GDPR packet

for corporate customers

mBank.pl

Table of content

GDPR – general information

We will start applying GDPR (General Data Protection Regulation) as of 25 May 2018.

Full name: 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.

What is the objective of GDPR?

GDPR introduces and harmonises the principles of personal data processing throughout the European Union. In particular, it promotes the security of personal data and protects the right to privacy.

Brief glossary of terms

Controller – means a person or entity who (either alone or jointly with other controllers) determines why and how to process personal data. The controller of customers' personal data is mBank S.A. with its registered office in Warsaw.

Processor – means a natural person or entity that processes personal data on behalf of the controller.

Personal data – means information that identifies (or allows to identify) a natural person (also referred to as the "data subject" or "customer"). This will include in particular the full name, type, series and number of the identity document, address, telephone number, e-mail address, date of birth, PESEL (Personal ID No), Tax ID No (NIP), Statistical ID No (REGON), video surveillance pictures, etc.

Personal data processing – means activities relating to personal data. They may be carried out automatically or manually. Data processing occurs when data: are collected, recorded, organised, structured, stored, adapted or altered, retrieved, consulted, used, disclosed (e.g. by transmission), disseminated or otherwise made available, aligned or combined, restricted, erased or destructed.

How does our Bank communicate with customers?

With regard to all issues, including personal data, we communicate with our customers: via the website, electronic banking systems, e-mail, telephone and mail as well as corporate branches.

Contact details of mBank:

Head Office and Management Board of mBank:
ul. Senatorska 18, 00-950 Warszawa, skr. poczt. 21
tel. (22) 829-00-00,
website: www.mbank.pl

Correspondence addresses of corporate branches of mBank:

https://www.mbank.pl/placowki-bankomaty/#msp-i-korporacje_placowki

Basic principles of GDPR

GDPR sets 6 principles of personal data processing that our Bank follows when processing personal data of customers. These include:

- principle of lawfulness, fairness and transparency: we process personal data in a lawful manner. We inform customers in detail about all issues related to this matter using specified communication channels and the simplest language so that they are aware that we collect, store or otherwise process their specific personal data;
- principle of data minimisation and adequacy: we process such data (adequate, relevant) that are indeed needed to achieve a given objective;
- principle of data accuracy: we take utmost care to ensure that the data we process are true, up-to-date and accurate. That is why, every so often, we can ask customers to check and update their data. We ask them to inform us about any changes in their personal data (full name, address, etc.);
- principle of limiting the purpose and storage of processed data: personal data of customers are only collected for specified, explicit and legitimate purposes that we could not achieve otherwise. We store data in a form that allows the data subject to be identified. We process them only as long as it is necessary to achieve the purpose for which we have obtained them (unless we are obliged to their further processing by law);
- the principle of data integrity and confidentiality: we provide such IT and organisational solutions that the personal data we process are safe. We protect data against unauthorised or unlawful processing and against accidental loss, destruction or

damage;

- principle of accountability: we are able to demonstrate, in a way required from us by law, that with regard to personal data, we are acting in accordance with law, we take into account data protection in the design phase (e.g. of a new product) and ensure the default protection of personal data.

How do we process personal data – basic information

What data do we process and on what basis?

We process personal data. Personal data means information that identifies (or allows to identify) the data subject. We most often process data such as:

- full name;
- other identification data: PESEL (personal ID) number, date of birth, address, e-mail, telephone number;
- Tax ID No (NIP);
- Statistical ID No (REGON);
- type, number and series of identity document;
- video surveillance records;
- other data needed to enable us to offer products and services.

Personal data may be processed if:

- the data subject has consented to it; on that basis we process data when we do marketing of products or services of entities other than our Bank and entities belonging to our capital group (marketing of our services and of entities belonging to our capital group does not require consent);
- we are doing it to examine applications and to perform agreements between us and the data subject, including when:
    - we calculate the customer's creditworthiness to examine a credit application;
    - examine customers' applications for other banking products (accounts, deposits, etc.);
    - we are processing complaints;
- we meet legal obligations in this way; on this basis, we process customers' data in order

to prevent fraud and ensure security of business operations. We are required to meet specific obligations in line with legal provisions such as the Banking law; Act on anti-money laundering and terrorist financing or Act on Trading in Financial Instruments;

- it is required by our (controller's) legitimate interest, i.e. in situations where:
    - we build an accurate and secure risk model for the loan portfolio, assessing the creditworthiness of customers;
    - we do direct marketing of our Bank's products or services and of entities belonging to our capital group (see full list at https://www.mbank.pl/o-nas/informacje-wymagane-przepisami-prawa/);
    - we establish and exercise legal claims or defend ourselves against them;
    - we prepare statistics and internal reports;
    - we build our statistical and operational risk assessment models;
    - we survey customer satisfaction;
    - we prepare or change our offer, operational plans and the Bank's strategy;
    - we sell receivables;
    - we archive data;
    - we prevent and detect crime (we care about security).

Where do we get the data we process?

We process data that the customers provide us with in forms, e.g. when they open an account or apply for a loan, data submitted during meetings with the Bank's employees (e.g. business cards). We can also use the data that other controllers provided us with (e.g. Biuro Informacji Kredytowej S.A. – Credit Information Bureau) or that we obtained from publicly available databases (e.g. Central Registration and Information on Business).

Disclosure obligations towards customers (data subjects)

All information on personal data protection is available to our customers at all times on our website www.mbank.pl/rodo. We are also happy to answer all questions asked by the customers. We provide individual information in two cases: when we collect data or when we change the purpose of their processing.

When do we inform our customers?

If we collect data directly from the data subject, we provide them with such information immediately. When the data originate from another source, we inform the data subject:

- within a reasonable time, no later than one month from the collection of the data;
- at the latest, when we first communicate with the data subject (if we use the data when communicating with that person);

unless informing them proves impossible or it would require a disproportionate effort.

How do we inform our customers?

We can provide this information:

- in the information clauses included in documents intended for the data subject or in electronic banking systems;
- either personally or by telephone, in the course of a conversation with the Bank's representative;
- electronically, including by publishing this information on our website.

What are the rights of data subjects and how do we respect them?

Right of access to data

The data subject is entitled to obtain information about whether we process their personal data. The data subject is entitled to know:

- why we process certain data;
- what types of data are processed;
- to what recipients or categories of recipients have we disclosed (or may disclose) their data – this regards in particular recipients in countries other than the member states of the European Economic Area or international organisations;
- how long do we plan to process their data (if we can define a timer period) or on the basis of what criteria, do we establish that period.

In order to obtain access to their personal data, the customer must provide us with an appropriate request submitted at a corporate branch. We provide answers in writing within the time limits set

out in GDPR.

Right to rectification

The data subject may request that we rectify their inaccurate personal data without undue delay or complete incomplete data.

In order to rectify the data of the data subject, we need to obtain a request from them, filed at a corporate branch, that will specify the scope of the rectification. We provide answers in writing within the time limits set out in GDPR.

Right to erasure (right to be forgotten)

The data subject may request that we erase their data when:

- the data are no longer necessary in relation to the purposes for which we collected them;
- the data have been processed in violation of GDPR or other laws;

In order to erase the data of the data subject, we need to obtain a request from them, filed at a corporate branch, that will specify their demands. We will take them into account if, in our opinion, we do not have legally justified grounds to continue processing the data. We provide answers in writing within the time limits set out in GDPR.

If we erase the data of a customer, we have the right to keep information about the person at whose request we did it.

Right to restriction of data processing

The data subject may also request that we restrict the processing of their data. This right concerns the following cases:

- the accuracy of the personal data is contested by the data subject;
- the data subject is of the opinion that we process their data unlawfully and requests the restriction of their use (but opposes their erasure);
- we no longer need the personal data to achieve the intended objective, but the data subject opposes their erasure because they need them for the establishment, exercise or defence of legal claims;
- the data subject wishes to object on grounds relating to their particular situation (when we process the data on the basis of our legitimate interest).

It may happen that we will process data, despite a request of the data subject to restrict the processing of their data. This is particularly the case when we are establishing, exercising or defending ourselves against legal claims.

In order restrict the processing of their personal data, the customer must provide us with an appropriate application submitted at a corporate branch. We provide answers in writing within the time limits set out in GDPR.

Right to data portability

Every data subject shall also have the right to data portability. We shall transmit the data directly to the customer or, additionally, to the controller designated by the customer.

In order to transmit the data of the data subject, we need to obtain an appropriate request from them, filed at a corporate branch. We will transmit the data in an encrypted e-mail within the time limits set out in GDPR.

Right to object to processing

The data subject may object to our processing of their personal data that is based on our legitimate interest. The applicant shall each time indicate to us to what specifically they are objecting. In particular, customers are entitled to object to the marketing of the Bank's products and services and of companies from our capital group.

The data subject who wishes to exercise their rights may submit a request at a corporate branch. In this request, the data subject shall indicate the data that will enable us to identify them, namely:

- full name,
- PESEL (Personal ID) number,
- type series and number of identity document,
- correspondence address (street, house/apartment No, city, postal code, country),
- Statistical ID No (REGON) and Tax ID No (NIP) (in the case of a natural person conducting business activity),
- e-mail addresses and mobile phone numbers that the customer uses or has used in contacts with us,
- whether and what agreements the customer has concluded with our Bank (has or had in the past).

Customer requests shall be executed within the time limits set out in GDPR.

Rules of conduct regarding personal data breaches

A personal data breach occurs when, accidentally or unlawfully, the controller destroys, loses, alters, discloses or provides access to personal data.

Who and when will we inform in case of a breach at our Bank?

Data subject	if we have estimated the risk to the rights and freedoms as **high**;	without undue delay (should it be very difficult to provide direct information, we will issue a public statement).
Supervisory authority	if we assess – with a probability **higher than low** – that there was a risk to the rights and freedoms of natural persons;	without undue delay, as far as technically feasible, no later than 72 hours after the occurrence of the breach.

To whom and for what purpose can we transmit customer data?

In accordance with the law, we can transmit customer data to other institutions in order to conclude and perform agreements with customers and to meet statutory obligations. In particular, we transmit customer data to the following institutions:

- The Polish Bank Association, the controller of the database "Banking Register System" (BR);
- Credit Information Bureau (BIK). More information at www.mbank.pl/rodo;
- business information bureaus;
- banks (customer inquiries – Article 105(1) of the Banking law);
- entities with whom we have concluded outsourcing agreements in the manner resulting from the Banking law (they are, in particular, our credit intermediaries or courier companies providing documents to customers), their full list is available at https://www.mbank.pl/o-nas/informacje-wymagane-przepisami-prawa/. The following

file is to be opened: “Informacje o przedsiębiorcach zgodnie z art.111b ustawy Prawo bankowe” (Information on entrepreneurs in line with Article 111(b) of the Banking law act);

- SWIFT – the Society for Worldwide Interbank Financial Telecommunication (under the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program);
- entities of mBank Group, Commerzbank AG and entities belonging to Commerzbank Group – only with the consent of the customer – Article 104(3) of the Banking law.

The data collected by BR and by BIK may be made available to:

- other banks,
- financial institutions operating as subsidiaries of banks,
- other entities authorised by law,
- business information bureaus.

Rules for transmitting data outside Poland

Personal data can be transmitted to entities (of course, when there are grounds for doing so) from the European Economic Area (EEA). EEA consists of member states of the European Union Iceland, Norway and Liechtenstein. We can transmit personal data to a third country (outside EEA) if it guarantees at least the same data protection as that in force in Poland. In practice, such a guarantee is the fact that the country has been recognised by the European Commission as a country that provides adequate protection.

We can transmit personal data to other third countries without the consent of the authority supervising the personal data protection in Poland if we have applied special arrangements in agreements with entities from these countries, as provided for by law or approved by the authority supervising the personal data protection in Poland.

Access to personal data can exceptionally be obtained by the government administration of the United States of America, because we execute foreign transfers through SWIFT (Society for Worldwide Interbank Financial Telecommunication). The U.S. authorities have obliged themselves to using these data solely in the fight against terrorism (respecting the guarantees provided by the European personal data protection system).

Personal Data Inspector at mBank

We have appointed a Personal Data Protection Officer - Agata Rowińska who is responsible for compliance with data protection regulations at our Bank.

Contact with the Personal Data Inspector:

- by e-mail: Inspektordanychosobowych@mbank.pl
- by post to:

  Personal Data Inspector
  mBank S.A.
  ul. Senatorska 18, 00-950 Warsaw

How can the customers complain about the protection of their personal data?

If a customer suspects that their data are being processed in breach of GDPR, they may lodge a complaint with the supervisory authority for the protection of personal data as indicated on the website of the supervisory authority at www.giodo.gov.pl

How long do we process data?

We process customer data for as long as is necessary to achieve the purpose of the processing. Specific periods are indicated in the documentation provided to customers.

We apply the principle of restricting the storage of personal data, which safeguards data against being processed for an unlimited period of time. When we achieve the purpose of processing, we erase the data or make them anonymous (their recovery is then impossible). There are cases where we need to store data because of separate regulations (e.g. in order to carry out tasks relating to crime prevention). In particular, we erase or make customer data anonymous when:

- the customer withdraws their consent to the processing of personal data (if their consent was the ground for processing);
- the data subject expresses an effective objection to further processing (if the Bank's legitimate interest was the ground for processing);

- any legal claims lapse (if the data were processed for the purpose of executing an agreement);
- the time limits laid down in other regulations, e.g. in the Accounting Act, Act on anti-money laundering and terrorist financing, etc., have expired.

Useful documents and information

- www.mbank.pl/rodo
- the Office for Personal Data Protection website www.uodo.gov.pl/en
- GDPR text: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679