PERSONAL DATA PROTECTION POLICY OF HRVATSKA POŠTANSKA BANKA PLC

Office of Corporate Security

V 1.0

PUBLIC

In Zagreb, on 15th March 2018

Document details

Document title	Personal Data Protection Policy of Hrvatska poštanska banka plc
Document version	1.0
Document label	
Document owner	Office of Corporate Security
Document classification	PUBLIC
Document prepared by	Dalibor Kovačević
Document approved/verified by	All business units of the Bank
Document adopted by	The Management Board of the Bank
Document prepared on	15th March 2018
Date of entry into force	20th March 2018
Date of application	20th May 2018

Change history

Version	Date	Author	Notice
1.0	15th March 2018	Dalibor Kovačević	Initial version

CONTENTS

Based on Article 13 of the Articles of Association of Hrvatska poštanska banka plc, Zagreb, Jurišićeva 4 (hereinafter: the Bank) and General Data Protection Regulation (Regulation EU 2016/679), the Management Board of the Bank adopted at its meeting held on 20th March 2018 the following document

PERSONAL DATA PROTECTION POLICY

I. GLOSSARY

Personal data – information relating to an identified or identifiable natural person ("data subject")

Data subject - is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal data processing - 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 - the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Processor - a natural or legal person which processes personal data on behalf of the controller;

Information system - a total of technological infrastructure, organisation, human resources and procedures for the collection, processing, generating, storage, transmission, representation and distribution of information and the disposal thereof. The information system can also be defined as an interaction between information technology, data and data processing procedures and the people collecting and using these data.

Supervisory authority - an independent public authority which is established by the Republic of Croatia for the purpose of controlling and ensuring the implementation of the Regulation

Confidentiality - a property of information (data) implying that it is not made available or disclosed to unauthorised parties

Integrity - a property of information (data) and processes implying that they have not been subject to unauthorised or unforeseen alterations.

Consent - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her ;

Pseudonymisation - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional

information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

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

Profiling – any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

Third parties – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

Distribution channels – are means of and ways in which access, contracting and use of the Bank's products and services are enabled, and sending commercial information and offers in connection with the Bank's products and services, including branch offices of the Bank and its partners, ATMs, online banking, mBanking and the Bank's website: www.hpb.hr, etc. Any information on available distribution channels of the Bank is available to a Customer at any time from the Contact Centre.

Binding corporate rules - personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity

II. PRINCIPAL PROVISIONS

For the purpose of this Policy Hrvatska poštanska banka Group comprises Hrvatska poštanska banka d.d. HPB Invest d.o.o., HPB-Nekretnine d.o.o and HPB Stambena štedionica d.d.

Data protection has an important place in Hrvatska poštanska banka Group's business (hereinafter: HPB Group, the Group) which in its everyday operations collects and processes personal data of customers, employees, business partners and other persons with whom it cooperates in business (hereinafter: data subjects). This Policy sets forth the fundamental principles of, and rules on the data protection in compliance with the business and security requirements of HPB Group, as well as with laws, best practices and internationally accepted standards.

The Personal Data Protection Policy (hereinafter: the Policy) is the fundamental act describing the purpose and goals of collecting, processing and managing personal data within HPB Group, based on the leading global practices in the area of personal data protection. The Policy ensures the adequate level of data protection in compliance with the General Data Protection Regulation (hereinafter: the Regulation) and other applicable current laws in connection with personal data protection, ensured additionally by the Group by detailed internal Acts.

All members of HPB Group have adopted this Policy.

III. SCOPE AND GOAL

The Personal Data Protection Policy is the fundamental act of HPB Group having for its purpose the introduction of the framework relating to personal data protection in compliance with the General Data Protection Regulation.[1] The Policy lays down rules relating to the protection of natural persons with regard to the collecting and processing of personal data and rules relating to the free movement of personal data.

The goal of the Policy is to establish the adequate processes of protecting and managing personal data of data subjects, or customers, employees, business partners of the members of HPB Group and other persons whose personal data are processed.

The Policy is applied to all personal data processed within the Group, with the exception of cases where information rendered anonymous is processed or concerning the processing for statistical analysis purposes where natural persons are not identifiable.

[1] 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

IV. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

The principles relating to processing of data are fundamental rules adhered to by HPB Group when processing personal data of data subjects. The processing carried out in compliance with the principles specified below shall be regarded as lawful.

Each business unit of HPB Group shall ensure the adherence to the principles specified below within its own domain and when processing personal data for which a business unit is a controller.

HPB Group processes personal data in compliance with the following principles relating to processing:

1. **Lawfulness and fairness** – in relation to data subjects and their rights, HPB Group shall process personal data in compliance with current laws and taking into consideration all the rights of data subjects. The Group shall sometimes have to require also certain personal data from data subjects not necessary to provide a relevant service but required by law (as for example, the Anti-Money and Terrorist Financing Act). Consequently, within the Group clear rules and processes have been defined in order to ensure lawful and fair processing, and control mechanisms have been also established (as for example, periodical audits, technical measures).
2. **Transparency** – HPB Group shall ensure transparency of personal data processing and shall in compliance with the Regulation provide data subjects with all required information and make data, purpose of, grounds for and lawfulness of processing, etc., on request, available to data subjects. By means of this Policy and other channels available to data subjects, the Group shall provide data subjects with information that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. Data subject shall be in a timely manner provided with all relevant information.
3. **Purpose limitation** – personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. For example, if a data subject has made available a set of personal data (for example, first name, family name, PIN, level of salary, etc.) for the purpose of a loan application, the Group shall not process such data for any other purpose, unless there is other processing required by law or necessary to provide a service itself in a quality manner.
4. **Storage limitation** – HPB Group shall ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Group may store personal data for longer periods insofar as it has clear purpose in terms of legal obligation (for example, the Archival Matter and Archives Act) or a legitimate interest (for example, in case of a lawsuit).
5. **Data minimisation** – HPB Group shall collect and process personal data in a manner that they shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The processes in the Group have been designed not to collect data unless there is reasonable need to collect them and every member of the Group and every business unit of the members of the Group shall ensure the adequate adherence to this principle.
6. **Accuracy** – HPB Group shall ensure that personal data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. The Group ensures the adherence to this principle having introduced regular controls and also transparent process of

communication with data subjects where a rectification of data may be required if a data subject notices that any of his/her personal data is incorrect.

7. **Integrity and confidentiality** – HPB Group shall collect and process data in a manner that insures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The Group has implemented IT systems for the purposes of detection and prevention of data leaks, systems for data anonymisation/pseudonymisation, methods by which to control access to data, data access limitations according to the requirement of a work position, etc.

In compliance with the above principles, personal data of data subjects shall be accessed by the Group's employees depending on their mandates and work positions, in order that they may successfully perform the jobs designated for their work positions. Also, some services have been provided for HPB Group by other legal persons with whom the data of data subjects shall be shared only if such data has been necessary for the performance of the obligations arising under the Contracts between HPB Group and such providers. The example of this is the production of bank cards, documentation storage and sending of account statements to home addresses.

The Group shall transfer data of data subjects also to the Associations or national institutions where there is a legal ground for that (for example, for the purposes of the central register of accounts and the Financial Agency “FINA”).

V. LAWFULNESS OF PROCESSING

HPB Group shall regard data subjects as the owners of their data and shall treat such data accordingly. However, in order that the Group may provide a service to a data subject, in compliance with the lawfulness criteria below, it is required to process a minimum set of data necessary to adequately provide a service. Otherwise, or if a data subject refrains from providing a necessary set of data, HPB Group will not be able to provide a service to such data subject.

Consequently, personal data of data subjects shall be processed when one of the following conditions has been met:

a) 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) processing is necessary for HPB Group compliance with legal obligations (current regulations to which the Bank is subject) – at any moment when a law authorises or obliges HPB Group in respect of certain processing, HPB Group shall process on the basis of such law personal data of data subjects. For example, where there is a legal obligation, such as the Anti-Money Laundering and Terrorist Financing Act, HPB Group shall collect and process a set of data defined by law, and in case a data subject refrains from providing a necessary set of data, HPB Group will not be able to provide a service to such data subject.

c) processing is necessary for the purposes of the legitimate interests pursued by HPB Group 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. The legitimate interests of the Group include data processing in order to improve process, develop products

and improve business, update services, offer products and services which would clearly facilitate the data subject's transactions with the Bank, improve data subject's own finance management, and for the benefit of resolving lawsuits.

d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes – the consent shall be demonstrable and freely given, composed using clear and plain language, and the data subject shall have the right to withdraw his or her consent at any time (the withdrawal of consent shall be equally simple as giving of consent). The Group shall request the data subject for consent for data processing and contacts for the purpose of direct marketing through contact details provided to the Group by the data subject. The presentation of new products and services, inaccessibility of a certain service communicated by the Bank via available distribution channels, the Bank regards as a part of the service and shall not request the consent of the data subject insofar as the processing has been compliant with the principles of processing referred to in Section V and has been based on any of the specified lawfulness criteria.

e) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

f) 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;

Each business unit within HPB Group shall identify the lawfulness of each processing carried out in their business domain. Fort such identification a data protection officer shall be also consulted who shall on the basis of clear and predefined criteria advise a business unit for the identification of lawfulness of processing.

VI. RIGHTS OF THE DATA SUBJECT

HPB Group is aware that the personal data of the data subject is his or her property, and although we need such data to provide a service, data subjects reserve at any time certain rights in respect of the processing of their data, and HPB Group shall collect and process data only if such processing has been lawful.

HPB Group shall at the time when personal data are collected from the data subject, provide the data subject with the following information: the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the legitimate interests, the recipients or categories of recipients of the personal data, the intent to transfer personal data to a third country (if any), the period for which the personal data will be stored or the criteria used to determine that period, the consent related rights, the potential existence of automated decision-making, including profiling (meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject), and the existence of the rights specified below. Where personal data are not collected from the data subject, in addition to the above information it shall be also stated from which source the personal data originate.

HPB Group shall process personal data in compliance with the rights of the data subjects defined in the Regulation, as specified below:

- **Right to erasure ("right to be forgotten"** - the data subject shall have the right to obtain from HPB Group the erasure of personal data concerning him or her and HPB Group 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 on which the processing is based, and where there is no other legal ground for the processing
c. the data subject objects to the processing, and there are no overriding legitimate grounds of the Group for the processing and/or storing of the personal data
d. the personal data have been unlawfully processed
e. the personal data have to be erased for compliance with a legal obligation

- **Right of access to data** - the data subject shall have the right to obtain from HPB Group 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 purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data will be disclosed, etc.
- **Right to rectification** - the data subject shall have the right to obtain from HPB Group 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, including by means of providing a supplementary statement. The data subjects are also obliged to update personal data in the business relationship with the Group.
- **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 HPB Group, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller. The right to data portability shall refer exclusively to the personal data of the data subject.
- **Right to object** - 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. HPB Group shall no longer in such a situation process the personal data unless it 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. 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.
- **Right to restriction of processing** – The data subject shall have the right to obtain from HPB Group restriction of processing where the accuracy of the personal data is contested by the data subject, the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead, and where the data subject has objected to processing and pending the verification whether the legitimate grounds of the controller override those of the data subject.

The data subject has the right to request at any time the exercise of any of the above rights. HPB Group shall on the data subject's request provide information on actions taken in respect of the above rights, at the latest within 3 months of receipt of the request (depending on the number and complexity of the requests) – efforts shall be made to address all requests within 1 month, and that period may be extended by two further months where

necessary. If HPB Group does not take action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action. The reasons for not taking action include the existence of lawfulness of processing preventing HPB Group to act accordingly.

In addition, the data subject shall have the right not to be subject to a decision which is based solely on automated processing, including profiling, and which produces legal effects concerning him or her or similarly significantly affects him or her, unless such decision:

- is necessary for entering into, or performance of, a contract between the data subject and HPB Group
- is authorised by law
- is based on the data subject's explicit consent

VII. OBLIGATIONS OF HPB GROUP IN COMPLIANCE WITH THE REGULATION

Individual members of HPB Group in complying with the Regulation shall assume certain obligations. The obligations shall depend on the role an individual member of the Group has in respect of relevant processing of data. The members of the Group are in some business processes the controllers, and in others joint controllers, and they may also be the processors. An individual member of the Group is the controller in the business processes where it has alone determined the purposes and means of the processing of personal data, while it is the joint controller in the business processes where it has determined, together with other controllers, for example business partners whose products and services are contracted by it in its business network, the purposes and means of the processing of customer personal data. An individual member of the Group may also be the processor in the situations where it processes personal data on behalf of the controller (for example, a member of the Group contracts services for another legal person).

The Group is continuously implementing appropriate technical and organisational measures, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of the data subjects.

The above measures include the implementation of appropriate policies of data protection:

- The personal data of the data subjects is kept in accordance with the HPB Group's internal standards of safety. The Group is continuously using significant organisational and technical measures in order to protect the personal and all other data of the data subjects. Where appropriate, HPB Group is implementing the protection measures such as encryption, and is continuously working on the improvement of security measures at HPB Group level. In addition to that, advanced tools for the protection of data and the prevention of data leaks are used, and the critical systems within the Group are controlled, etc.
- HPB Group does not permit unauthorised collecting, processing and using of personal data. The rule of restriction of access to data is applied only to the data necessary to perform individual business tasks. Consequently, the roles and responsibilities within the Group have been clearly defined. The employees of the Group have been strictly prohibited to use the personal data of the data subjects for any purpose inconsistent with the conditions defined in Section IV Lawfulness of processing. It is necessary to stress that individual business units of the Group, in accordance with current laws (for example, the Anti-Money Laundering and Terrorist Financing Act), have the right to access and process some personal data but exclusively within the scope necessary to satisfy the regulatory requirements or to perform the contract with the data subject. These processes are under a strict control and comprised by monitoring systems.
- Personal data are protected from unauthorised access, use, alteration and loss. Mechanisms to ensure the protection of personal data are applied within the Group regardless in which form it is kept – in paper form or by electronic means.
- The compliance with this Policy and other policies and procedures in connection with data protection are also regularly monitored within the Group by the data protection officer.

VIII. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

HPB Group shall not process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership or data concerning a natural person's sex life or sexual orientation.

Processing of special categories of personal data referred to above shall be carried out by HPB Group exclusively if one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of HPB Group or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union, the Republic of Croatia law or a collective agreement pursuant to the Republic of Croatia law providing for appropriate safeguards for the fundamental rights and the interests of the data subject
- processing is necessary to protect the vital interests of the data subject or of another natural person
- processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defence of legal claims

HPB Group shall apply specific protection of personal data of children, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Children are persons under sixteen years of age.

IX. AUTOMATIC PERSONAL DATA PROCESSING

Decision-making based on automated data processing is the integral part of the Group's business and is necessary, and is carried out in compliance with:

- current laws to which HPB Group is subject, among others for the purposes of monitoring and preventing fraud, money laundering and tax-evasion, etc., and is conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies
- to ensure the security and reliability of a service provided by HPB Group
- if necessary for the entering or performance of a contract between the data subject and a controller, including mitigating the risk involved in business, improving business, certain overnight processing which is inherent to IT system, etc.
- when the data subject has given his or her explicit consent

In compliance with the Regulation, HPB Group recognizes the right of the data subject to object to automated, but also to manual processing, for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge.

X. TRANSFER OF PERSONAL DATA

The members of HPB Group as a whole cooperate at multiple levels seeking to provide services of as high as possible quality and on as advantageous terms as possible. In order that this cooperation may proceed smoothly it is necessary to exchange customer personal data within the Group.

The members of HPB Group exchange personal data if necessary in order to provide the data subject with the requested service i.e. only if necessary on the basis of the conditions referred to in Section IV Lawfulness of processing or for the activities entrusted to the Bank by the members of the Group, as governed by special agreements.

Furthermore, on the data subject's request the transfer of personal data is possible also to the partners of HPB Group entrusted with the provision of certain services on behalf of individual members of the Group. Where transferring the personal data of the Group's data subjects to external partners, the principle of restriction of processing has been strictly adhered to and the minimum of data necessary to provide the requested service is transferred. The Group has also in place mechanisms requiring the partners to have in place at least the level of protection of personal data the members of the Group have.

For the purpose of risk mitigation, the Group shall when entering into, but also during the business relationship, be required to identify the customer's creditworthiness and monitor the performance of contract obligations. Creditworthiness shall be verified on the basis of information obtained from the customer, available registers of data and the history of business relationship with the Group in case of the customer with the history of such business relationship. For example, when approving loans or credit cards, the customer's creditworthiness will be assessed. Also, the loan repayments, salary payments, if the customer has obtained certain loan related benefits on the basis of them, regular insurance policy renewals, etc. will be monitored. In case any member of the Group assesses that the customer is not creditworthy, a member of the Group has the right to refuse to provide the requested loan or credit card to the customer.

HPB Group will transfer personal data to third countries or international organisations when necessary, and exclusively in compliance with the conditions referred to in Section IV Lawfulness of processing. In such situations appropriate safeguards have been provided for where disclosing personal data in compliance with the Regulation. These may be provided for by a legally binding and enforceable instrument, binding corporate rules, certification, etc.

XI. USE OF PERSONAL DATA IN TRANSACTIONS WITH BUSINESS CUSTOMERS

Business customers of the Group are any legal person, national authority, unit of local or self-government and their bodies, association and society (sports, culture, charity, etc.), and any natural person (who is not a consumer), acting within the area of its registered business activities or liberal profession.

The Group shall collect and process data related to business customers, transactions, use of products and services and personal data of natural persons (who are not consumers), acting within the area of their registered business activities or liberal profession, as well as personal data of natural persons (consumers) - related parties of business customers.

The related parties of a business customer in the context of this Policy may be natural persons – business customer's owners, authorised persons, procurators, attorneys-in-fact, representatives, persons authorised under transaction account, users of online banking

services, users of business cards, guarantors, co-debtors, pledgers and other natural persons whose personal data has been provided by a business customer to the Group for its use for the purposes of establishing and maintaining business relationship.

The Group shall collect, process and share data of business customers, including personal data of business customers and related parties, in compliance with above Section V Lawfulness of processing.

The members of the Group may process collected data of business customers, including personal data of natural persons (who are not consumers), acting in the area of their registered economic activities or liberal profession, and of related parties, provided to the Group by a business customer for the following purposes:

- Identification
- Risk assessment when establishing and maintaining business relationship
- Prevention of risks which may arise under a business relationship
- Compliance with the laws and regulations inside and outside the territory of the Republic of Croatia
- Contracting and using the products and services provided by the Group
- Performing all types of banking transactions inside and outside the territory of the Republic of Croatia
- Identification of creditworthiness
- Recovery of claims
- Reporting
- Processing for statistical purposes
- Developing and improving products and services in order to ensure better customer experience
- Defining products and services useful to business customers of the Group
- Contacts for the purposes of performance of contracts within the Group
- Contacts for marketing purposes.

The Group may share data of business customers, including personal data of natural persons (who are not consumers), acting in the area of their registered economic activities or liberal profession, and of related parties, provided to the Group by a business customer, complying with Section V Lawfulness of processing and with principles of processing referred to in Section IV Principles relating to processing of personal data, with:

- A member of the Group
- Legislative, oversight and regulatory bodies inside and outside the territory of the Republic of Croatia
- Financial institutions with which the Group is cooperating
- Institutions providing services of Embargo Lists checks
- Ministries, units of local and regional self-government with which the Group is cooperating
- Croatian Registry of Credit Obligations and other credit registers
- Auditors inside and outside the Group and other audit licensed bodies
- Card companies and card processors with which the Group is cooperating
- Other agencies, institutions, associations, insurance companies and partnering companies with which the Group has entered into contracts on business cooperation

based on which business customers may contract and use the products and services provided by the Group

- Etc.

XII. DATA PROTECTION OFFICER (DPO)

HPB Group has appointed a data protection officer who acts in an independent manner and in the interest of the protection of the rights of the data subjects and their personal data. The responsibility of the data protection officer is to ensure that the Group applies the Personal Data Protection Policy and other policies and procedures defining the rules of collecting and processing of the personal data of the data subjects. The data protection officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data. The data protection officer participates in the Group's processes related to the management of changes and projects and has timely access to information

The data protection officer directly reports to the highest management level of HPB Group and is bound by secrecy or confidentiality concerning the performance of his or her tasks. The data protection officer shall have at least the following tasks in HPB Group:

- to inform and advise HPB Group and the employees who carry out processing of their obligations pursuant to the Regulation and to other Union or the Republic of Croatia data protection provisions;
- to monitor compliance with the Regulation, with other Union or the Republic of Croatia data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter.

The data protection officer does not receive any instructions regarding the exercise of those tasks, ensuring him or her further independence.

The data protection officer acts also as the first contact point for the data subjects who want to exercise their rights (issues related to the processing of their personal data and exercising of their rights under the Regulation), make an inquiry in connection with the protection of personal data, request additional information, express concerns related to the processing of their personal data, submit complaints in connection with the protection of personal data and exercise of their rights referred to in the General Data Protection Regulation. The data subjects may contact the data protection officer via the e-mail address dpo@hpb.hr.

HPB Group may charge a reasonable fee taking into account the administrative costs or refuse to act on the request where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character.

The contact details of the data protection officer are also available on the Bank's website, www.hpb.hr.

XIII. IMPACT ASSESSMENT

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, a member of HPB Group shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, if it acts as the controller. A single assessment may address a set of similar processing operations that present similar high risks. Furthermore, HPB Group shall carry out the assessment of the impact of all currently active processing operations corresponding to said categories.

Each individual business unit of the members of the Group shall carry out an assessment of the impact in compliance with the above criteria and applicable internally defined rulebooks and procedures. The business units should contact the data protection officer if uncertain whether or not to carry out an assessment of the impact of a certain processing operation.

The data protection officer shall be responsible for ensuring that "an assessment of the impact on the protection of personal data" is carried out, and shall provide support when such assessment is carried out. HPB Group shall always carry out a data protection impact assessment in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- processing on a large scale of special categories of data
- a systematic monitoring of a publicly accessible area on a large scale
- processing operations established by the supervisory body (Croatian Personal Data Protection Agency)

The assessment of the impact shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued by HPB Group;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

XIV. REGISTER OF PERSONAL DATA PROCESSING OPERATIONS

HPB Group maintains records of processing activities under its responsibility, i.e. where acting as the controller or joint controller. That record shall be in electronic form and contain at least the following information:

- the name and contact details of the controller and the data protection officer;
- the purposes of the processing;

- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;
- where possible, the envisaged time limits for erasure of the different categories of data;
- a general description of the technical and organisational security measures.

The data protection officer shall be responsible for maintaining records of processing activities, and all business units of the Group shall be responsible for delivery of accurate and timely information in order that the records of processing activities would include required data.

XV. INCIDENTS/DATA LEAKS AND RIGHT TO LODGE A COMPLAINT

HPB Group shall take significant technological measures and have processes in place in order to protect the personal data of the data subjects. Furthermore, all HPB Group's employees are obliged to report to responsible persons (first of all, the data protection officer) any incident related to the protection of personal data, and in case of any personal data breach, HPB Group shall report such incident to the Croatian Data Protection Agency within 72 hours of becoming aware of such breach, where possible. HPB Group shall report incidents to responsible persons directly where acting as the controller or joint controller, and where acting as the processor, through the controller acting as the first contact point.

Also, in the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of the natural persons, HPB Group shall communicate without undue delay to the data subject a personal data breach.

By way of derogation, HPB Group shall not communicate to the data subject a personal data breach, if at least one of the following conditions is met:

- HPB Group has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
- HPB Group has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

The data subject has the right to lodge a complaint with the supervisory authority (Croatian Data Protection Agency) in case of incidents related to his or her personal data or if he or she feels that HPB Group is breaching his or her rights under the General Data Protection Regulation.

XVI. FINAL PROVISIONS

This Policy shall enter into force on the day of its adoption, and it shall apply from 20th May 2018.

Member of Management Board	Member of Management Board
Mladen Mrvelj	Domagoj Karadjole