HNB
EUROSUSTAV

Trg hrvatskih velikana 3, HR-10000 Zagreb
Phone: +385 1 4564 555 · Fax: +385 1 4610 551
www.hnb.hr

PRIVACY STATEMENT

– for payment service users regarding services contracted with reporting entities –

Controller

The Croatian National Bank, Trg hrvatskih velikana 3, Zagreb, OIB: 95970281739 (hereinafter referred to as 'CNB'), processes the personal data of payment service users: the personal identification number of a payment service user, the number of cards held by the payment service user, information on whether the payment service user has a transaction or another payment account opened in the territory of the Republic of Croatia (hereinafter referred to as 'RC'), whether the payment service user has contracted the service of Internet banking, e-account, mobile banking, standing order, direct debit and telebanking and the information on whether the payment service user has contracted the service of acquiring of payment transactions through an accepting device – EFTPOS terminal and/or the Internet.

Source of the collection of personal data

Once a year, the CNB collects personal data from reporting entities, which include credit institutions with head offices in the RC, payment institutions and electronic money institutions with head offices in the RC and branches of the mentioned entities from a third country or from a state signatory to the Agreement on the European Economic Area with head offices in the RC (hereinafter referred to as 'reporting entities').

The CNB does not collect personal data directly from consumers – users of payment services, that is, from natural persons and craftsmen; it collects them indirectly from the reporting entities. The reporting entities collect personal data directly from consumers, that is, from natural persons and craftsmen when establishing or exercising contractual relationships (e.g. contract on the opening of a current account, contract on a deposit, etc.).

Purpose and legal basis of the processing

The CNB processes personal data for the purpose of obtaining accurate information on the number of payment service users that have payment accounts opened with reporting entities, the type of payment accounts the payment service user has opened, the precise number of payment cards, the type of the individual service used by the payment service user and whether the payment service user has contracted the service of acquiring payment transactions through an accepting device – EFTPOS terminal and/or the Internet, as well as for the purpose of collecting payment statistics and preparing publications in the area of payment operations.

The personal identification number of payment service users as information that is collected is required since a single user may have several payment cards with a number of reporting entities. Therefore, for the purpose of obtaining the information on the number of cards held by the individual payment service user, it is necessary to match the collected data at the level of the whole reporting system obtained from all reporting entities. The data on the types of services (Internet banking, e-account, mobile banking, standing order, direct debit and telebanking) used by individual payment service users are matched in

the same manner, as well as the data on whether the payment service user has contracted the service of acquiring payment transactions through an accepting device – EFTPOS terminal and/or the Internet.

Article 86, paragraph (1) and Article 89, paragraph (1), item (5) of the Act on the Croatian National Bank[1], which prescribe the collection and processing of data for statistical purposes as one of the CNB's tasks of public interest, constitute the legal basis of the processing.
Therefore, the legal basis is Article 6, paragraph (1), item (e) of the General Data Protection Regulation[2].

In order to fulfil the mentioned purpose, aggregated data on payments statistics are not sufficient to the CNB. Specifically, the aforementioned data collection enables the presentation of the habits of consumers, that is, of natural persons and craftsmen in using payment services and it serves for the purpose of preparing publications in the area of payment operations.

Categories of personal data processed by the CNB

In the course of reporting, the reporting entities submit to the CNB the following personal data:

- ✓ personal identification number (hereinafter referred to as 'OIB') of the payment service user;
- ✓ the number of cards held by the OIB holder;
- ✓ data on whether the payment service user has opened a transaction or another payment account;
- ✓ the type of services the payment service user is using at the reporting entity (Internet banking, e-account, mobile banking, standing order, direct debit and telebanking);
- ✓ data on whether the payment service user has contracted the service of acquiring payment transactions through an accepting device – EFTPOS terminal and/or the Internet;
- ✓ details of the responsible person (employee) in the reporting entity who is sending the report (name, surname and contact details: e-mail and/or phone number).

Data subjects whose data are collected are natural persons that have opened payment accounts with reporting entities, they are holders of payment cards and users of services provided by reporting entities. The data are submitted annually for 31 December for all payment service users in the RC.

Personal data that will be processed do not fall within the special categories of personal data, but they are the data of sensitive nature since they refer to the individual payment service user, the total number of cards per user of payment services and the type of service used by the individual payment service user with the reporting entity.

Mechanisms for the protection of personal data at the CNB and the recipients of personal data
Reporting entities protect the files in which they submit the requested data with passwords and submit the protected files to the CNB in accordance with the instructions received from the CNB.

The CNB does not transfer the collected data to third persons or disclose them in the form in which it is possible to identify the person. The reporting entity does not have insight into the data submitted by

[1] The Act on the Croatian National Bank (Official Gazette 75/2008, 54/2013 and 47/2020).
[2] General Data Protection Regulation – 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, OJ EU L119, in force since 25 May 2018.

another reporting entity. Access to the database is only granted to CNB employees who need access to perform their work and tasks, i.e., those to whom the need-to-know principle applies.

Persons that have the right of access to the data cannot identify the payment service user without additional information (key) because the data are pseudonymised in the CNB system. Therefore, the data cannot be used for other purposes that are not related to the preparation and publishing of publications in the area of payment operations.

The CNB does not transfer the personal data to third countries or international organisations and does not carry out profiling or automated decision making.
The rights of access are managed at several levels:

- ✓ control of the right of access to the CNB premises by means of the individual card for entry/exit and control of the entry/exit carried out by the security service (access of third persons that are not CNB employees or in another form of contractual relationship with the CNB must be announced in advance and such persons are identified at entry to the CNB premises);
- ✓ control of the right of access to the computer and the CNB information system (on computers located in the CNB business premises or on official laptops) by means of the individual employee card and a specific password;
- ✓ control of the right of access to the database concerned by using a specific user name and password;
- ✓ monitoring access to data with a potential identification of the person making unauthorised access or unintended changes or erasure of data;
- ✓ storage of data exclusively within the CNB, on CNB servers in a pseudonymised form;
- ✓ technical measures to protect the equipment and premises against unintended access or damage caused by external conditions (weather adversities, fire, etc.);
- ✓ regulatory measures – rules on personal data protection prescribed by the internal ordinance governing the protection of personal data.

Keeping personal data

The data are stored for seven (7) years.

The control of the right of access to the database concerned by means of a specific user name and password prevents unauthorised access to data. Access to data is constantly monitored with the possibility to identify the person making an unauthorised access or unintended changes or erasure of data. When loading data, the collected OIBs are pseudonymised and entered in the database.

Rights of persons whose data are processed

In accordance with the conditions of the General Data Protection Regulation persons whose data are processed have the following rights: a) the right to information in relation to the processing of and access to personal data, b) the right to rectification, c) the right to restriction of personal data processing and d) the right to object. The forms prepared in order to facilitate the exercise of these rights may be downloaded from the CNB website (link: https://www.hnb.hr/en/protection-of-personal-data).

In a specific case, the CNB processes personal data for the purpose that does not require the identification of the person (data subject). Since for the purpose of exercising the mentioned rights of individuals the CNB should process additional information (unnecessary to the CNB) to identify the

individual, in accordance with Article 11 of the General Regulation, the mentioned rights are not applied, unless the specific individual provides additional information enabling the identification for the purpose of exercising the rights.

If an individual requests the exercise of rights with respect to the processing of personal data carried out by the reporting entity (from whom the CNB has received personal data) in the course and for the purpose of exercising contractual relationships with a client (for example, the rectification of the number of payment cards), then the individual should address the request to that reporting entity because the CNB does not influence the processing of personal data within the business relationship of the reporting entity and the individual.

Data protection officer and supervisory authority

Any complaints regarding CNB actions in connection with your personal data processing should be addressed to the Croatian Personal Data Protection Agency (AZOP), Metela Ožegovića 16, Zagreb, the supervisory authority responsible for personal data protection in the RC.

For more information on this topic, visit the CNB website at https://www.hnb.hr/en/protection-of-personal-data. All queries should be addressed to the CNB data protection officer (sluzbenik.osobni@hnb.hr).