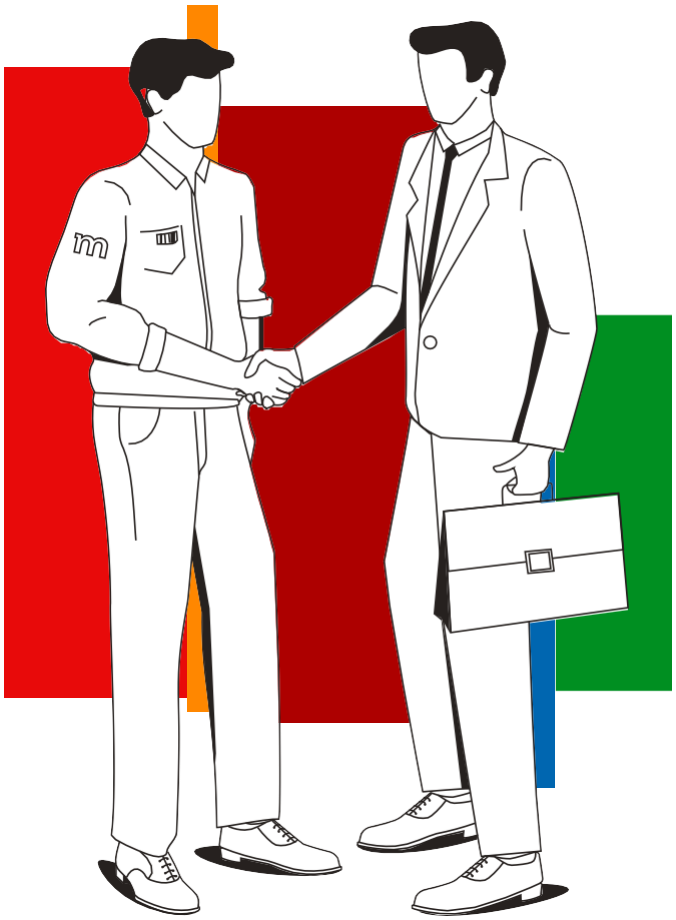
GDPR packet for counterparties and their employees



mBank.pl

Table of Contents

GDPR – general information

The GDPR
(General Data Protection Regulation) has been applied since 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 Directive95/46/EC.

What is the objective of the GDPR?

The GDPR introduces harmonised principles of personal data processing in the entire 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 personal data is mBank S.A. with its registered office in Warsaw (“bank”).
Personal data	means information that identifies (or allows the identification of) a natural person (also referred to as a “data subject”). Personal data shall include, in particular: full name, address, telephone number, date of birth, Tax ID No (NIP), Personal ID No (PESEL), remuneration, CCTV monitoring footage, etc.
Processor	means a natural person or entity that processes personal data on behalf of the controller.
Personal data processing	means 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 does our bank communicate with counterparties and their employees?

With regard to all issues (including those relating to personal data), we communicate with our counterparties and their employees in a manner to be defined in an agreement concluded with the counterparty or via the bank’s website.

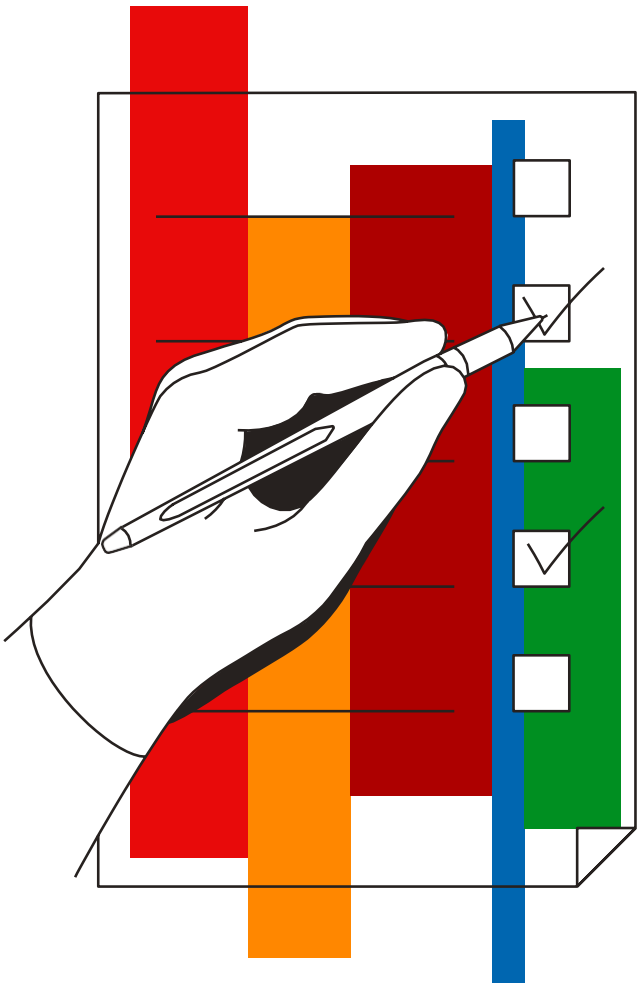
Contact details of mBank:

- **Head Office and Management Board of mBank S.A.**
  ul. Prosta 18, 00-850 Warszawa
  tel.: (22) 829-00-00
  www.mbank.pl

Basic principles of the GDPR

The GDPR sets out 6 principles of personal data processing. Our bank follows them when we process personal data. These include:

- **principle of lawfulness, fairness and transparency:**
  we process personal data in a lawful manner. We inform in detail about all issues related to this matter using specified communication channels and the simplest language. We want data subjects to be aware that we collect, store or otherwise process their specific personal data;
- **principle of data minimisation and adequacy:**
  we process such data that is indeed necessary to achieve a given objective;
- **principle of data accuracy:**
  we take utmost care to ensure that the data we process is true, up-to-date and accurate. That is why, every so often, we may ask individuals whose data is processed by us to check and update their data;
- **principle of limiting the purpose and storage of processed data:**
  personal data is 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 data only for as long as is necessary to achieve the purpose for which we have obtained it (unless we are obliged to its further processing by law);
- **principle of data integrity and confidentiality:**
  we provide such IT and organisational solutions that the personal data we process is 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 by design and by default.



How do we process personal data – basic information

What data do we process and on what basis?

We process general and special personal data. Personal data means all information that identifies (or allows the identification of) a data subject. We collect personal data that has been provided to us by counterparties or their employees when entering into an agreement, as well as during cooperation.

Usually we process general data, such as:

- full name;
- other identification data: Personal ID No (PESEL), correspondence address, e-mail, telephone number;
- identification number;
- whereabouts of a counterparty or their employee (location data);
- online identifier (IP address);
- occupation and employment information;
- Tax ID No (NIP);
- Statistical ID No (REGON);
- ID card/passport series and number, date of issue of the ID card/passport, expiry date of the ID card/passport of a counterparty or their employee;
- data contained in public registers (such as e.g. the National Court Register);
- information about powers of attorney and employees' rights to represent a counterparty;
- numbers of authorisation cards and documents confirming certain entitlements.

Personal data may be processed if:

- **we are doing it to conclude and perform agreements between us and a data subject;**
- **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 required to meet specific obligations in line with legal provisions, such as the Banking Law, he Act on trading in financial instruments, the Act on Accounting and the Tax Code;
- **it is required by our (controller's) legitimate interest, i.e. in situations where:**
  - we are managing an agreement between a counterparty or their employees and us, including in the event of exercising claims;
  - we are verifying the competences of a counterparty or their employees;
  - we are checking the performance of an agreement;
  - we are managing the granting of permissions to the bank's IT systems.

Where do we get the data we process from?

We process data of a data subject which has been provided to us by counterparties before the conclusion of an agreement and during its performance. These data subjects are the counterparties themselves and their employees. We can also use data that has been provided to us by other controllers or has been obtained from publicly available databases (e.g. Central Registration and Information on Business, CEIDG).

Data profiling

We do not profile data of counterparties or their employees.

Information obligations vis-à-vis counterparties and their employees (data subjects)

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

When do we inform?

If we collect data directly from the data subject, we provide such information in the content of an agreement. If data originates from another source, we communicate such information to the data subject within a reasonable time, no later than one month from the collection of the data. We may do that through our counterparties. We do not do that when the provision of information proves impossible or would require a disproportionate effort.

How do we inform?

- In the information clauses that we include in agreements or deliver together with an agreement;
- Either personally or by telephone, in the course of 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 respect them?

Right of access to data

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

The data subject has the right 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 we plan to process their data (if we can define a time period) or on the basis of what criteria we determine that period.

Right to data rectification

A counterparty or their employee may request that we immediately rectify their inaccurate personal data or complete their incomplete data.

Right to data erasure (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 we collected it,
- the data has been processed in violation of the GDPR or other legal regulations.

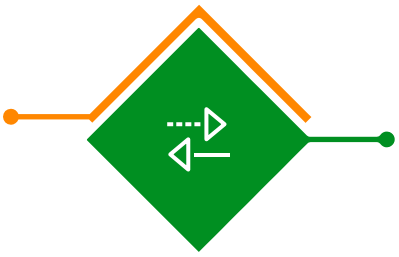
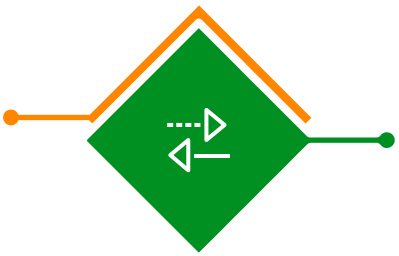
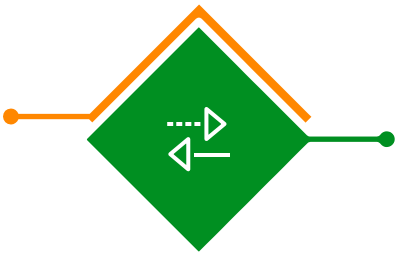
We will take the request into account if – in our opinion – there are no legitimate grounds for us to continue the processing.

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

We will process the request as soon as possible considering the circumstances and technical capabilities.

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 cases:

Situation		Our action
The accuracy of data processed by us is contested by the data subject.		We verify whether the data is correct and propose its correction.
The data subject believes that we process their data unlawfully and demands that we restrict its use (but opposes to its 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 establishment, exercise or defence of legal claims.		We will restrict the processing of such data, mark the respective data and will not erase it until the data subject cancels their restriction request.
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).		We will analyse the situation and ask the counterparty or their employee to specify a particular purpose they are opposing to.

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 ourselves against legal claims.

Right to object to processing

A data subject may object to our processing of their personal data that is based on our legitimate interest. The data subject shall each time indicate to us what specifically they are objecting to. We will implement 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?

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 might have occurred a risk to the rights and freedoms of natural persons	without undue delay, as far as technically feasible, no later than within 72 hours after the identification of the breach.

To whom and for what purpose can we transfer counterparties' and their employees' data?

According to law, counterparties' data is published at: https://www.mbank.pl/o-nas/informacje-wymagane-przepisami-prawa/.

We may transfer counterparties' and their employees' data to:

- the institutions that supervise us (e.g. **Polish Financial Supervision Authority, Personal Data Protection Office**);
- law enforcement authorities (e.g. Police, Public Prosecutor's office);
- entities with whom we have concluded personal data processing agreements.

Rules for transferring data outside Poland

Where there are grounds for it, we may transfer personal data 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 consists in the fact that the European Commission recognises a given country as providing adequate protection.

We may transmit 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. You can obtain information about such solutions or, in cases where it is possible, their copy by contacting us.

Personal Data Officer at mBank

We have appointed a Personal Data Officer – Ms Agata Rowińska.
Contact with the Personal Data Officer:

▼

by e-mail:
inspektordanychosobowych@mbank.pl

▼

by post to:
Personal Data Officer
mBank S.A.
ul. Prosta 18, 00-850 Warszawa

How to file a complaint regarding the protection of one's personal data

If a data subject suspects that their data is being processed in breach of the GDPR, they may lodge a complaint with the Personal Data Protection Office in the manner described on the website www.uodo.gov.pl.

How long do we process data?

We process data for as long as is necessary to achieve the purpose of the processing, i.e.:

- for 6 months, if the bank, for any reason, refuses to grant the powers to perform the activities contracted in an agreement concluded with a counterparty;
- for not more than 7 years after termination/end of an agreement with a counterparty (in case of a court case) or to fulfill a legal obligation;
- 90 days for security camera footage after it's recorded.

We apply the principle of restricting the storage of personal data, which safeguards data against its processing for an unlimited period. When we achieve the purpose of processing, we erase or anonymise the data; this makes data recovery impossible.

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 Corporate Income Tax Act, etc.) have expired.

Useful documents and information:

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