GDPR Pack
for corporate clients

mBank.pl

Table of contents

GDPR – General

GDPR
(General Data Protection Regulation) applies since 25 May 2018.

Its full name is: 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 purpose of GDPR?

GDPR introduces and unifies the principles of personal data protection across the European Union. In particular, it ensures safety of personal data and protects the right to privacy.

Glossary:

Controller	means the person or entity which (alone or jointly with others) determines the purposes and means of the processing of personal data. mBank S.A. with its seat in Warsaw is a personal data controller.
Personal data	means any information relating to an identified (or identifiable) natural person (known as 'data subject'), including: first name and surname, client ID, address, phone number, date of birth, credit history, bank account number, tax ID (NIP), personal ID (PESEL), salary, image recorded by a visual monitoring system image or during a video call, voice, etc.
Processor	means a person or entity which processes personal data on behalf of and for the controller.
Profiling	means automated processing of personal data which uses personal data to evaluate certain personal aspects relating to a client.
Processing	means any operation on personal data, either automated or manual. We process data whenever we collect, record, organise, structure, store, adapt or alter, retrieve, consult, use, disclose (e.g. transmit), disseminate, align or combine, restrict, erase or destroy data.
Data subject	means the bank's client, prospective client, client's representative, client's proxy, beneficial owner, members of companies' authorities.

How do we communicate with data subjects?

We communicate with data subjects on all matters, including personal data, via our website, transaction service, by email, phone/video and mail, and at our branches. The agreement with each client specifies the agreed forms of communication.

mBank's contact details

- **mBank Head Office and Management Board**
  ul. Prosta 18, 00-850 Warsaw
  Phone (22) 829 00 00

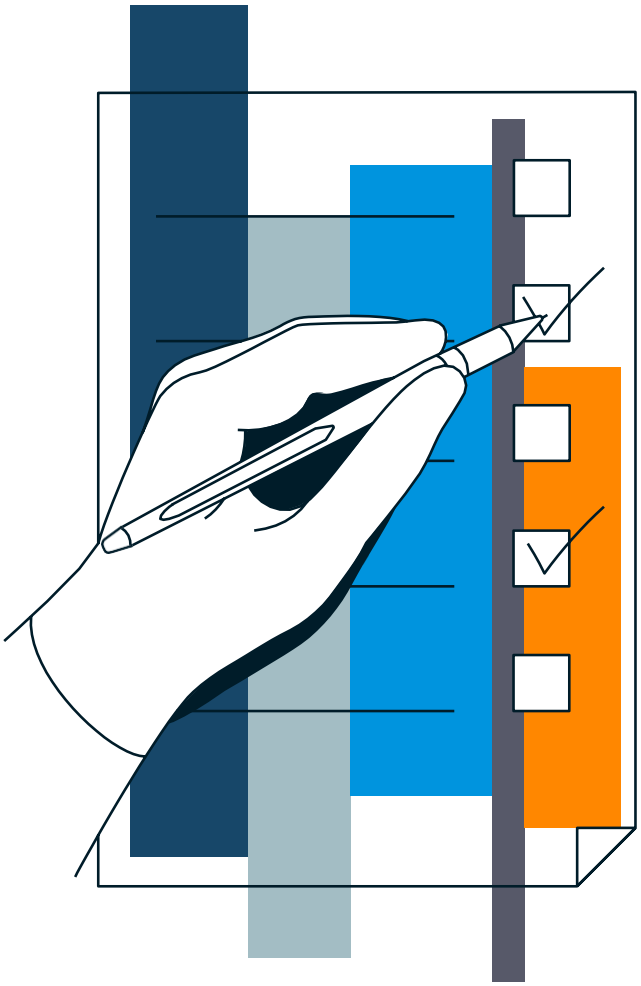
- **Corporate Client Centre:**
  Phone 801 273 273

www.mbank.pl

GDPR principles

GDPR defines six principles of data processing which our bank follows whenever we process personal data. These principles include:

- **lawful, fair and transparent processing:**
  we process personal data in accordance with the law. We communicate all related matters exhaustively via the agreed communication channels in a simple language to make sure that the data subjects understand that we collect, store or otherwise process their personal data;
- **data minimisation and adequate processing:**
  we only process data which are really necessary (adequate) to achieve a purpose;
- **data accuracy:**
  we make best efforts to ensure that the data we process are true, up to date and accurate. This is why we may ask data subjects from time to time to check and update their data. We also ask clients to let us know of any changes to their personal data (first name and surname, address, etc.);
- **purpose limitation and storage limitation:**
  we only collect personal data for specified, explicit and legitimate purposes which could not be achieved otherwise. We store data in a form which permits identification of data subjects. We process personal data for no longer than is necessary for the purposes for which the personal data are collected (unless we are required by law to continue processing);
- **integrity and confidentiality:**
  we use appropriate technical or organisational measures to ensure security of processed data. We protect data against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- **accountability:**
  we can demonstrate (as required by law) that we process personal data lawfully, use data protection by design (e.g. in product development) and data protection by default.



How do we process personal data? – General

What data do we process, and on what basis?

We process general and special personal data.

We typically process general data, including:

- first name, middle name, surname;
- other identification details: gender, PESEL, data, city and country of birth, address of residence, mailing address or registered address, email, phone number;
- client identifier (client ID);
- tax identifier (NIP or tax ID in a jurisdiction other than Poland);
- statistical number REGON;
- data concerning our communications;
- series and number of the client's identity card/passport/permanent residence card/other identity document, its date of issue and expiry date;
- we record images when monitoring the bank's premises or during video calls in the process of establishing business relationships or providing day-to-day service;
- cookies, which are processed according to the mBank Cookies Policy available at https://www.mbank.pl/o-nas/o-mbanku/polityka-prywatnosci.html;
- other data necessary to achieve the purpose of processing;
- information on employees' powers of attorney and authorisations to represent the counterparty;
- numbers of ID cards and documents confirming the authorisations granted.

We may process personal data provided that:

- **the data subject has given his or her consent:**
  we process data on that basis for the purposes of marketing of products and services of providers other than the bank and our group members (marketing of services of the bank and our group members requires no consent) or during phone calls or video calls;
- **we process applications and perform agreements between us and the data subject, including whenever we:**
  - determine creditworthiness to process a loan application;
  - process applications for bank products (accounts, deposits, etc.);
  - process complaints;
- **we comply with a legal obligation:**
  we process data on that basis in particular to prevent fraud and protect security of transactions. We are subject to specific legal obligations under the Banking Law, the Act on Anti-Money Laundering and Combatting the Financing of Terrorism, the Act on Trading in Financial Instruments, the Accounting Act, the General Tax Law, the Act on Financial Market Complaints Processing and the Financial Ombudsman, the Payment Services Act, the Act on the Treaty between the Government of the Republic of Poland and the Government of the United States of America to Improve International Tax Compliance and to Implement FATCA, the Act on Exchange of Tax Information with Other States (CRS);

- **for the purposes of our legitimate interests, i.e. whenever we:**
  - develop an adequate and secure risk model for a loan portfolio and rate creditworthiness;
  - engage in direct marketing of products and services of our bank and our group members (the full list is available at https://www.mbank.pl/o-nas/grupa/);
  - establish, enforce or defend claims;
  - generate statistics and reports;
  - develop, monitor and change internal methods as well as methods and models in response to prudential requirements including operational risk;
  - survey customer satisfaction;
  - develop or modify our offer and the bank's operating plans and strategy;
  - sell debt;
  - keep data records;
  - prevent and detect crime (protect security).

Special personal data:

With the consent of the data subject, we process information provided by the data subject concerning:

- disability – we do so in order to prepare our services for the needs of clients with disabilities (e.g. hard of hearing, with vision impairments);
- health and life situation.

Where do we get the data we process?

We process data provided by data subjects in forms, e.g. when opening an account, applying for a loan, or communicating at meetings with bank employees.

We may also use data transmitted by other controllers (e.g. Biuro Informacji Kredytowej S.A., the Ministry of Finance, law enforcement services), data we source from public databases (e.g. Central Business Register CEIDG, National Court Register KRS), and data we receive from third-party providers under contract or from our clients in the performance of legal obligations.

Data profiling

Data profiling means that we use algorithms or mathematical models to analyse clients' features, preferences, and future behaviour. We use the appropriate (technical and organisational) measures to mitigate the risk of error in profiling.

We use best efforts to ensure that our assessment is objective and our processes are non-discriminatory. Our statistical models comply with the good practice of the banking industry (including Recommendation W of the Polish Financial Supervision Authority KNF).

Why do we use profiling?

We use profiling to discharge our legal obligations:

- we protect the security of assets and transactions;
- we prevent money laundering and financing of terrorism, we develop models to recognise such crime;
- we decide which products and services do not match the needs of customer groups and we do not offer them in order to protect clients from misselling of financial products;
- we verify clients' investment expertise and experience (to decide whether a brokerage or investment service is appropriate for a client);
- we monitor the quality of granted loans in order to manage the risk of retail credit exposures effectively.

We use profiling whenever necessary to conclude or perform a contract:
when a client applies for a loan or for modification of the terms of a loan, we rate the client's creditworthiness in order to ensure an appropriate and secure risk profile of the bank. For that purpose, we may issue queries to third-party databases.

We use profiling to pursue our legitimate interests:

- we rate data subjects' creditworthiness to ensure a secure risk profile of the bank and set loan/credit limit amounts available to clients in a quick and simple procedure (no additional documents, no visit to a branch);
- we provide personalised functions in electronic banking systems (transaction system, mobile application) to support finance management (e.g. classification of clients' payments in transaction history, payment assistant, etc.); the full list of such functionalities is available at www.mbank.pl/rodo;
- we engage in direct marketing of products and services of the bank and our group members in order to provide customer service and offer products adequate to the clients' needs and situation (e.g. service channels, product specificity, fees, communications);
- we classify clients (depending on income level, marketing, products) to address their individual needs (e.g. services, costs, service channels, communications and sales processes).

Obligation to inform data subjects

All personal data protection information is available at all times on our website www.mbank.pl/rodo. We are happy to address all questions of our clients. We communicate individual information in two cases: when we collect data and when we change the purposes of processing.

When do we provide information?

Whenever we collect data directly from a data subject, we provide such information immediately. When data come from a different source, we communicate it to the data subject:

- within a reasonable time limit but no later than within one month after we collect data;
- no later than during the first communication with the data subject (if we use data in communication with the data subject);

unless the provision of information proves to be impossible or would involve a disproportionate effort.

How do we provide information?

We may provide information:

- in information notices inserted in documents addressed to the data subject or posted in our electronic banking systems (transaction service, mobile application);
- in person or by phone in conversation with the bank's employee or representative;
- electronically, including by publishing such information on our website.

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

We enforce rights subject to successful verification of the identity of the data subject. Requests for the enforcement of rights may be presented at a branch or via the electronic banking system. We send our reply to the address provided by the data subject.

Right to access data

Each data subject has the right to be informed by the bank whether we process his or her personal data. The data subject has the right to know:

- why we process specific data;
- what data we process;
- to what recipients or categories of recipients we have disclosed (or may disclose) data;
- how long we are planning to process data (if that can be established) or the criteria on the basis of which we define that period.

Right to rectification

Each data subject may request that we immediately rectify his or her inaccurate personal data or complete his or her incomplete personal data. To rectify the data of a data subject, we need to receive the data subject's request which defines the extent of such rectification.

Right to erasure (right to be forgotten)

Each data subject may request that we erase his or her data if:

- the personal data are no longer necessary in relation to the purposes for which they were collected;
- the personal data have been processed in violation of GDPR or other regulations.

To erase the data of a data subject, we need to receive the data subject's request which defines the data subject's wishes. We will execute such request if, in our opinion, we have no legal basis to continue the processing.

We will execute each request as soon as possible considering the circumstances and our technical capacity.

If we erase data of a data subject, we have the right to retain information about who requested the erasure.

Right to restriction of processing

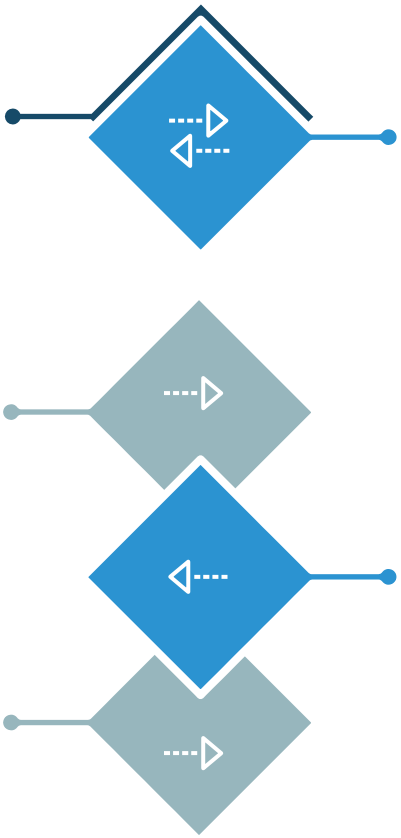
Each data subject may request us to restrict the processing of his or her data. The right applies in the following cases:

- the data subject contests the accuracy of the personal data;
- the data subject believes that the processing is unlawful and requests the restriction of their use (but opposes erasure);
- we no longer need the personal data for the purposes of the processing, but the data subject opposes erasure as he or she requires data for the exercise or defence of legal claims;
- the data subject objects due to his or her specific situation (where we process data on the basis of our legitimate interest).

It may happen that we will process data although the data subject requests restriction of the processing, in particular where we establish, exercise or defend legal claims.

To restrict the processing of the data of a data subject, we need to receive the data subject's request.

Situation	What we do
The data subject contests the accuracy of processed data.	We check the accuracy of data and suggest a correction.
The data subject believes that the processing is unlawful and requests the restriction of their use (but opposes erasure). We no longer need the personal data for the purposes of the processing, but the data subject opposes erasure as he or she requires data for the exercise or defence of legal claims.	We restrict the processing of such data, flag the accurate data and do not erase them until the data subject recalls the request for restriction of processing.



Right to portability

Each data subject has the right to transmit his or her data. We transfer data directly to the requesting data subject and, in addition, to a controller named by the data subject.

We transmit data in encrypted format by email. The dataset includes data provided by the data subject and data generated as a result of his or her actions. We do not disclose data which we have inferred.

If we are unable to differentiate between data of the requesting data subject and other data in our systems, we may withhold the request until we jointly agree which data may be disclosed.

The right to object

Each data subject has the right to object to our processing of his or her personal data on the basis of our legitimate interest. The requesting data subject should at each time define the objection in detail.

The data subject may object to:
- marketing of products and services of the bank and members of our group;
- marketing based on profiling;

Objection	What we do
Objection to marketing based on profiling.	We no longer prepare and present offers customised to the client's needs and situation.
Objection to marketing of products and services of the bank and members of our group.	We no longer engage in any marketing addressed to the client, including marketing based on profiling.

Each data subject who wishes to exercise his or her rights may present the relevant request.

The data subject's request should contain necessary identification details including:
- first name and surname,
- personal ID (PESEL),
- type, series and number of the identity document;
- mailing address (street, house/apartment number, city, post code, country);
- REGON and NIP identifiers (natural persons who carry out economic activities);
- email address and mobile phone numbers used by the client to contact bank now or in the past;
- agreements signed by the client with the bank (active or past).

Handling data breaches

A data breach occurs when we accidentally or unlawfully destroy, lose, alter, disclose or give access to personal data. Whom do we notify of a breach and when?

Data subject	if we believe that the risk to fundamental rights and freedoms is **high**	immediately (if it is very difficult to provide the information directly, we will issue a public statement).
Supervisory authority	if we believe that there is a **bigger than low** probability of an infringement of rights and freedoms of natural persons	immediately, depending on technical capacity, no later than within 72 hours after detecting an infringement.

To whom and for what purpose are we allowed to transfer personal data we process?

According to the regulations, we may transfer personal data of data subjects to other institutions for the purposes of conclusion and performance of contracts and compliance with statutory obligations.

We transfer such data to institutions including:

- Polish Bank Association (ZBP), administrator of the database System Bankowy Rejestr (BR);
- Biuro Informacji Kredytowej, biura informacji gospodarczej; for more information, visit https://www.mbank.pl/rodo;
- banks, (queries about clients – Article 105 (1) of the Banking Law);
- Ministry of Finance, (we send monthly transaction logs to the General Inspector of Financial Information GIIF in accordance with the anti-money laundering and financing of terrorism regulations);
- the Office of Competition and Consumer Protection (UOKiK), the Financial Supervision Authority (KNF), the National Revenue Administration (KAS), the Bank Guarantee Fund (BFG), the Polish National Bank (NBP) in accordance with applicable regulations;
- our outsourcing contractors under the Banking Law – for the full list, visit: https://www.mbank.pl/o-nas/informacje-wymagane-przepisami-prawa/ (file name: Informacje o przedsiębiorcach zgodnie z art.111b ustawy Prawo bankowe);
- SWIFT – Society for Worldwide Interbank Financial Communications (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);
- members of the mBank Group, Commerzbank AG, and members of the Commerzbank Group – only with the client's consent – Article 104 (3) of the Banking Law;

Data maintained by BR and BIK may be transferred to:

- other banks;
- financial institutions which are banks' subsidiaries;
- other entities authorised by law;
- business information bureaus.

Data transmission outside Poland

We may transfer personal data on specific grounds to entities in the European Economic Area (EEA), which includes the European Union Member States, Iceland, Norway, and Liechtenstein. We may transfer personal data to third (non-EEA) countries provided that they guarantee at least the same level of data protection as Poland. In practice, such guarantee means that the European Commission considers the country to ensure the necessary protection.

We may transfer personal data to other third countries without the consent of Poland's personal data protection supervisor (Personal Data Protection Office, UODO). That is possible provided that our agreements with entities in such countries include special solutions provided by law or approved by Poland's personal data protection supervisor.

The government administration of the United States of America may exceptionally have access to personal data because we execute international money transfers via SWIFT (Society for Worldwide Interbank Financial Communications). The US Government has agreed to use such data only for the purpose of combatting terrorism (subject to the guarantees offered by the European personal data protection system).

mBank's Data Protection Officer

We have appointed Agata Rowińska as our Data Protection Officer.
Contact details of the Data Protection Officer:

▼

email:
inspektordanychosobowych@mbank.pl

▼

mailing address:
Data Protection Officer
mBank S.A.
ul. Prosta 18, 00-850 Warsaw

How to lodge a complaint concerning personal data protection?

If a data subject believes that his or her data are processed in violation of GDPR, the data subject has the right to lodge a complaint with the personal data protection supervisor (Personal Data Protection Office, UODO) according to the procedure described on its website at www.uodo.gov.pl.

For how long do we process data?

We process data for a period of time necessary for the purposes of processing:

- five years if we conclude no agreement for the use of a deposit product;
- two years if we conclude no agreement for the use of a credit product;
- no longer than 10 years after the termination of an agreement (to be able to establish, assert or defend our claims of for purposes of compliance with a legal obligation);
- 90 days for security camera footage after it's recorded.

We follow the principle of storage limitation which protects data from processing for an unlimited period of time. When we have achieved the purpose of processing, we erase or anonymise data, which means that such data may no longer be recovered. The exceptions are situations when we need to store data due to separate provisions (e.g. to carry out tasks related to crime prevention).

Useful documents and information:

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