INFORMATION ON GATHERING DATA FOR CASH2GOLOAN

Pursuant to Regulation (EU) 2016/679 of the European Parliament and Council dated 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 (hereinafter: the Regulation), OTP banka d.d. (hereinafter: the Bank)) now shares information on the processing of your personal data as detailed below:

1 **Personal data gathered via the application or detailed in the Loan Application:**

a) Name and surname, taxpayer ID No., requested loan amount, currency and repayment period, number and place of issuance of ID, ID expiry date, date of birth, street and house number, postal code, town, municipality/city, county, e-mail, mobile number, marital status, number of household members, number of dependents, housing situation, professional qualifications, employment status, employer's name, taxpayer ID no. and registration no., type of employer, date of first employment, average net income for the past 3 months, alimony amount, applicant's existing credit commitments - loan type, role in these loans, total loan value, and amount of monthly commitments or total commitments over the past 60 days, are collected and processed by the Bank as mandatory information for identification and assessment of the client's creditworthiness to execute the loan agreement and perform other activities linked to finalising the agreement and meeting contractual obligations, supervising the regular repayment of the loan, enforced collection of the loan in case of default, along with potential sale of NPLs, all aimed at executing the contractual relationship with the data subject/client, and in accordance with legal bases such as: Credit Institutions Act, Consumer Credit Act, Housing Consumer Credit Act, Enforcement Act, Land Registry Act and the related secondary legislation.

b) Name and surname, taxpayer ID No, e-mail, mobile number, expiration date, and issuer of the ID are collected as processed by the Bank as mandatory information for the purpose of issuing a one-time certificate for signing a loan agreement with a qualified electronic signature. To furnish you with a one-time valid electronic signature certificate allowing you to electronically sign the agreement, the Bank shares your data with Namirial SpA, a company recognized as a qualified trust service provider under EU Regulation No. 910/2014 of the European Parliament and Council dated 23 July 2014o n electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) and on the basis of legitimate interest as the legal basis in accordance with the General Data Protection Regulation (Article 6(1)(f)) and the Consumer Credit Act.

The result of not supplying the requested data is the failure to establish a business relationship.

In this scenario, or when granting a Cash2go loan, the Bank utilizes automated individual decision-making, which is essential for the formation or execution of the agreement, and based on your application for a Cash2go loan.
Even though the choice in this instance is solely determined by automated systems without human involvement, the resulting decision does not generate legal consequences that pertain to you or impact you in a similarly significant manner, as you always have the option to take a loan from the Bank's alternative offers (including this product under identical conditions) by visiting a Bank branch, without the use of automated decision-making.

Please note that the Bank has implemented all required actions in line with the General Data Protection Regulation should your data be sent to third countries due to a specified maintenance and support service from a supplier with whom the Bank has a contractual partnership, all to guarantee an adequate level of protection of for your personal data.

Furthermore, we would like to inform you that Bank carries out the following data processing based on legitimate interest:

a) Data processing with purpose to protect persons, property, work environment and ensure safety of all persons in business premises of the Bank and external ATMs, including video surveillance and record of visitors.

b) Data processing with purpose to prevent and investigate fraud or other criminal offenses and all types of misuse of bank’s services.

c) Data processing with purpose of transparency, traceability and consumer protection, also including audio records.

d) Data processing with purpose of detecting the future difficulties of client in order to prevent failing of fulfilling his financial obligations in time and aiming timely and preventive reaction.

e) Data processing of contact data in order of giving the client important information form business relationship like system unavailability, loss of credit cards, card or account fraud attempting, in case of any kind of complaints, reaching agreement on debt settlement, etc.

f) Data processing with purpose of detailed analysis of credit exposure, including shared credit exposure of client and his/her spouse regarding the Bank, and processing related to requests for clients with high risk indicator (including suspicions of fraudulent activities) in the approval process of any transaction, in aim of minimizing manifestation of financial loss, and mitigating of potential operational, reputational and credit risk in order to improve long-term quality of credit and total portfolio of the Bank.

g) Data processing by reviewing client transactions related to games of chance for the purpose of risk management in loan operations.

h) Data processing of public information in order to perform debt recovery activities.

i) Data processing in terms of client segmentation with purpose to offer products and services to existing clients at Bank’s sales point, through bank’s service channels or inbound calls.

j) Data processing for purpose of direct marketing when the offer is made for equal or comparable products and services of the Bank that data subjects already use, considered by the Bank as better suited to the needs of certain categories of clients or intended as easier access or product /service management, as much as data subjects don't oppose this processing.
k) Data processing of official contact data related to natural person performing activities inside the business entities (Bank's clients/potential clients) in purpose of direct marketing which may include performing of surveys and questionnaires, etc.
l) Publishing adds of public auction with link to the official FINA site.
m) Data processing of branch usage, data of POS transaction usage, including POS location, amount and number of transactions, cash withdrawals on ATMs, including total amount, location and number of withdrawals, data of services payments, including type of payment, total amount of payment and number of transaction, data of deposits in Bank, incoming and outgoing transfers, investments in financial instruments, including payment method, total amount paid, and type of financial instrument, reasons of usage or non-usage regarding offered banking products. The purpose of data processing is establishment of advanced analytics client data analyzing, the probability of fund transfers out of the Bank, to perform client segmenting for better price adjustment categories of banking products and services. Data are being processed based on legitimate interest of Bank to improve our products and services. Processing of above-mentioned data helps us to understand in better way client's financial needs and habits in order to offer products and services with price conditions adjusted to client needs.
n) Processing/delivery of the debtor's contact information to the receivables buyer for the purpose of establishing communication with the debtor and optimizing the collection process.
o) Data processing through necessary (technical) cookies in order to provide the possible service and user experience for OTP bank website visitors.
p) Data processing that includes the transfer of client data to a third party in order to provide the service of issuing certificates in accordance with relevant regulations and standards in the field of application of electronic signatures and data security, in the online loan approval process.
q) Data processing for the purpose of resolving requests/complaints of individuals and preventing potential financial losses of the Bank, related to the process of accepting and replacing banknotes partially stained due to ink leakage from electrochemical protection on ATMs.

The Bank offers you the subsequent details regarding the processing of your personal data:

- The data controller responsible for your personal data is the Bank with the following contact info: OTP banka d.d., Domovinskog rata 61, 21000 Split, taxpayer ID No. 52508873833, info phone 0800 210021, e-mail: info@otpbanka.hr;
- Contact information for the Data Protection Officer of OTP banka d.d. is: Domovinskog rata 61, 21000 Split, email: zastita-osobnih-podataka@otpbanka.hr
- Your rights under the General Data Protection Regulation are as follows:

- the right to access personal data and detailed information about the processing of your personal data
- the right to rectification of data
- the right to erasure (right to be forgotten) of personal data
- the right to restriction of processing of personal data
- the right to data portability
- the right to object to the processing of personal data (including the right to object to processing based on legitimate interest)
- the right to object to automated individual decision-making, including profiling
- the right to file a complaint with the competent supervisory authority in the Republic of Croatia, the Personal Data Protection Agency, Ulica Metela Ožegovića 16, 10 000 Zagreb

All customers' personal data shall be treated as a bank secret and shall be used exclusively for Bank's requirements, save for the cases of keeping bank secrets referred to in Article 157(3) of the Credit Institutions Act:
1) where the client's consent is given that specific confidential information may be disclosed to another natural and/or legal person, provided that the consent may be
verified. To the extent that the confidential information involves personal data, the consent shall be given in accordance with the regulations governing the protection of personal data
2) where this enables the credit institution to realise its interest when exercising the sale of client's receivables
3) where confidential information is disclosed to the Croatian National Bank, the Financial Inspectorate of the Republic of Croatia or another supervisory or competent authority for the purposes of supervision or oversight within their competence
4) where confidential information is exchanged within a group of credit institutions for the purpose of risk management
5) where confidential information on clients is disclosed directly to another credit institution in accordance with Article 321 of this Act
5.a) where confidential information on clients is disclosed directly to another credit institution and/or financial institution or to a legal person which collects and exchanges information between credit and/or financial institutions, and the information is required for assessing client's creditworthiness or managing credit risk
6) where confidential information on clients who defaulted on their obligations is disclosed to a legal person who collects and disseminates such information among credit and/or financial institutions
7) where the disclosure of confidential information is essential for collecting and establishing facts in criminal or preliminary proceedings, when requested or ordered in writing by the competent court
8) where the disclosure of confidential information is necessary to carry out foreclosure or bankruptcy proceedings over the property of a client, legacy proceedings or other property-rights proceedings, and such disclosure is requested or ordered in writing by the competent court or public notary in the course of performing the functions entrusted to them pursuant to law

9) where the interests or obligations of a credit institution or its client require the disclosure of confidential information to establish the legal relationship between the credit institution and the client in court proceedings, arbitration proceedings or conciliation proceedings
10) where confidential information is disclosed to the Office for the Prevention of Money Laundering pursuant to the law governing the prevention of money laundering and terrorist financing
11) where confidential information is disclosed to the Office for the Prevention of Corruption and Organised Crime pursuant to the law governing the prevention of corruption and organised crime
12) where confidential information is required by the tax authorities (Tax Administration and Customs Administration) in procedures carried out within the framework of their competence under law, and is disclosed at their written request
13) where confidential information is disclosed to the Croatian Deposit Insurance Agency pursuant to the law governing deposit insurance
14) where the account balance reflects inability to effect payments and the certificate is requested to substantiate the existence of grounds for bankruptcy
15) disclosure of information to insurance undertakings within the procedure of insuring the credit institution's receivables
16) if disclosure of information in the course of concluding legal arrangements which have the effect of insuring the credit institution's receivables, such as derivative credit instruments, bank guarantees and similar arrangements
17) disclosure of information, subject to written consent of the credit institution's management board, to a holder of a qualifying holding in the credit institution, to a person intending to acquire a qualifying holding in the credit institution, to a person to whom the credit institution is merged by acquisition or with whom the credit institution merges by formation of a new credit institution, to a legal person intending to take over the credit institution as well as to auditors, legal and other experts authorised by a holder of a qualifying holding or a potential holder
18) disclosure of information necessary for the exercise of the credit institution's activities which are subject to outsourcing, where information is disclosed to the providers of outsourced activities
19) if a credit institution which provides services of storing and administering financial instruments for the account of clients, including custody services, discloses information on the holder of securities to a credit institution which is the issuer of these non-material securities at its request;
20) where confidential information is disclosed to social welfare centres at their written request, within the framework of their competence under law and for the purpose of taking measures to protect the rights of children (persons under 18) and persons under guardianship
21) where requested in writing by a State Attorney's Office of the Republic of Croatia or where a State Attorney's Office of the Republic of Croatia orders the Ministry of the Interior in writing to collect information in preliminary proceedings
22) where confidential information is disclosed to a co-debtor, pledgor, guarantor or another participant in the credit relationship, and only information on that credit relationship
23) where confidential information is disclosed at written request to a person who incorrectly paid funds to an account of a credit institution's client, and only information necessary to initiate court proceedings for the repayment of incorrectly paid funds
24) if the confidential information is provided to resolution bodies and the Ministry of Interior base on the Act on the Resolution of Credit Institutions and Investment Firms;
24.a) where confidential information is disclosed to the Single Resolution Board in accordance with Regulation (EU) no. 806/2014 and
25) where so provided in other laws.

Pursuant to the Credit Institutions Act, the bank must keep data for a minimum of 11 years following the conclusion of the year in which the business relationship ended.

Additional details regarding the processing of your personal data in line with the General Data Protection Regulation (EU 2016/679) can be found in the Data Protection Policy, accessible on the Bank's website www.otpbanka.hr www.otpbanka.hr and at any Bank branch, upon your request.

2 Information on the processing of personal information within the Basic Registry System among credit and financial institutions

Pursuant to Regulation (EU) 2016/679 of the European Parliament and Council dated 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 (hereinafter: the Regulation), we offer you this information to inform you about the potential processing of your data within the Basic Registry System (hereinafter: BRS system).

The BRS system facilitates the processing and exchange of customer data among credit and financial institutions that utilize the BRS system (hereinafter: users) through HROK to evaluate creditworthiness and/or manage credit risk.

For the purpose of the Regulation, users include both individual and joint controllers within the BRS system, and the company Hrvatski registar obveza po kreditima d.o.o. Zagreb, Ulica Filipa Vukasovića 1 (hereinafter: HROK) is, based on the circumstances, either their individual or joint processor.

Pursuant to Articles 13 and 14 of the Regulation, we inform you, as our client in the capacity of debtor, co-debtor, and/or guarantor, that we, as a user of the BRS system, process your personal data within the BRS system if you currently have, or have had, any financial obligation to us (including a loan, overdraft, card debt, or leasing contract, etc.) We process your information, including personal details, within the BRS system so that we can share data regarding your financial responsibilities with other users of the BRS system.

Objectives of processing and legal grounds for processing

The purpose of processing and sharing your personal data within the BRS system among credit and financial institutions using the BRS system is to evaluate your creditworthiness and/or to manage our credit risk concerning you, if you are our client or plan to become one.

The exchange of your data within the BRS system:

a) among credit institutions (banks, savings banks, and housing savings institutions) relies on adherence to the legal requirement (in line with Article 6, paragraph 1, item c) of the Regulation) outlined in Article 321 of the Credit Institutions Act, which governs the obligation to share data and information about customers among credit institutions for assessing creditworthiness and/or managing credit risk and
b) among credit and financial institutions, and financial institutions themselves relies on our legitimate interest, as well as the legitimate interests of all users (in line with Article 6, paragraph 1, item f) of the Regulation) to evaluate clients' creditworthiness (clients' capacity to meet their obligations systematically) to minimize and/or prevent the risk of bad loans and client over-indebtedness, as well as to manage credit risks associated with their clients, which is a regulatory requirement for the client.

Which of your data is processed within the OSR system?

The BRS system processes and exchanges the following categories of your data:

- identification data and
- information on current, settled, or otherwise repaid liabilities

<u>Identification data include:</u>

▪ Taxpayer ID No, name and surname
▪ Taxpayer ID No, name and registration number (if you engage in a business activity)

<u>Information on current, settled, or otherwise repaid liabilities (pecuniary obligations) is:</u>

▪ type of liability,
▪ total amount of the liability,
▪ capacity in which you participate in the liability (debtor, co-debtor and/or guarantor)
▪ amount and frequency of the annuity/instalment/payment,
▪ regular settlement of liabilities,
▪ number of outstanding liabilities,
▪ amount of outstanding liabilities
▪ DPD.

How, why and when is your data processed within the OSR system?

Your data is processed by supplying and saving information in the BRS system and by sharing this information among BRS system users at an individual user's request when evaluating creditworthiness and/or managing credit risk.

Consequently, we, similar to other BSR system users, provide updated client personal information to the BRS system every month.

We can request an exchange just like other users when we evaluate your creditworthiness and/or when we manage or another user manages credit risk related to you. In line with the request, any details concerning your financial liabilities kept in the BRS system at the time of the request are shared and consolidated, resulting in a BRS report generated from the data in the BRS system.

If the BRS system lacks information regarding your financial liabilities, a notification is created rather than a report indicating that there is no data available for you in the BRS system.

How does data processing within the BRS system affect you?

The information in the report, derived from the data exchange concerning your financial liabilities in the BRS system, could impact our business decisions involving you, particularly those where your creditworthiness is important and in matters related to credit risk management associated with you.

How long do we keep your personal data?
In the BRS system, information regarding your financial liabilities that are not older than 4 (four) years is kept and shared. Once your financial liability is completely paid off or otherwise settled, your information will be kept for up to 4 (four) years from the date the financial liability is fully paid off or otherwise settled.

Who receives your personal data?
Only users of the BRS system who have made a request for data exchange receive data from the BRS system, and these users receive either a report detailing your financial liabilities or a notice indicating that no data on your financial liabilities exists in the BRS system. Indirectly, the recipient is also HROK as the processor in the BRS system.

The current list of BRS users is published on the website www.hrok.hr/osr-korisnici.

Your rights

Should your data be processed in the BRS system, you have the right to request us, as the data controller, to exercise any of the following rights:

a) Right to access personal data

Concerning the data processed in the BRS system, you can ask for verification of whether your personal data is being processed and obtain a copy of the personal data if it is being processed.

b) Right to rectification

If you think the information processed in the BRS system is incorrect or lacking, you may ask for the data to be corrected or completed.

c) Right to erasure ("right to be forgotten")

You are entitled to invoke the right to erasure of personal data if any of the subsequent conditions are met:
▪ The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
▪ You have contested the processing, and your legitimate reasons for erasure take precedence over our legitimate interest in the processing (as well as the legitimate interest of other users);
▪ The personal data are not processed lawfully or the personal data must be erased to comply with a legal requirement.

The right to erasure according to the Regulation is not applicable, even if one of the aforementioned conditions is fulfilled, if the processing is essential for the execution of the right to free expression and information; for fulfilling a legal obligation that necessitates processing under Union or Member State law applicable to the user or for carrying out a task performed in the public interest or in the exercise of official power granted to the user; for public interest archiving, for scientific or historical research, or for statistical objectives in line with regulations; for the creation, exercise, or defence of legal claims.

d) Right to restriction of processing

You can invoke the right to restrict processing if any of the subsequent conditions apply:
▪ You contest the accuracy of the personal data for a period enabling the Bank to verify the accuracy of the personal data;
▪ The data processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
▪ The user no longer needs the personal data for the processing purposes, but you seek them for the establishment, exercise or defence of legal claims;
▪ You have objected to the processing under Article 21 (1) of the Regulation while awaiting verification of whether the user's legitimate interests take precedence over your reasons.

e) Right to object

In the segment where your personal data is processed and shared within the BRS system based on legitimate interest, and according to Article 21, paragraph 1 of the Regulation, you have the right to object, on grounds relating to your personal situation, to the processing of your personal data at any time, which would supersede both our legitimate interest in processing your data in the BRS system and the legitimate interests of other users in processing that data.

Please note that your objection to the processing and sharing of your data in the BRS system based on legitimate interest does not affect the processing and sharing of your data in the BRS system in the segment where such processing and sharing is compliant with a legal obligation that credit institutions hold under Article 321 of the Credit Institutions Act, as it pertains to the processing and sharing of data for purposes of fulfilling a legal obligation according to Article 6, paragraph 1, item c) of the Regulation.

Moreover, every individual whose personal information is processed in the BSR system has the right to object to processing of their personal data with the supervisory authority, specifically the Personal Data Protection Agency.

Important: When you submit a request to exercise your rights, please include your taxpayer ID no., full name, or the description of the business activity along with the registration number of the business entity.

You may exercise the aforementioned rights by submitting a request that clearly identifies you as a client, in writing personally or through a representative at any customer branch, or you can send it by mail to OTP banka d.d., Domovinskog rata 61, 21000 Split, or via email to info@otpbanka.hr.

You can also send a written request to Hrok d.o.o. to exercise your right to access personal data at the address Filipa Vukasovića 1, 10000 Zagreb, on the condition that the request includes your signature verified by a notary public in the Republic of Croatia or at a diplomatic or consular office of the Republic of Croatia.

For any inquiries or feedback concerning the processing of your personal data in the BRS system, please reach out to our Data Protection Officer via email at zastita-osobnih-podataka@otpbanka.hr or in writing to OTP banka, Domovinskog rata 61, 21000 Split.

Additional details regarding the processing of your personal data in line with the Regulation can be found in the Data Protection Policy, accessible on the Bank's web site Data Protection | OTP bank d.d. and at any Bank branch, upon your request.

All client personal data is treated as a bank secret and is used exclusively for Bank’s purposes, save for the cases outlined in the Credit Institutions Act.