J&T BANKA

RULEBOOK ON PROTECTION OF PERSONAL DATA

PURPOSE AND OBJECTIVE

Rulebook on protection of personal data is an umbrella regulation of J&T banka d.d., purpose of which is to establish personal data protection in accordance with provisions of General Data Protection Regulation (Regulation) and the Act on implementation of the General Data Protection Regulation (Act).
Objective is to ensure legal certainty and transparency in regard to personal data processing and in regard to activities of processing of personal data of Bank's clients, employees and of any other persons whose personal data is being processed, and to set the basis and purpose of processing, categories of persons whose data is being processed, natural person's rights, protection measures, and similar.

TERMS AND ABBREVIATIONS
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 (Regulation)
Act on implementation of the General Data Protection Regulation (Act) (provision of the Act highlighted in green colour)
J&T banka d.d. (Bank)
European Union (Union)
Croatian Personal Data Protection Agency (Agency)

Terms in this Rulebook have the same meaning as the terms used in the Regulation:
Personal data, Data subject, Processing, Restriction of processing, Profiling, Pseudonymisation, Controller, Processor, Recipient, Consent, Personal data breach, Genetic data, Biometric data, Data concerning health, Supervisory authority and other terms used in the Regulation.

SCOPE OF APPLICATION
The provisions of this Rulebook shall apply to all employees of the Bank, in particular organizational unit working in direct contact with clients.

Principles relating to processing of personal data
Personal data in the Bank is being processed in such manner that the Bank as the controller, in all its organizational units, strictly complies with the following principles:

(a) **lawfulness, fairness and transparency;** controller processes data in line with all provisions of law, protecting all necessary rights of data subject's; controller shall provide to data subject any additional information necessary to ensure fair and transparent processing takin into consideration special circumstances and the context of personal data processing; controller doesn't conduct profiling nor automated decision making
(b) **purpose limitation;** data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; but further processing is possible for purposes of archiving in the public interest, scientific or historical research purposes or statistical purposes
(c) **data minimisation**; data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
(d) **accuracy**; data must be accurate and, where necessary, kept up to date; Bank shall undertake reasonable measures to ensure that personal data that are inaccurate are erased or rectified without delay
(e) **storage limitation**; data must be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes, subject to implementation of appropriate protection measures set by the Regulation

(f) **integrity and confidentiality**; data shall be processed in a manner that ensures 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. Cited measures are implemented in all organizational units of the Bank. It is an obligation for the personal data in all branch offices and in the "back office" to be kept in locked cabinets. It is an obligation to implement clean work desk policy throughout the Bank, while places where personal data is contained must not be left unlocked and without appropriate supervision. All employees of the Bank have signed a confidentiality statement by which they undertake to adhere to the principles of integrity and confidentiality of personal data processing.

Lawfulness of processing

The Bank has set up mechanisms by which it processes personal data lawfully and 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; consent is voluntary, specific, informed and unequivocal expression of data subject's preferences by which it states or by clear affirmative action gives consent for processing of personal data related to it; data subject can revoke its consent at any time

(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; e.g. processing in accordance with the Act on Prevention of Money Laundering and Financing of Terrorism or processing thru video surveillance in accordance with Monetary Institutions Protection Act

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e.g. competent authority's disclosure of one parent's data to the other parent for purposes of child support

(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 controller 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. E.g. for improvements of the process.

Processing of special categories of personal data

The Bank doesn't process personal data which would reveal natural person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, nor does it process 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.

Previously stated shall not apply only if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller 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 laws of the Union or Republic of Croatia;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of laws of the Union or Republic of Croatia;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

(i) processing is necessary for reasons of public interest in the area of public health;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

According to the Act, in the course of personal data processing with the purpose of producing official statistics in line with special regulations in the field of official statistics, authorities producing official statistics are not obligated to ensure data subjects' right to access personal data, right to rectify personal data, right to processing limitations nor the right to object to personal data processing, and this is done to ensure the necessary conditions for fulfilling the purpose of official statistics to the extent to which it is likely that such rights might render impossible or seriously impair the achievement of the objectives of such processing, and when such derogations are necessary for achievement of these objectives.
Authorities competent for producing official statistics are obligated to apply technical and organisational measures for protection of data collected for statistical purposes.
The Bank as the controller of personal data processing isn't obligated to notify data subjects on the transfer of personal data for statistical purposes when transferring personal data to the authorities competent for official statistics.
Personal data processing for statistical purposes is considered compatible with the purpose for which such data was collected, provided appropriate protection measures are taken.
Personal data processed for statistical purposes must not enable identification of a person to which they relate.

Rights of data subjects
The Bank has set up business mechanisms by which all data subject's rights are satisfied in line with the Regulation. The process of exercising data subject's rights is undertaken following the delivery of a request thru the following channels: primarily the personal data protection officer or a branch office, by filling in the Request for the realisation of the rights of the respondents (APPENDIX 1). If the request is delivered thru a branch office, simultaneous notification from the branch office towards the personal data protection officer is necessary. Personal data protection officer is in charge of further coordination with competent organizational units of the Bank in relation to request processing as well as distribution of the request and implementation supervision.

Transparent information, communication and modalities for the exercise of the rights of the data subject
Banka as the controller takes appropriate measures to provide any information referred to in Articles 13 and 14 of the Regulation (APPENDIX 2) and enable for the data subject to exercise its right to access, right to rectification, right to erasure, right to restriction of processing, right to be informed, right to data portability, right to object and notification to the data subject of a personal data breach.
Bank as the controller shall provide information on action taken to exercise data subject's rights 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 controller 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 means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
If the Bank as the controller does not take action on the request of the data subject, the controller 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 and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
Any data subject who considers that any of its rights under the Regulation or the Act is being breached, can file a request for establishing the breach of its rights with the Agency.
It is the obligation of each employee to record the above in the register of the client / person with whom the bank establishes a business relationship, and / or from whom the bank takes personal data (and also a copy of APPENDIX 2), in order to be visible in the client's financial picture.

Izjava o porez.rez.: DA GDPR: DA

Information to be provided where personal data are collected from the data subject
Where personal data relating to a data subject are collected from the data subject, Bank as the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where applicable, the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any; and
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation.
In addition to the information above, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where applicable, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before it was withdrawed;
(d) the right to lodge a complaint with a supervisory authority;
(e) information on whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
Where personal data have not been obtained from the data subject, the source of personal data is added to above mentioned information.

Right of access by the data subject
The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, to access the personal data and the information on, amongst other, personal data which was processed, purpose of processing, storage period and exporting to third countries.

Right to rectification
The data subject shall have the right to obtain from the controller 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.

Right to erasure ('right to be forgotten')
The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following 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 pursuant to Article 21 of the Regulation;
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Republic of Croatia law.

Right to restriction of processing
Data subject's personal data shall be used by the Bank solely for the purpose for which they were collected. In case where business reasons will require for the personal data to be used for any

purpose other than initially envisaged, data subject shall be notified timely and if needed a consent will be requested.
Where need arises to use the personal data for any purpose other than for which it was initially collected, personal data protection officer must be informed and he must allow for such change in written form.
The data subject shall have the right to obtain from the controller restriction of processing when he contests the accuracy of the personal data, when processing is unlawful or when the controller no longer needs the personal data for the purposes of the processing.

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

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 shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is carried out by automated means and the processing is based on consent or on a contract. The Bank has set up a mechanism by which the data is provided to the data subject in a machine-readable format and delivered by e-mail.

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; in such situation the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests of the data subject or for the protection of legal claims; in addition, where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed. The Bank doesn't conduct direct marketing activities.

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, unless where such decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, where it is authorised by Union or Republic of Croatia law or where it is based on the data subject's explicit consent. The Bank doesn't adopt decisions based on automated decision-making nor does it profile.

Restrictions
Protection of personal data isn't an absolute right but one that needs to be balanced with other rights. Therefore, based on Union or Republic of Croatia law the controller or processor may restrict the scope of data subject's rights when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard significant values such as national security, defence, public security, other important objectives of general public interest for the Union or a Member State, protection of judicial independence and similar.
Any such legislative measure contains specific provisions as to the purposes of the processing or categories of processing, the categories of personal data, the scope of restrictions introduced, the safeguards to prevent abuse, the specification of the controller or categories of controllers and other aspects as to achieve protection of rights of natural persons.

Controller and processor

Obligations of the controller and of the processor
Taking into account the nature, scope, context and purposes of processing as well as its risks, the controller shall implement appropriate technical and organisational measures to ensure and to be able

to demonstrate that processing is performed in accordance with the Regulation. Those measures shall be reviewed and updated where necessary.

Data protection by design and by default

The Bank has implemented methodologies and processes which ensure for issues of privacy and protection of personal data appropriately addressed during the initial design and architecture of the systems which process personal data (*Privacy by design*).

Personal data processing system must be configured in a way that measures for privacy and protection of personal data are enabled by default with the objective of securing maximum privacy of the data subject (*Privacy by default*).

For each system where personal data is processed there is a written record which confirms that control over privacy and protection of personal data has been addressed while designing the system and that all relevant settings have been enabled by default. Possible exclusions of controls which ensure privacy and protection of personal data shall be documented and appropriately elaborated. Personal data protection officer must be acquainted with previously mentioned records and the same must be approved together with the head of Information security service.

Processor

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subjects.

The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the category of data subjects, and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor shall amongst other act on documented instructions from the controller, that natural persons authorised to process the personal data have committed themselves to confidentiality and that they shall act in accordance with the Regulation.

Records of processing activities

Controller maintains a record of processing activities under its responsibility. That record shall contain all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative 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;
- authorised persons which have access to the data;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of Regulation;
- basis for processing: legislative frame, legitimate interest, consent

Each processor and the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of the controller, containing:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- where possible, a general description of the technical and organisational security measures

Record is managed and kept up to date by the personal data protection officer, according to data provided from the authorized organizational units of the Bank. Record must be in written form, including electronical form.

Security of personal data

Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Notification of a personal data breach to the supervisory authority

Where it is likely for a data breach to result in a risk to the rights and freedoms of natural persons, the controller shall without undue delay after having become aware of it, notify the personal data breach to the supervisory authority (not later than 72 hours after having become aware of the breach). Supervisory authority is the Agency. Cited notifications must contain a description of the breach together with the information on the data subjects and personal data, description of likely consequences of such breach, description of measures undertaken or proposed to remedy the breach and controller's contact point. If a breach related to protection of personal data occurs, all employees of the Bank are obligated to immediately inform the personal data protection officer on such occurrence.

Communication of a personal data breach to the data subject

Where it is likely for a breach to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject. As an exception, this communication shall not be required if the controller has implemented appropriate protection measures for prevention of usage of personal data under breach, if the controller has taken subsequent measures following which high risk is not likely, or if contacting each data subject would involve disproportionate effort, where it is then necessary to inform the data subjects by public communication or other effective manner.

Data protection impact assessment and prior consultation

Data protection impact assessment

Where a type of processing is likely to result in a high risk to the rights and freedoms of data subjects, the controller shall undertake impact assessment.
A data protection impact assessment shall be required where personal aspects relating to natural persons are evaluated thru a systematic and extensive evaluation based on automated processing (profiling) / which the Bank doesn't perform /, where processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences (this doesn't include processing of politically exposed persons or processing of sick-leave confirmations by the Bank), and where a systematic monitoring of a publicly accessible area on a large scale is applied (this doesn't include video surveillance of Bank's exterior surroundings).

Impact assessment must contain a description of processing operations and their purposes, assessment of necessity and proportionality, assessment of risk and description of measures which mitigate the risk of processing.
Where the controller doesn't adopt measures for risk mitigation, if personal data protection impact assessment would show that processing will result with high risk then the controller must contact the supervisory authority and deliver to the same amongst other the information on the purpose and means of processing, protective measures, performed impact assessment, etc.
At this time the Bank doesn't carry out systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions would be based that produce legal effects concerning the natural person or similarly significantly affect the natural person; it doesn't carry out processing on a large scale of special categories of personal data; it doesn't carry out systematic monitoring of a publicly accessible area on a large scale, therefore there is no need for risk impact assessment.

Data protection officer

Designation of the data protection officer

The controller has designated a personal data protection officer. The officer is designated based on professional qualifications, and the ability to perform the following tasks:
(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the Regulation and other provisions of Union or Republic of Croatia law;
(b) to monitor compliance with the Regulation, with other Union or 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;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;
(d) to cooperate with the supervisory authority;
(e) 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;
(f) to enforce the provisions of this Rulebook;
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. Data protection officer is the person responsible for participation and involvement in all processes and all matters relating to personal data protection. In the context of the need to exercise data subject's rights, contact details of the data protection officer are:
Personal data protection officer, Međimurska ulica 28, 42000 Varaždin; Tel: 042 659-443; Fax: 042 659-491; e-mail: zastita.osobnih.podataka@jtbanka.hr