protecting the data subjects, the Bank may set up video surveillance over the Bank's Branches and other business premises and their immediate surroundings.

The Bank shall independently collect the above-mentioned personal data for the purpose of fulfilling legal obligations under the Act on the Protection of Financial Institutions, and in particular for the purpose of protecting persons and property when using devices for depositing, withdrawal and storing cash and valuables, protecting persons and property in branches of financial institutions, protecting persons and property when distributing cash and valuables, and protecting the confidentiality of personal and other data in financial institutions.

The Bank must mark that the facility or an individual room in the facility and the external surface of the facility are under video surveillance, and the mark will be visible at the latest upon entering the recording perimeter.

Only authorized persons of the Bank have the right to access personal data collected through video surveillance.

An authorized person can not use recordings from the video surveillance system contrary to the purpose for which they were collected. The video surveillance system must be protected from access by unauthorized persons.

The Bank shall keep recordings obtained through video surveillance for a maximum of six months, unless another law stipulates a longer storage period or if they represent the evidence in a court, administrative, arbitration or other equivalent procedure.

9. RECORDS OF PROCESSING ACTIVITIES

9.1. MAINTAINING A RECORD OF PROCESSING ACTIVITIES

The Bank shall keep records of processing activities, which shall describe in detail all personal data processing procedures carried out by the Bank, in a manner that enables detailed insight into information on each individual processing. The Bank shall keep the said records in a written form, including electronic form. The Bank shall appoint authorized persons for personal data protection in individual organizational units who shall be obliged to keep the said records up-to-date for their organizational unit. The personal data protection officer shall be responsible for keeping consolidated records of processing activities.

The persons authorized for personal data protection shall be obliged to inform the personal data protection officer of all changes related to the processing of personal data and to check the up-to-dateness of the records in their area of competence at least once a year, and more frequently if necessary.

10. DATA PROTECTION OFFICER

10.1. DESIGNATION OF THE DATA PROTECTION OFFICER

Acting as the controller, the Bank shall designate a Data Protection Officer, publicly disclose his or her contact details and communicate them to the supervisory authority without delay.

When making a decision to appoint a Personal Data Protection Officer, the Bank shall ensure that the appointed person has the appropriate professional knowledge to implement all measures and activities for the protection of personal data. The officer must have the necessary professional qualifications, and in

particular, professional knowledge of the law and practices in the area of the protection of personal data. Although the certificates obtained by the officer may be helpful, the ongoing trainings, knowledge of the processes and understanding of the Bank's IT system as well as the legal framework of the Bank's operations are of greater importance for the performance of the officer's function.

The Bank may outsource the function of the Personal Data Protection Officer.

10.2. POSITION OF THE DATA PROTECTION OFFICER

The Data Protection Officer is autonomous and independent in his or her work and is authorized to take all necessary actions and measures to ensure compliance of the Bank's operations with the regulations and personal data protection. The Bank shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The Bank shall support the data protection officer in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The Bank shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the Bank for performing his tasks. The data protection officer shall directly report to the Management Board of the Bank.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the General Data Protection Regulation. The data protection officer may fulfil other tasks and duties. The Bank shall ensure that any such tasks and duties do not result in a conflict of interests. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

The Bank shall ensure that all organizational units of the Bank, starting from their managers and downwards, are familiar with the role of the Personal Data Protection Officer and with the importance of informing the officer about requests to exercise the rights of data subjects, personal data breaches, new types of processing, intended use of new technologies and similar.

10.3. TASKS OD THE DATA PROTECTION OFFICER

The officer is obliged to perform his or her tasks personally, properly and conscientiously. The Personal Data Protection Officer is responsible for implementing all measures and activities aimed at achieving the objectives of the privacy and personal data protection policy of the data subjects, implementing legal, sublegal and other binding acts in the field of personal data protection.

The obligations and tasks of the Data Protection Officer shall in particular include the following:

- to inform and advise the Management Board and the employees of the Bank of their obligations pursuant to the General Data Protection Regulation and other applicable laws and data protection provisions;
- to monitor compliance with the General Data Protection Regulation and other data protection provisions and with the policies of the Bank, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations
- to carry out revisions of the Bank's policies and regulations/rulebooks on personal data protection

- preparing and reviewing responses to requests for the exercise of the rights of data subjects and keeping records of received requests for the exercise of the rights of data subjects and responses to their requests,
- keeping records of personal data breaches and acting in accordance with the Bank's internal regulations in the event of a breach, and actively engaging in research and reporting on personal data breaches that may occur,
- advisory role in the preparation of the data protection impact assessment referred to in Article 35 of the General Data Protection Regulation (when there is an obligation to prepare an impact assessment),
- regular training by attending training courses intended for personal data protection officers in agreement with the Management Board, but also independently monitoring changes and practices in the area of the protection of personal data,
- to act as the contact point for the supervisory authority,
- performing other activities that contribute to raising the level of personal data protection.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The Personal Data Protection Officer shall inform the Bank's Management Board of any observed non-compliance in the area of the protection of personal data. The Bank's Management Board shall decide on the measures to be taken to eliminate any non-compliance.

The Officer shall be obliged to permanently maintain the confidentiality of all information and personal data that he or she has learned in connection with the performance of his or her duties.

11. PERSONAL DATA BREACH

11.1. PERSONAL DATA BREACH IN GENERAL

Despite the established measures to protect personal data, the possibility of a breach of their confidentiality, integrity or availability cannot be ruled out.

A breach of personal data can have a number of harmful consequences for the data subjects and it is therefore of utmost importance that the Bank reacts to breaches as soon as possible.

A breach of personal data means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data that has been transmitted, stored or otherwise processed.

A breach of personal data is an information security incident.

11.2. ACTIVITES TO BE TAKEN IN THE CASE OF PERSONAL DATA BREACH

The Data Protection Officer is responsible for and coordinates the response to a personal data breach.

The Data Protection Officer must record the personal data breach in the Personal Data Breach Register.

In the event of a personal data breach, the Bank must notify the Supervisory Authority without undue delay, and within 72 hours at the latest if the personal data breach is likely to result in a risk to the rights and freedoms of the data subject. In the event that the Bank fails to notify the Supervisory Authority within the specified period, it shall state and explain the reasons for the delay in its statement to the Supervisory Authority.

In the event of a personal data breach that is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Officer must notify the data subjects of the personal data breach without undue delay, describing the nature of the personal data breach in clear and plain language.

The Bank's actions in the event of a personal data breach are stipulated in detail in the Bank's internal acts.

12. SPECIAL OBLIGATIONS RELATED TO PERSONAL DATA PROTECTION

12.1. EMPLOYEE TRAINING

In order to make employees as aware as possible of the importance of personal data protection, the Bank is obliged to educate all its employees on the significance and methods of personal data protection within the first month of employment.

The Bank shall conduct periodic training of employees during the term of the employment contract with the aim of raising the level of personal data protection and raising employees' awareness of the need to protect their confidentiality. These trainings will be conducted at least once a year and will be recorded by the Bank.

Employees will be informed during the trainings that they can report any deficiencies and non-compliances in the area of personal data protection to the officer or their managers.

The training program shall be determined by the personal data protection officer in agreement with the Bank's Management Board, taking into account the level of risk for individual job positions so that the content of the program is adapted to the employees' work tasks and the extent to which they come into contact with personal data.

12.2. OBLIGATION OF AN ASSESSMENT OF THE IMPACT ON THE PROTECTION OF PERSONAL DATA

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Bank shall carry out an assessment of the impact on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

The Bank may determine that other types of personal data processing it performs pose a high risk and require the preparation of an impact assessment in accordance with the provisions of the General Data Protection Regulation.

A data protection impact assessment in particular be required in the case of:

- a processing involving assessment or scoring, including profiling and envisagement, particularly based on aspects of the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movement
- automated decision making that produce legal effects or similarly significantly affect the data subjects;
- processing involving sensitive data or data of a highly personal nature,
- systematic monitoring of data subjects,
- processing of data relating to sensitive data subjects,
- innovative use or application of new technological or organizational solutions,
- a situation in which the processing itself prevents data subjects from exercising rights or using services or contracts
- other processing that would result in a high risk to the rights and freedoms of individuals.

The Data Protection Officer is actively involved in the preparation of the impact assessment. If a data processor and/or a joint controller are or need to be involved in the processing, the Bank may seek assistance from the latter in preparing the impact assessment.

12.3. ENTERING INTO CONTRACT WITH PROCESSORS

The Bank may decide to entrust certain aspects of the processing of personal data to processors, who will process personal data on behalf of and under the instructions of the Bank.

The Bank will only use processors providing sufficient guarantees to implement appropriate technical and organizational measures to protect personal data.

The Bank is obliged to conclude a written contract with the processor that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the Bank and the processor.

Depending on the circumstances of the case, the Bank may, before engaging a specific processor, conduct controls that it deems reasonable and appropriate, such as:

- request information on whether the processor has appointed a personal data protection officer,
- request information on whether the processor engages sub-processors as well as who is engaged and in which countries they are located,
- check with the processor whether it keeps records of processing activities,
- check with the processor whether it has any internal policies and procedures regarding the protection of personal data,
- conduct discussions on the way in which the processor's relevant processes are organized,
- request information on whether the processor has a certificate that it is compliant with the GDPR (certification is not mandatory, but it is useful to state if they have one),
- request information on whether the processor has any ISO certificates in the area of IT security,
- visit the processor's business premises,
- if it is a processor with which the Bank has been cooperating for a long time, their conscientiousness and regularity in the previous performance of contractual obligations may be taken into account
- other reasonable controls

The Bank shall, as a rule, avoid cooperation with processors where personal data should be transferred to a third country (outside the EU). Cooperation with such processors may occur if appropriate safeguards are implemented in accordance with Chapter V of the General Data Protection Regulation.

12.4. CONTRACTS THAT INCLUDE THE EXCHANGE OF DATA WITH OTHER RECIPIENTS

In its business operations, the Bank may enter into legal relationships with other legal and natural persons with whom it does not act as a joint controller or engage them as its processors. In such legal relationships, certain personal data may be exchanged. Personal data may also be exchanged with state authorities.

In all such cases, depending on the circumstances, the Bank assesses whether it is necessary to conclude a written contract that more closely defines the rights and obligations of the contracting parties, and whether and to what extent such a written contract, in addition to the general provision on the obligation of both contracting parties to maintain the confidentiality of all information and personal data that they receive from each other for the purpose of performing contractual obligations, should include additional provisions on the exchange of personal data.

Such additional provisions on the exchange of personal data may in particular include provisions specifying the purpose of the exchange of personal data, the categories of personal data transferred, the legal basis for the transfer of data, the limitation of further recipients of the personal data, the obligation to maintain confidentiality, the period during which the recipient will store the personal data, the consequences of a breach and similar.

Personal data exchanged with recipients shall in any case be limited to what is necessary to achieve the purpose for which the transfer is made.

12.5. CROSS BORDER TRANSFER OF PERSONAL DATA

The Bank may transfer personal data to the countries that ensure an adequate level of protection. The countries that ensure an adequate level of protection are:

- Member States of the European Union,
- Countries and territories for which the European Commission has adopted a decision that they ensure an adequate level of protection of personal data.

The Bank may transfer personal data to other countries, but only on condition that appropriate safeguards are applied and that one of the derogations for special cases provided for in the General Data Protection Regulation can be applied to the intended transfer.

In such cases, the Bank shall agree to the application of standard contractual clauses adopted by the European Commission or special contractual clauses approved by the competent authority.

The Bank shall transfer employee personal data in the above manner only if there is a legal basis for the transfer.

In the case of doubt as to whether the transfer of personal data to a country that does not ensure the adequate level of protection is permitted, the Bank shall seek prior advice and opinion of the Data Protection Officer.

12.6. USE OF COOKIES

The Bank's websites use cookies.

Cookies are small text files that the websites store on the visitor's computer when they visit the website. The Bank uses cookies that do not identify the visitor but provide necessary support for the functionality of the website.

For the avoidance of any doubt, the Bank does not seek to use cookies to determine the identity of individuals but uses cookies only for the purposes stated above.

When visiting the Bank's website, the visitor is provided with information about the type of cookies used by the website, their purpose and the possibility of their exclusion.

12.7. SAFEGUARDS AND COOPERATION

The Bank will take all necessary measures to rectify any weaknesses identified during the supervision that will or might affect the violation of the obligation to protect personal data.

The Bank is obliged to cooperate with the Personal Data Protection Agency (AZOP) or other competent authority. The Bank shall require its processors to cooperate with the supervisory authorities in cases where this is necessary.

13. FINAL PROVISIONS

13.1. INTERPRETATION

This Policy shall be interpreted in accordance with the General Data Protection Regulation and the applicable legislation of the Republic of Croatia in the area of the protection of personal data.

13.2. COMPETENCE AND JURISDICTION OF THE COURT

Laws and other regulations applicable in the Republic of Croatia shall apply for any disputes arising from a personal data breach, and the court competent to resolve the dispute is the court with the subject-matter jurisdiction over the Bank's registered office location.

13.3. NULLITY OF INDIVIDUAL PROVISIONS

In the event that a certain provision of this Policy is found to be null and void, such provision shall be deemed to have been replaced by a provision that, to the greatest extent possible, corresponds to the intention that the Bank sought to achieve with the invalid provision.

13.4. PRIOR CONSULTATION AND ENTRY INTO FORCE

This Policy shall enter into force on 19 March 2024. On the date of entry into force of this Policy, the Personal Data Protection Policy version 1.2. of 16 December 2021 shall be repealed. This Policy or its individual parts may be published on the Bank's website.