

**mBank**

# **GDPR Package for Employees, Job Candidates and Partners**



**mBank.pl**

Table of contents

GDPR - general information..... 3

Basic principles of the GDPR..... 4

How do we process personal data? - basic information ..... 5

Automated decision-making and profiling ..... 7

Obligations to inform employees (data subjects) ..... 7

What are the rights of data subjects and how do we facilitate their exercise? ..... 7

Rules of conduct regarding data breaches..... 11

Principles of transferring data outside the European Economic Area (EEA) ..... 12

mBank’s Data Protection Officer..... 13

How to complain about personal data protection?..... 13

How long do we process data? ..... 13

Useful documents and information..... 14

# GDPR – general information

## GDPR

The GDPR (General Data Protection Regulation) has been in force 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 security of personal data and protects the right to privacy.

## Who is the GDPR Package addressed to?

It is addressed to the employees and partners of mBank S.A. Employees include persons who are or used to be employed with the bank under an employment contract (both full-time and part-time) and job candidates (including those who ultimately were not employed). Partners are persons who provide services to or on behalf of the bank under civil-law contracts but do not pursue business activity.



## Glossary:

<b>Controller</b>	a person or entity which (either alone or jointly with other controllers) determines for what purpose and how personal data should be processed;
<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 include, in particular: first name and surname, employee number, address, phone number, date of birth, bank account number, tax identification number (NIP), personal identification number (PESEL), family information, children’s names, remuneration, etc.;
<b>Processor</b>	a person or an entity who/which processes personal data on behalf of the controller;
<b>Profiling</b>	automated processing of personal data which uses personal data to evaluate certain personal aspects relating to a data subject;
<b>Personal data processing</b>	operations performed on 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 about matters relating to personal data?

- **job candidates, former employees and former partners** – by email (rododlapracownikow@mbank.pl), online (www.mbank.pl/kariera/rodo), via the ATS-eRecruiter system (job candidates) or by mail.  
**Mailing address:**  
mBank S.A.  
Departament Relacji Pracowniczych i Kultury Organizacji  
ul. Prosta 18, 00-850 Warszawa
- **employees** – via the GDPR Service Desk app available in the intranet, via the HR Service Desk, which is a tool for day-to-day management of employee affairs, or to the email address rododlapracownikow@mbank.pl
- **associates** – via the GDPR Service Desk app available in the intranet, to the email address rododlapracownikow@mbank.pl or by mail.  
**Mailing address:**  
mBank S.A.  
ul. Prosta 18, 00-850 Warszawa

## 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 law. We communicate all matters exhaustively via the agreed communication channels in the simplest language possible 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 necessary (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, from time to time, ask data subjects to check and update their data. We also ask them 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 keep data in a form that permits identification of data subjects. We process personal data for no longer than is necessary for the purposes for which the personal data was collected (unless we are required by law to continue processing);

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

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

- **principle of accountability:**

we can demonstrate (as required by law) that we process personal data lawfully and ensure data protection by default.

## How do we process personal data? – basic information

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

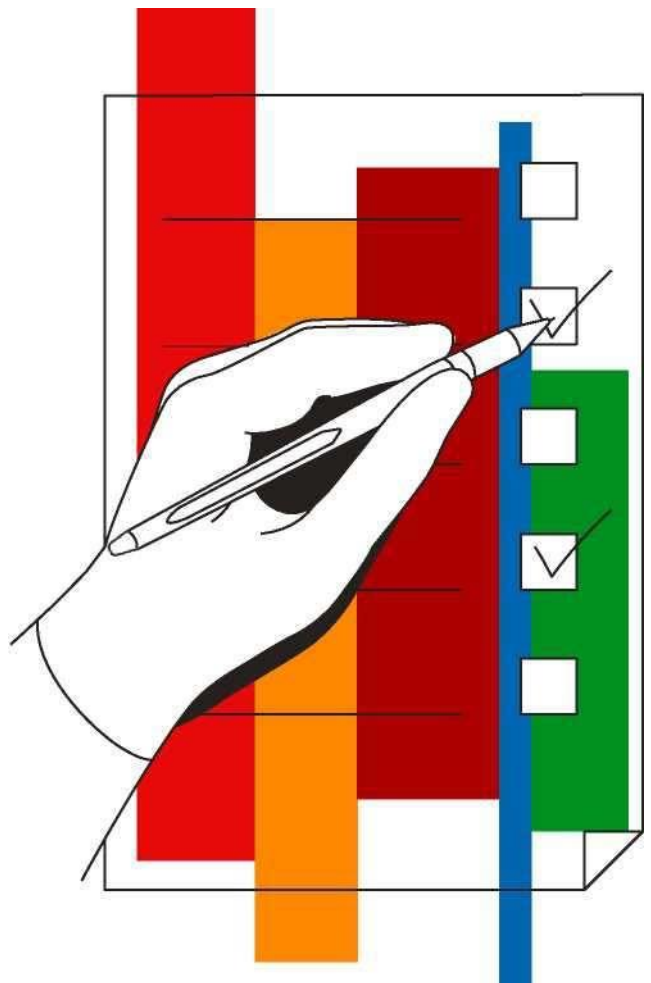
We process general and special categories of personal data. Personal data means all information that identifies (or allows the identification of) a data subject. We collect personal data provided to us by our employees and partners during the recruitment process and during employment. We collect personal data on various occasions and in various ways: when we receive a completed employee questionnaire or a medical certificate, or when our employees or their family members want to use employee perks or benefits from the Company Social Benefits Fund (ZFŚS), or when our employees use the bank's systems and apps.

We may also collect data when we have an appropriate legal basis for it.

We usually use such sources of general data as: job applications, recruitment forms, job offers, employment contracts, business correspondence, declarations, benefit application forms or performance assessments.

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

- first name (and any middle names) and surname;
- date of birth;
- personal identification number PESEL or, if a given person does not have a PESEL, the type and number of an identity document, e.g. passport number in the case of foreigners);
- correspondence address, residence address, and registered address;
- other identification data: email, landline/mobile phone number, citizenship, gender;
- education;
- educational background and work experience;
- employee number;
- image recorded by the bank's monitoring systems or during video calls, e.g. via MS Teams;
- data regarding phone calls, e.g. with the bank's clients;
- employee's location data, online identifier (IP address), and cookies which are processed in accordance with 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);
- financial data (including the bank account number, number of a business credit/payment card, remuneration).



## **When and why do we process personal data?**

We use and process the necessary personal data based on various legal bases: ■ when pursuing our legitimate interests that require us to enter into and manage relationships with employees and partners; our purposes of personal data processing include, in particular:

- recruitment processes;
- business processes (including maintenance of business and statutory registers, management analyses, audits, forecasts, planning, transactions, business continuity, and risk prevention at work);
- safety at the workplace, protection of property, employees, and personal data of employees, clients and consumers, including monitoring (described below);
- extraordinary activities, such as mergers and acquisitions, relocation of business or of a branch thereof, and entering into joint venture agreements;
- programmes and policies regarding training and development, performance assessment, bonuses, planning and organisation;
- crime prevention and detection (to ensure security);
- performance of employment contracts and service agreements, including management of human resources and payment of remuneration;
- compliance with law, regulations and legal obligations (e.g. related to accounting, taxes, employee insurance and pensions);
- performance of obligations and exercise of rights arising from labour law.

We can also, based on consent, process data in other cases, e.g. when a data subject joins a voluntary programme or uses a benefit. An employee or a partner has the right to withdraw such consent at any time (the instruction will not affect the lawfulness of processing based on consent before its withdrawal).

In some circumstances, we need data to meet our statutory obligations or to comply with the terms and conditions of an employment contract or a civil-law contract we are bound by. If, in such a case, an employee or a partner refuses to provide data, we will be forced to terminate the employment contract or cooperation based on any other contract type (as we will not have the personal data necessary to effectively administer and manage the relationship).

If the purpose of the processing of personal data changes to a purpose other than the purpose for which we originally collected the personal data, we will inform the data subject of this different purpose.

We will inform the data subject if the provision of certain data is necessary (in particular when the provision of this data is required by an agreement or by law). If we do not receive it, we will not be able to carry out certain HR processes.

## **Monitoring**

We use our systems to monitor phones, email, voice mail, network traffic and other means of communication. We reserve the right to capture, record and monitor an employee's or a partner's use of IT systems and networks of the bank without prior notice. We only do it to the extent permitted by law and, if necessary and for legitimate business purposes, in particular in order to control the quality and security of communications and IT systems, to protect confidential information and legitimate business interest of the bank, to keep documentation, collect evidence, meet legal requirements, and to detect and prevent misconduct or illegal or criminal activity.

Under certain circumstances we can store or process the personal data of an employee in an electronic database. We can also disclose the information about an employee to public authorities, our legal advisors and consultants, the police, and to competent courts in accordance with the applicable laws.

## **Special personal data:**

We process special categories of personal data only where it is necessary for us to comply with our legal obligations as an employer. In particular, we process the following data:

- degree of disability (PFRON subsidy, establishment of leave entitlements),
- health data connected with occupational medicine (e.g. eye defect).

## **Processing data of family members of an employee or a partner:**

We only obtain such data for a legitimate purpose, e.g. to sign up a family member with the Social Insurance Institution (ZUS) or to provide employee health benefits, benefits offered by the Company Social Benefits Fund (ZFŚS), or employee perks.

## Automated decision-making and profiling

We never make automated decisions or profile the personal data of employees and partners.

## Obligations to inform employees (data subjects)

All information on personal data protection is available to our employees at all times on our website ([www.mbank.pl/kariera/rodo](http://www.mbank.pl/kariera/rodo)) and on the Employees site on the bank's intranet.

### When and how 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 inform the data subject about it by email, by phone or by mail:**

- immediately but not later than within one month after we obtained the data,
  - not later than during the first communication with the data subject (if we use the data in communication with this data subject).

### **We may provide this information:**

- in data processing statements included in documents addressed to the data subject or in internal regulations, or posted in electronic banking systems and banking apps,
- personally or by phone during a conversation,
- electronically (e.g. by email), including by posting this information on our website and on the intranet.

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

The GDPR guarantees certain rights to data subjects. To exercise these rights, data subjects should submit a request via communication channels dedicated to:

- employees – in the GDPR Service Desk app available on the intranet or in the HR Service Desk, which is a tool for day-to-day management of employee affairs, or to the email address [rododlapracownikow@mbank.pl](mailto:rododlapracownikow@mbank.pl)
- partners – in the GDPR Service Desk app available on the intranet, to the email address [rododlapracownikow@mbank.pl](mailto:rododlapracownikow@mbank.pl) or by mail.

### **Mailing address:**

mBank S.A.  
ul. Prosta 18  
00-850 Warszawa



## Right of access to data

A data subject is entitled to obtain information about whether we process their personal data.

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

- why we process specific data,
- what types of data are processed,
- 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.

The right of access to data is exercised free of charge.

## Right to rectify and complete data

A data subject may request that we immediately rectify their inaccurate personal data or complete their incomplete personal data. Employees can modify their data themselves in the Employee Zone in the 'HR issues' tab.

In all other cases, data correction requests should be submitted via the communication channels listed above.





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

### A data subject may request that we erase their data when:

- 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.

We will execute the request where there are no legal grounds for continuing the processing of the data concerned. If we erase the data, we will have the right to keep information about the requesting person.

### For this purpose we can process:

- employee number (in the case of existing employees),
- tax identification number (NIP), and where NIP is unavailable, first name and surname, and personal identification number (PESEL) (in the case of partners),
- first name and surname, and tax identification number (NIP) (in the case of former employees),
- first name and surname, and phone number (in the case of job candidates),
- information on the erased data and the erasure date.

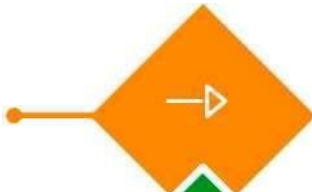



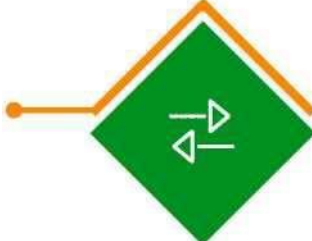
We will store this data in accordance with the principle of data minimisation and adequacy. We will inform every entity to which we disclose the data of a given data subject that the data subject has exercised the right to erasure of data.

We will exercise such requests as soon as practicable, but not later than within 30 days.

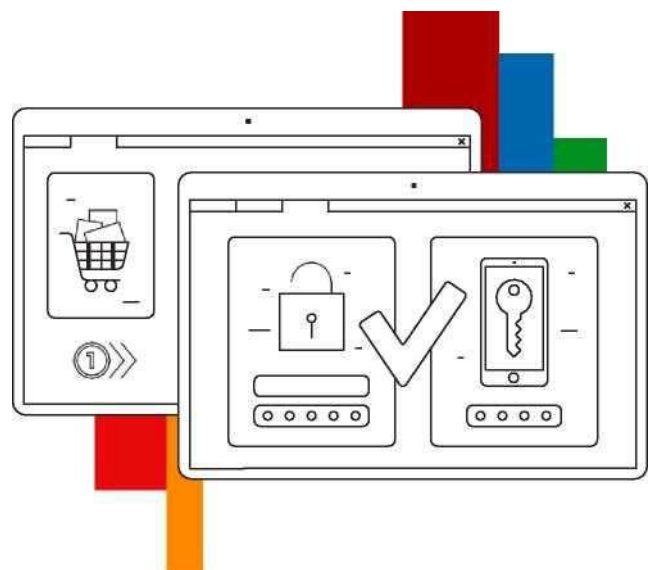


## Right to restriction of personal data processing

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

Situation		What we do
A data subject contests the accuracy of data processed by us.		
A data subject believes that we process data unlawfully and requests the restriction of data use (but opposes erasure).		We check the accuracy of data and suggest a correction.
We no longer need the personal data to achieve the intended purpose, but a data subject opposes its erasure because they need the data for the establishment, 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 (when we process the data on the basis of our legitimate interest).		We analyse the situation and ask the data subject to indicate to which purpose of data processing they object.

There may be situations where we will process data despite a data subject's request to restrict the processing of their data. This is particularly the case when we are establishing, exercising or defending legal claims.



## Right to data portability

Every data subject has the right to transfer their data. 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).

The data will be transferred in a PDF file via an encrypted email. 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. We will not disclose data which we have inferred.

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 may object to our processing of their personal data that is based on a legitimate interest. The requesting data subject should each time indicate the scope of their objection.

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

## Rules of conduct regarding 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 if there is a breach at our bank?

<b>Data subject</b>	if we assess that the risk to the rights and freedoms is <b>high</b>	immediately
<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?

Sometimes we have to disclose personal data to other members of mBank Group and to third parties.

We will only do so for necessary and legitimate business purposes. For example, we can transfer the personal data of an employee or a partner to:

- institutions supervising our bank and authorised to process data (e.g. the Polish Financial Supervision Authority (KNF) and the Office of Competition and Consumer Protection (UOKiK)),
- external providers (so that they can administer due benefits on our behalf),
- our advisors and insurers,
- competent public authorities and government agencies in accordance with the applicable laws on taxes, labour, social security, etc.,
- our carefully selected service providers to which we contractually entrust the provision of services connected with our operations. These may include entities processing the data of our employees and partners, remuneration and cost data, and other remuneration-related information. We include relevant safeguards compliant with the GDPR in agreements with our carefully selected service providers (e.g. the obligation to use specific measures to protect the confidentiality and security of personal data),
- our clients with whom we cooperate to perform the concluded agreements,
- new (or potential) owners where there is (may potentially be) a change of the owner of the bank, its organisational units or divisions in which the data subject whose data we process is employed, and/or
- external parties – in accordance with the applicable laws or for the purpose of court proceedings, or for other purposes to which the data subject granted its consent.

We entrust the processing of personal data to entities that provide sufficient guarantees - in particular in terms of expertise, reliability and resources - of the implementation of technical and organisational measures that comply with the requirements of the GDPR, including the security requirements for processing.

## Principles of transferring data outside the European Economic Area (EEA)

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 and 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.



## **mBank's Data Protection Officer**

We have appointed Sylwia Graczyk as our Data Protection Officer.  
Contact with the Data Protection Officer:



by email:

**inspektordanychosobowych@mbank.pl**



by mail:

**Inspektor Danych Osobowych (Personal Data Officer)**

**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>).

## **How long do we process data?**

We process data for a period of time necessary for the purposes of processing. Usually it is for the duration of employment / contract extended by the statutory limitation period after the end of employment. Certain data, e.g. information for pension purposes, may be stored for a longer period.

We may store specific types of data (e.g. tax documentation connected with personal/corporate income tax) for as long as necessary to meet the legal and regulatory requirements and for other legitimate business purposes.

**In particular, we erase or anonymise data when:**

- the data subject withdraws their consent to the processing of personal data (if their consent was the basis for processing),
- the data subject effectively objects to further processing (if our legitimate interest was the basis for processing),
- claims, if any, become time-barred (if we were processing data in order to perform an agreement),
- the time limits laid down in other regulations (e.g. in the Accounting Act, the Labour Code, etc.) have expired.

## Useful documents and information:

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

