



# GDPR Package for Individual and Business Clients



[mBank.pl](https://mBank.pl)

## Table of Contents

The GDPR - general information .....	3
Basic principles of the GDPR .....	7
How we process personal data - basic information.....	8
Where do we get the data we process from? .....	10
Automated decision-making .....	10
Data profiling .....	11
Obligation to inform data subjects .....	12
What are the rights of data subjects and how do we facilitate their exercise? .....	13
Rules of conduct regarding data breaches .....	16
To whom and for what purpose are we allowed to transfer personal data that we process? .....	17
Rules for transferring data outside Poland .....	18
mBank's Data Protection Officer .....	18
How to complain about personal data protection? .....	19
How long do we process data?.....	19
Useful documents and information: .....	19

## The GDPR – general information

---

### GDPR

We have applied the GDPR (General Data Protection Regulation) 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.

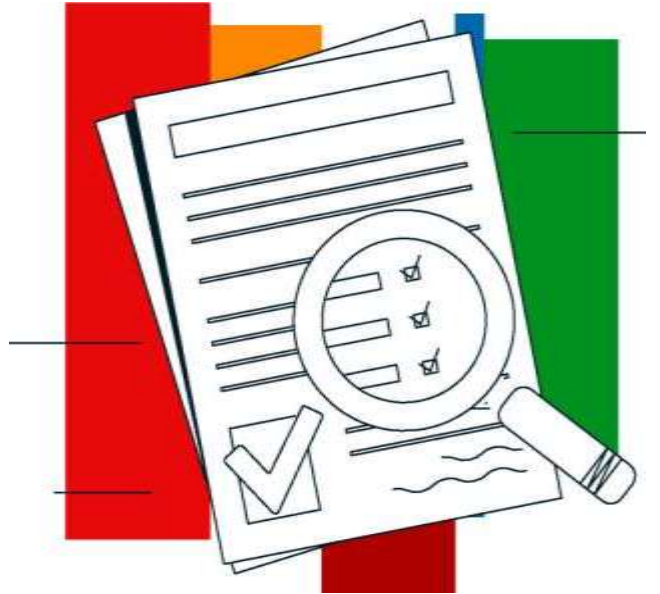
### What is the purpose of the GDPR?

The 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:

<b>Controller</b>	a person or entity which (either alone or jointly with other controllers) determines why and how to process personal data. The controller of personal data is mBank S.A. with its registered office in Warsaw (“bank”).
<b>Data subject</b>	the bank’s client, a prospective client, a natural person related to a client, e.g., a client’s attorney-in-fact, representative, proxy, beneficiary, beneficial owner, real estate seller.
<b>Profiling</b>	automated processing of personal data which uses personal data to evaluate certain personal aspects relating to a client.
<b>Automated decision-making</b>	decision-making without human intervention based on models and algorithms developed in IT systems.
<b>Personal data</b>	information that identifies (or allows the identification of) a natural person (also referred to as a “data subject”). Personal data includes, in particular: first name and surname, client number (client ID), address, phone number, date of birth, credit history, bank account number, tax identification number (NIP), personal identification number (PESEL), family information, children’s names, remuneration, CCTV monitoring or video call footage, voice, etc.
<b>Processor</b>	a person or entity which processes personal data on behalf of and for the controller.
<b>Personal data processing</b>	activities relating to personal data. They may be carried out automatically or manually. Data processing occurs when data is: 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 destroyed.



## How do we communicate with data subjects?

We communicate with data subjects on all matters, including personal data, via our website, online banking, by email, phone 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 Warszawa

phone no.: (22) 829-00-00

<http://www.mbank.pl>

- **Correspondence address**

mBank S.A. Bankowość Detaliczna

Skrytka Poczтовая 2108

90-959 Łódź 2

- **Kompakt Finanse, produkty bankowe dostarcza mBank**

Oddział Bankowości Mobilnej w Łodzi, Skrytka Poczтовая 2108

90-959 Łódź 2

mLine and the Kompakt Finanse helpline are available around the clock, seven days a week

## How to call mLine and the Kompakt Finanse helpline?



**+48 42 6 300 800**

from landlines all over the world

**783 300 800**



from mobile phones

**+48 42 678 21 78**



from mobile phones and landlines all over the world, Kompakt Finanse helpline

## Basic principles of the GDPR

---

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

■ **principle of lawfulness, fairness and transparency:**

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;

■ **principle of data minimisation and adequacy:**

we only process data that is actually needed (adequate, relevant) to achieve a given purpose;

■ **principle of data accuracy:**

we spare no effort to ensure that the data we process is 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.);

■ **principle of limiting the purpose and storage of processed data:**

we only collect personal data for specified, explicit and legitimate purposes which could not be achieved otherwise. We store data in a form that allows the data subject to be identified. We process personal data for no longer than is necessary for the purposes for which the personal data have been collected (unless we are required by law to continue processing);

■ **principle of data integrity and confidentiality:**

we use appropriate IT and organisational measures to ensure security of personal data processed. We protect data against unauthorised or unlawful processing and against accidental loss, destruction or damage;

■ **principle of 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 we process personal data – basic information

### What data do we process, and on what basis?

We process general and special category personal data.

#### Usually we process general data, such as:

- first names and surnames;
- PESEL, date, city and country of birth, birth name, mother's maiden name, father's and mother's first names, marital status, citizenship, mailing address, address of residence or registered address;
- country of residence, tax identification number in a jurisdiction other than Poland (TIN), gender, email address, phone number;
- data disclosed in identity documents (identity card or its copy, e-ID, passport or its copy, residence permit or its copy), series and number of the identity documents, date of issue and expiry date; image on a copy of the identification document or photo ("selfie") made by the client when opening a bank account;
- data disclosed in documents pertaining to real estate purchased by a client, including data on the real estate seller required for the purpose of compiling an appraisal report;
- name of the company, address of its registered office, correspondence address, information on: business classification as per the Polish Classification of Business Activities (PKD), beneficial owner, statistical number REGON, tax ID (NIP) or tax ID in a jurisdiction other than Poland (TIN), country of residence;
- financial data (bank account number, credit card number or payment card number, cardholders' first name and surname, card expiry date, income, source of income, credit history, products and services);
- history of transactions and current account balances with other banks indicated by the client as part of open banking;
- client identifier (client ID);
- image recorded on the bank's premises by the bank's monitoring systems or during video meetings when establishing the business relationship or as part of ongoing customer service;
- data concerning our communication;
- the client's location data, online identifier (IP address), cookies which are processed according to the mBank Cookies Policy available at [www.mbank.pl/o-nas/o-mbanku/polityka-prywatnosci.html](http://www.mbank.pl/o-nas/o-mbanku/polityka-prywatnosci.html);
- other data necessary to offer our products and services.

#### We may process personal data provided that:

- **the data subject has given their consent;** we process data on that basis when the client uses the open banking service or 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 or video conversations;
- **we are doing it to process applications and perform agreements** between us and the data subject, including when we:
  - determine creditworthiness to process a loan application;
  - process applications for bank products;
  - handle complaints,



- **we are complying with a legal obligation in this way;** on this basis, we process data in order to prevent fraud and ensure security of business operations. We are subject to specific legal obligations under the Banking Law Act, the Act on Counteracting Money Laundering and Terrorism Financing, the Act on Trading in Financial Instruments, the Act on Financial Market Complaints Processing and the Financial Ombudsman, the General Tax Law, the Accounting Act, 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);
- **on grounds of our legitimate interest (as a controller), i.e. whenever we:**
  - develop an adequate and secure risk model for the loan portfolio by determining the creditworthiness of clients;
  - value collateral and monitor its value and analyse our collateral portfolio;
  - provide banking system functionalities based on profiling, including in electronic banking systems (online banking, mobile app), customised to the needs of each client;
  - engage in direct marketing of products and/or services of our bank and our group members (the full list is available at [www.mbank.pl/o-nas/grupa/](http://www.mbank.pl/o-nas/grupa/));
  - present an individualised marketing offer, establish, exercise or defend claims;
  - generate statistics and reports;
  - develop, monitor and change internal approaches as well as approaches and models relating to prudential requirements, including operational risk;
  - survey customer satisfaction;
  - develop or modify our product range and our operating plans and strategy;
  - sell or recover receivables;
  - archive data;
  - 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;
- mouse dynamics, keyboard input and activity on the device used to confirm a payment transaction (behavioural biometrics).

#### **Processing children's data:**

We offer dedicated products for children and teenagers (including bank accounts), giving them an opportunity to learn from an early age how to consciously manage their personal savings. To protect children's rights, we always ask parents (or legal guardians) for consent to their children using such services.





## Where do we get the data we process from?

---

We process data provided by data subjects in forms, e.g. when opening a bank account or applying for a loan. We check such data against the identification documents produced by the data subject for purposes of verification. We also use the identity card register (RDO) and the PESEL database. We make copies of identity documents in selected processes.

As regards beneficial owner data, we receive such information from our clients' representatives.

We may also use data transmitted by other controllers (e.g. Biuro Informacji Kredytowej S.A., 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 our clients in connection with the performance of legal obligations or in connection with the bank's programmes in which clients participate, as well as data from other banks obtained as part of the open banking service.

In the case of real estate sellers, we receive their data from persons applying for loans.

## </> Automated decision-making

---

Automated decision-making means that decisions concerning clients' applications are made without human intervention based on models and algorithms. We use it to shorten the waiting time for clients awaiting our decision and to provide top quality service.

For example, we use automated decision-making to handle complaints and grant loans. We automatically rate the client's creditworthiness, credit history, and their relationship with the bank. We use data provided by the client in the application, the client's history with the bank, and data from other sources including:

- Bankowy Rejestr system operated by the Polish Bank Association (ZBP),
- Biuro Informacji Kredytowej S.A.,
- other credit institutions or providers of information authorised by law.

We alert clients to automated decision-making already in the complaint receipt confirmation or the loan application and later in the decision itself. Clients may appeal against such decisions via the mLine or at our branches.





## Data profiling

---

Data profiling means that we use algorithms or mathematical models to analyse clients' features, preferences, and future behaviour. We use appropriate (technical and organisational) measures to mitigate the risk of error in profiling. We spare no effort to ensure that our assessment is objective and our processes are non-discriminatory.

Our statistical models comply with best practices of the banking market (covered, among others, by Recommendation W of the Polish Financial Supervision Authority).

### Why do we use profiling?

#### **We use profiling to fulfil our legal duties:**

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

#### **We use profiling whenever necessary to conclude or perform an agreement:**

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 (online banking, mobile app) to support finance management (e.g. classification of clients' payments in transaction history, payment assistant, etc.);
- 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 (in the scope of services, costs, service channels, communication 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](http://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 purpose of its processing.

### When do we provide information?

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

- within a reasonable time limit, but not later than within one month after we have collected the data;
- not later than during the first communication with the data subject (if we use the data in communication with the data subject); unless the provision of information proves to be impossible or would involve disproportionate effort.

### How do we provide information?

**We may provide this information:**

- in information notices inserted in documents addressed to the data subject or published in our electronic banking systems (online banking, mobile app);
- personally or by phone, in the course of a conversation with a representative of our bank;
- electronically, including by publishing this information on our website.



## What are the rights of data subjects and how do we facilitate their exercise?

---

We respond to data subjects' requests to exercise their rights upon their successful authentication. Such requests may be filed via mLine, the Kompakt Finanse helpline or at our branch. We send our reply to a data subject's email address saved in our database.

### Right of access to data

A data subject has the right to be informed by the bank whether we process their personal data.

#### **A data subject has the right to know:**

- why we process specific data;
- what type of data we process;
- to what recipients or categories of recipients we disclosed (or may disclose) their data – this concerns, in particular, recipients in countries other than the member states of the European Economic Area or international organisations;
- how long we plan to process their data (if it can be specified) or on the basis of what criteria we determine this period.

### Right to rectification

A client may request that we rectify their inaccurate personal data or complete incomplete data without delay. Depending on the type of data, rectification may be requested via mLine, the Kompakt Finanse helpline, at a branch (e.g. in the case of an ID number), online banking or the mobile app.

### Right to erasure (right to be forgotten)

#### **A data subject may request that we erase their data if:**

- the data is no longer necessary to achieve the purpose for which it was collected,
- the data was processed in breach of the GDPR or other legal regulations.




A data subject who wishes their data to be erased may file a relevant request via mLine, the Kompakt Finanse helpline or at a branch. We will execute such a request if, in our opinion, there is no legal basis to continue the processing.

If we erase the data of a person submitting such a request, we have the right to keep information about the requesting person.

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

## Right to restriction of personal data processing

A data subject may also request that we restrict the processing of their data. The right applies where:

Situation		What we do
a data subject contests the accuracy of processed data;		We check the accuracy of data and suggest a correction.
a data subject believes that we process data unlawfully and requests the restriction of data use (but opposes erasure). We no longer need the personal data to achieve the intended objective, but the data subject opposes its erasure because they need the data for the exercise or defence of legal claims;		We restrict the processing of such data, mark the respective data and do not erase it until the data subject cancels their restriction request.
a data subject wishes to object on grounds relating to their particular situation (where we process the data on the basis of our legitimate interest).		We analyse the situation and ask the client to indicate to which purpose of data processing they object.

## Right to data portability

Every data subject has the right to transfer their data. Such requests may be filed via mLine, the Kompakt Finanse helpline or at our branch. We will transfer data directly to the requesting data subject so that they can transfer it to another entity (no standards for secure data transfers between controllers have been developed yet).

We will transmit data in an encrypted email message (in the format agreed by banks in the Polish Bank Association (ZBP)). The transferred data will include the data provided to us by the requesting data subject and the data generated as a result of their actions (including transaction data). We will not disclose data which we have inferred (in particular, when rating creditworthiness).

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

## Right to object to processing

A data subject has the right to object to our processing of their personal data on the basis of our legitimate interest. The requesting data subject should each time define the objection in detail.

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 subsidiaries of mBank Group.	We no longer engage in any marketing activities addressed to the client, including marketing activities based on profiling.
Objection to functions of the bank's systems based on profiling.	We deactivate those functions of our electronic banking systems (online banking, mobile app) that are based on profiling (advanced transaction history, payment assistant, etc.), including querying third-party databases. The client may only submit such an objection due to their particular situation (the client should describe it).
Objection to the development of the bank's appropriate and safe risk profile by rating the clients' creditworthiness.	We analyse each case and, if we find the objection to be reasonable, we no longer process client data for that purpose.

We will comply with the received objections as soon as technically practicable.



## Rules of conduct regarding data breaches

A data breach occurs when we accidentally or unlawfully destroy, lose, alter, disclose or give access to personal data.

Who and when will we inform if there is a breach at our bank?

<b>Data subject</b>	if we believe that the risk to the rights and freedoms is <b>high</b>	without undue delay (if it is very difficult to provide the information directly, we will issue a public statement)
<b>Supervisory authority</b>	if we assess – with a probability <b>higher than low</b> – that there might have occurred a risk to the rights and freedoms of natural persons	immediately, as far as technically practicable, not later than within 72 hours after the breach was identified





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

---

Under the law we may transfer clients' data to other institutions for the purposes of conclusion and performance of contracts with clients and compliance with statutory obligations.

### We transfer clients' data to institutions and entities, including in particular:

- **Polish Bank Association**, administrator of the database System Bankowy Rejestr;
- **Biuro Informacji Kredytowej**; for more information, visit <http://www.mbank.pl/pdf/rodo/klauzula-informacyjna-bik.pdf>;
- **Ministry of Finance** (we send monthly transaction logs to the General Inspector of Financial Information in accordance with the anti-money laundering and financing of terrorism regulations);
- **The Office of Competition and Consumer Protection, the Financial Supervision Authority, the Financial Ombudsman, the National Revenue Administration, the National Bank of Poland and the Bank Guarantee Fund** in accordance with applicable regulations;
- **our outsourcing contractors under the Banking Law Act** (in particular our credit intermediaries or couriers who deliver documents to clients) – 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);
- **third parties** – partners of the bank (only with a data subject's consent or authorisation or in line with an agreement concluded with a client) to which the data must be provided in order for them to perform a certain action, e.g. a payment transaction or another service or action; such third parties include clearing houses or other entities rendering clearing or settlement services, payment institutions or schemes, or entities representing such entities;
- **other banks** – if the client submitted an application and granted their consent at another bank to access information on transaction history and account balances;
- **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).





## Rules for transferring data outside Poland

---

We may transfer personal data on specific grounds to entities in the European Economic Area (EEA). The EEA consists of the member states of the European Union, 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 a guarantee means that the European Commission has recognised a given country as providing adequate protection.

We may transfer personal data to other third countries without the consent of Poland's personal data protection supervisor provided that our agreements with entities in such countries include special solutions, such as standard personal data protection clauses approved by the Commission, provided by law or approved by Poland's personal data protection supervisor. Contact us to obtain information about such solutions or, where possible, their copy.

The government of the United States of America may, in exceptional cases, gain access to personal data because we execute international money transfers via SWIFT (Society for Worldwide Interbank Financial Communications). The US authorities have agreed to use such data only for the purpose of combatting terrorism (subject to the guarantees offered by the European personal data protection system). For more information on the processing of personal data by SWIFT, go to <https://www.swift.com/about-us/legal/compliance/data-protection-policies>.



## mBank's Data Protection Officer

---

We have appointed Agata Rowińska as our Data Protection Officer.

Contact with the Data Protection Officer:



by email:

[inspektordanychosobowych@mbank.pl](mailto:inspektordanychosobowych@mbank.pl)



by mail:

**Data Protection Officer of mBank S.A.**

**ul. Prosta 18, 00-850 Warszawa**





## How to complain about personal data protection?

---

If a data subject believes that their data is processed in violation of the GDPR, they have the right to lodge a complaint with the personal data protection supervisor in the manner described on its website (<https://www.uodo.gov.pl>). In Poland, the President of the Personal Data Protection Office (UODO) is the personal data protection supervisor.

## How long do we process data?

---

**We process data for a period necessary to achieve the intended purpose of processing, i.e.:**

- for six months if we do not conclude an agreement on a deposit product;
- for two years if we do not conclude an agreement on a credit product or if we do not issue a credit card;
- for no more than 10 years after termination of the last agreement concluded with the bank (in order to identify, pursue or defend our claims or for purposes of compliance with a legal obligation);
- for 90 days from the date of consent to access information on bank accounts (transaction history and account balance) held with other banks (open banking service);
- for 90 days from the day on which a CCTV image was recorded;
- 2 days from the date of obtaining data from the mObywatel app if no application is filed.

We apply the principle of restricting the storage of personal data, which safeguards data against its processing for an unlimited period. When we have achieved the purpose of processing, we erase or anonymise data, which means that such data may no longer be recovered. In exceptional cases, we store data if doing so arises from separate regulations (e.g. in order to perform tasks related to crime prevention).



## Useful documents and information:

---

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