

GDPR Package for Clients Using the Services of the Brokerage Bureau of mBank S.A.

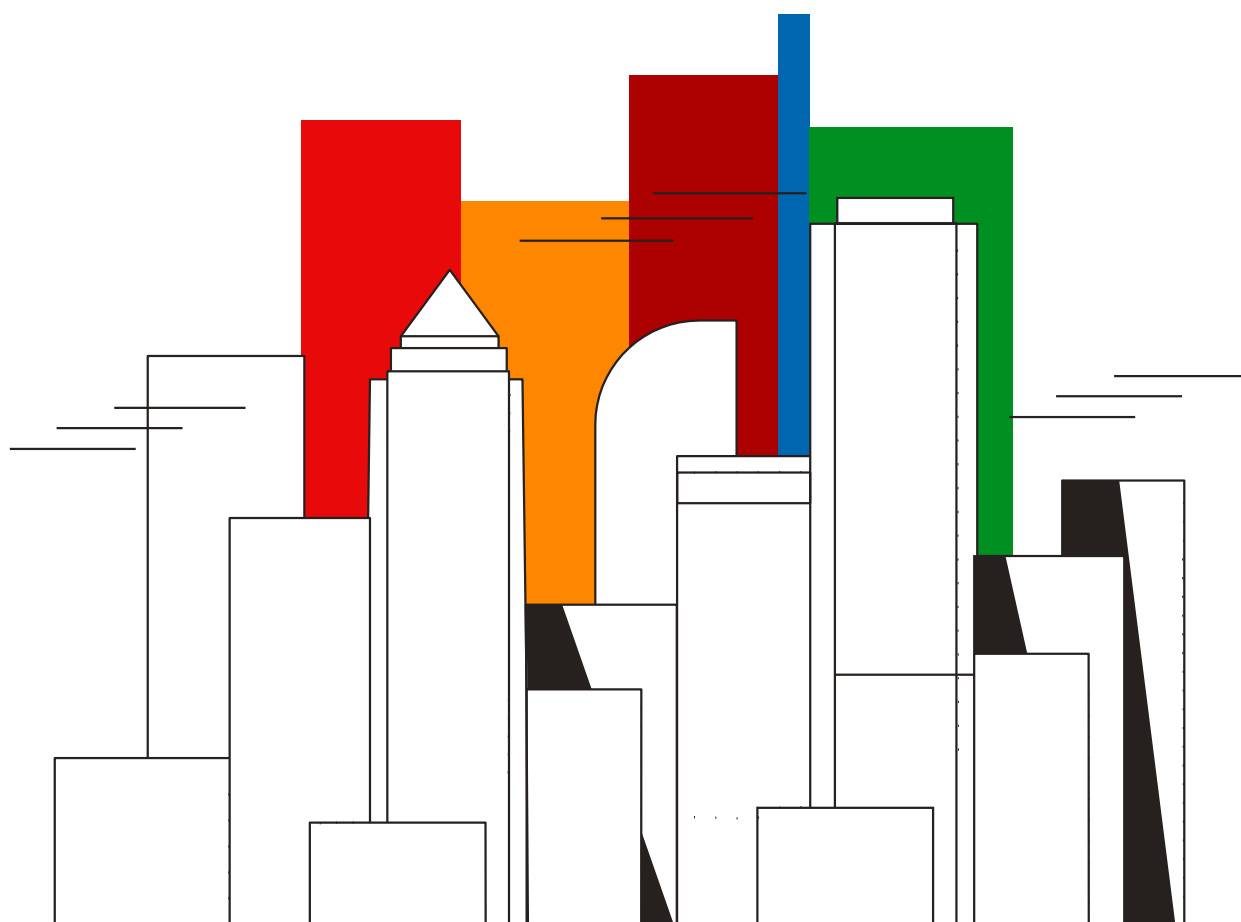


Table of Contents

GDPR: General information.....	3
How do we communicate with clients?	4
GDPR: Basic principles	5
How do we process personal data? General information	6
What data do we process, and on what basis?	6
Where do we get the data we process?	8
Automated decision-making	8
Data profiling.....	9
Obligations to provide information to data subjects	10
What are the rights of data subjects and how do we guarantee them?	11
Right of access.....	11
Right to rectification	11
Right to erasure (right to be forgotten)	11
Right to restriction of processing	12
Right to portability	12
Right to object to processing.....	13
Procedure for the exercise of rights (after successful identification of the data subject):	13
For how long do we process data?	16
To what entities may we disclose data of our clients?	16
What principles do we apply when transmitting clients' data outside Poland?	16
Handling personal data breaches.....	16
mBank's Data Protection Officer	17
How to lodge a complaint concerning personal data protection?	17
Useful documents and information	17



GDPR: General information

GDPR

means 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.



GDPR has been directly applied by the EU member states since 25 May 2018.

Glossary:

Controller	a person or entity which (alone or jointly with other controllers) determines the purposes and means of personal data processing. mBank S.A. with its registered office in Warsaw is a controller of personal data. In mBank's structure, there is an organisational unit operating under the name "the Brokerage Bureau of mBank", through which we provide brokerage services to our clients.
Automated decision-making	decision-making without human intervention based on models and algorithms developed in IT systems.
Personal data	any information which identifies or allows the identification of a natural person. It includes in particular: first name and surname, client identifier (client ID), contact details, date of birth, tax identification number (NIP), personal identification number (PESEL), image recorded on a CCTV system, etc.
Data subject	a client of the Brokerage Bureau, a prospective client of the Brokerage Bureau or a natural person related to a client, e.g., a client's attorney-in-fact, representative, proxy, beneficiary or beneficial owner.
Processor	a person or an entity who/which processes personal data on behalf of the controller.
Profiling	automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a client.
Personal data processing	any operation performed 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.

Any terms which are not defined here are understood as defined in the Private Banking or Brokerage Bureau rules.

How do we communicate with clients?

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:

- **at the Brokerage Service Point**

- as regards services provided by the Brokerage Bureau of mBank, at ul. Prosta 18 in Warsaw,

- **at Private Banking & Wealth Management Branches**

- as regards wealth management services the list of branches is available at www.mbank.pl/placowki-bankomaty/#private-banking_placowki.

Agreements with each client specify the agreed forms of communication.

mBank's contact data:

ul. Prosta 18, 00-850 Warszawa

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

www.mbank.pl

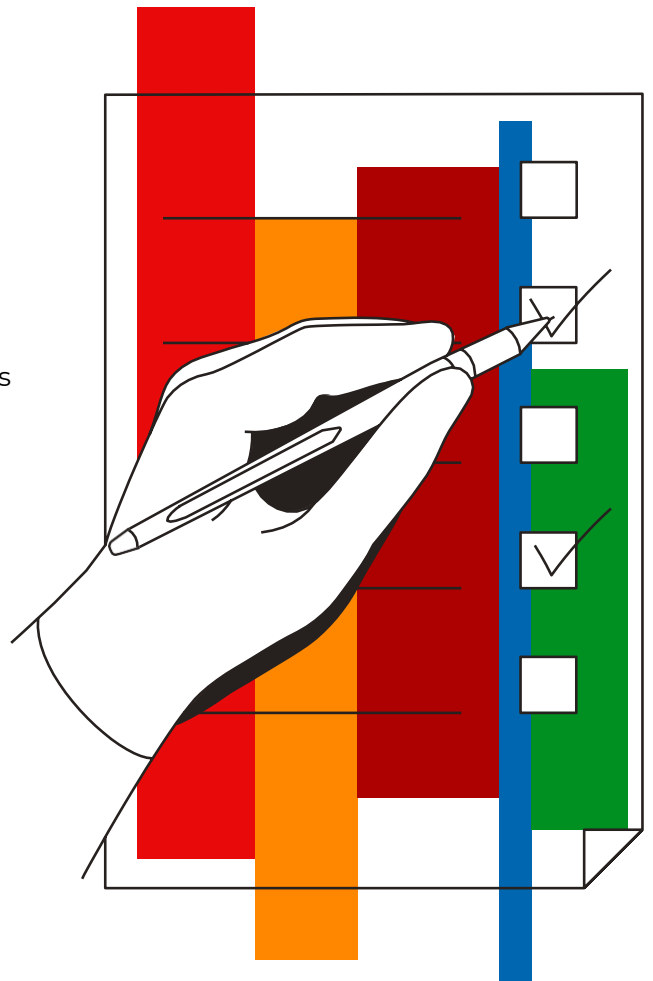




GDPR: Basic principles

GDPR defines six principles of data processing, which we follow whenever we process personal data. These include:

- **principle of lawfulness, fairness and transparency:**
we process personal data in accordance with the law. We inform our clients about all related matters exhaustively via the agreed communication channels in a simple language to make sure that data subjects understand that we collect, store or otherwise process their personal data,
- **principle of data minimisation and adequacy:**
we only process the data that are actually needed (adequate, relevant) to achieve a given purpose,
- **principle of data accuracy:**
we spare no effort to ensure that the data we process are true, up to date and accurate. This is why we may ask clients 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, contact data, address, etc.),
- **principle of purpose and storage limitation:**
we collect personal data solely for specified, explicit and legitimate purposes which could not be achieved otherwise. We store data in a form which permits the identification of data subjects. 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 technical or 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, apply the principle of data protection by design (e.g. in development of a new product) and data protection by default.





How do we process personal data? General information

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,
- gender, PESEL, date, city and country of birth, citizenship, address of residence or registered address, mailing address, email, phone number,
- client identifier (client ID),
- financial data (bank account number or investment account number, income, information on products and services),
- education, profession and occupation,
- tax identification number (NIP) or tax identification number in a jurisdiction other than Poland, statistical number (REGON),
- series and number of the client's identity card/passport/permanent residence card/other identity document, its date of issue and expiry date,
- image recorded on the bank's CCTV systems or image acquired at the stage of establishing a business relationship with the bank,
- online identifier (IP address), 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 that we need to offer our products and services.

We may process personal data:

- **if the data subject has given their consent:**
we process data on that basis for the purposes of marketing of products and services provided by entities other than the bank and our group members (marketing of services of the bank and our group members requires no consent);
- **when we process applications or implement agreements, including when:**
 - we process applications for bank products,
 - we present recommendations, analyses and other analytical and information materials, periodic reports and confirmations,
 - we handle complaints,
 - we communicate with a client's attorneys-in-fact or representatives;

■ **if this is required to fulfil our legal duty:**

- we process data on that basis in particular to prevent fraud and protect security of transactions. We are bound by specific obligations defined in particular legal regulations (including: Banking Law Act, Act on Combating Money Laundering and Terrorism Financing, Act on Trading in Financial Instruments, Tax Ordinance Act, Act on Personal Income Tax, Act on Handling Complaints by Financial Market Entities and on the Financial Ombudsman, Accounting Act, Act on the Performance of the Agreement 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, Act on Tax Information Exchange with Other Countries (CRS)),
- we assess the adequacy and suitability of offered services and financial instruments, and classify clients to target groups of buyers of financial instruments;

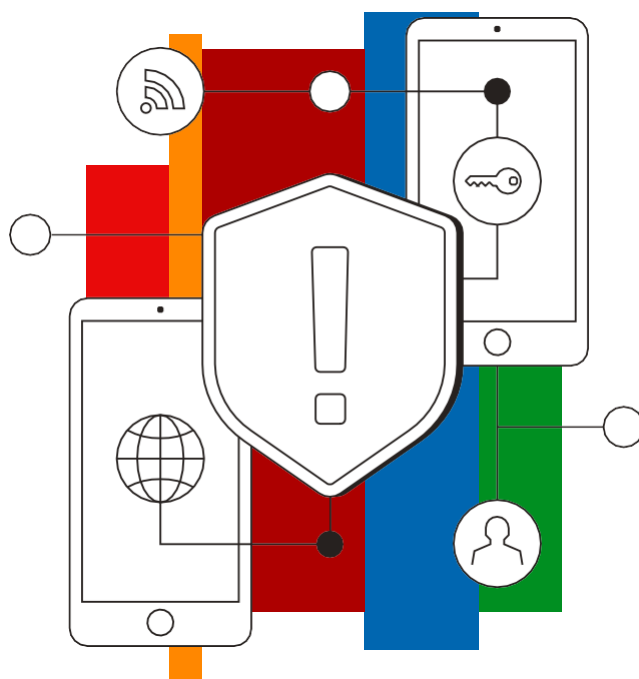
■ **on grounds of our legitimate interest (as a controller), i.e. whenever:**

- we provide banking system functionalities based on profiling, including in electronic banking systems (online banking, mobile app), customised to the needs of each client,
- we 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/>),
- we make a customised marketing offer,
- we establish and exercise legal claims or defend against legal claims,
- we generate statistics and reports,
- we develop, monitor and change internal approaches as well as approaches and models relating to prudential requirements, including operational risk,
- we survey customer satisfaction,
- we develop or modify our product range and our operating plans and strategy,
- we archive information,
- we prevent and detect crime (protect security).

Processing children's data:

We offer no special brokerage products to children and teenagers. We may process children's data where a child is named as a beneficiary of a pension savings account (IKE or IKZE) or acquires financial instruments through inheritance or donation.

To protect children's data, we always seek consent from parents (or legal guardians) to their children using such services.





Where do we get the data we process?

We process data provided by data subjects in dedicated forms at the stage of entering into an agreement with us. We check such data against the identification documents presented by data subjects to ensure correct identification. We also use the Identity Card Register (RDO) and the PESEL database. In addition, we obtain copies of identification documents or other documents confirming identity in selected processes.

We may also use data transmitted by other controllers (e.g. the Polish Financial Supervision Authority, the Ministry of Finance, law enforcement services), data we source from public databases (e.g. Central Registration and Information on Economic Activity CEIDG or the National Court Register), and data we receive from our clients in the performance of legal obligations.

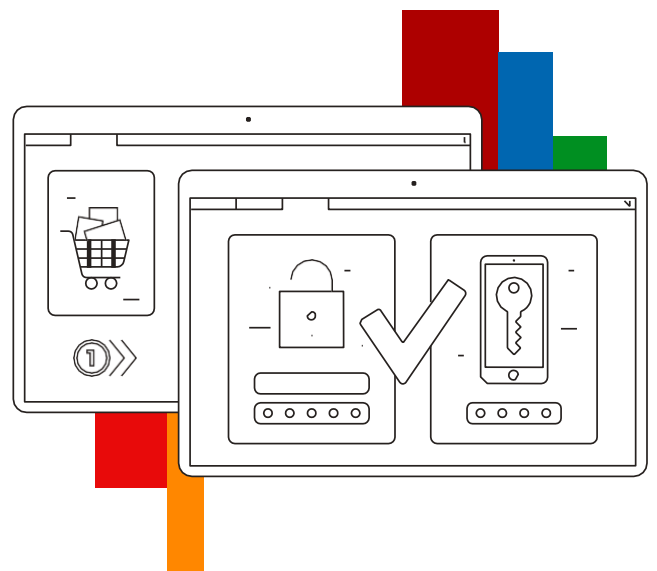
As regards beneficial owner data, we receive such information from our clients' representatives. We may receive clients' data from other financial institutions which provide services to such clients and open a brokerage account on behalf of the clients with our Brokerage Bureau.



Automated decision-making

Automated decision-making means that decisions concerning clients are made without human intervention based on models and algorithms.

Our Brokerage Bureau does not apply automated decision-making.





Data profiling

Data profiling means that we use algorithms or mathematical models to analyse clients' personal profiles. 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).

When profiling, we use data provided by clients as well as data collected in our IT systems (e.g. transaction history).

Why do we use profiling?

We use profiling to fulfil our legal duties, which oblige us to:

- prevent crime to the detriment of our bank and our clients,
- prevent fraud, money laundering and terrorism financing, and develop models to recognise such crime,
- prevent any instances of clients being offered financial products or services of the Brokerage Bureau which are not suitable for them; alert clients who want to acquire financial products or services which we believe are not suitable or for which a given client is not in the target group considering the client's investment profile.

We use profiling in the pursuit of our legitimate interests when:

- we engage in direct marketing by e.g. preparing and sending customised product offer to clients,
- 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).





Obligations to provide information to data subjects

All the information on processing and protection of personal data is available at all times to data subjects on our website www.mbank.pl/rodo. We are happy to address any questions of data subjects in this regard. We also provide individual information when we collect data and when we change the purposes of processing.

When do we provide information?

Whenever we collect personal data directly from a data subject, we inform them of it 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 have collected the data,
- no 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 information:

- in information notices (in documents addressed to a given data subject) or via online banking or mobile app,
- in person or by phone, in a conversation with the bank's representative,
- electronically, also by publishing such information on our websites: www.mbank.pl, www.mdm.pl or www.mforex.pl.





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

Right of access

Each 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 have disclosed (or may disclose) the data; this applies, in particular, to recipients in countries outside the European Economic Area or international organisations,
- how long we are planning to process personal data (if that can be established) or on what basis we have defined such period.

The right of access to data may be exercised via electronic or hard copy means, upon positive identification of a data subject.

We send our reply to the address saved in the systems of the Brokerage Bureau.

Right to rectification

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

Right to erasure (right to be forgotten)

Each data subject may request that we erase their 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.

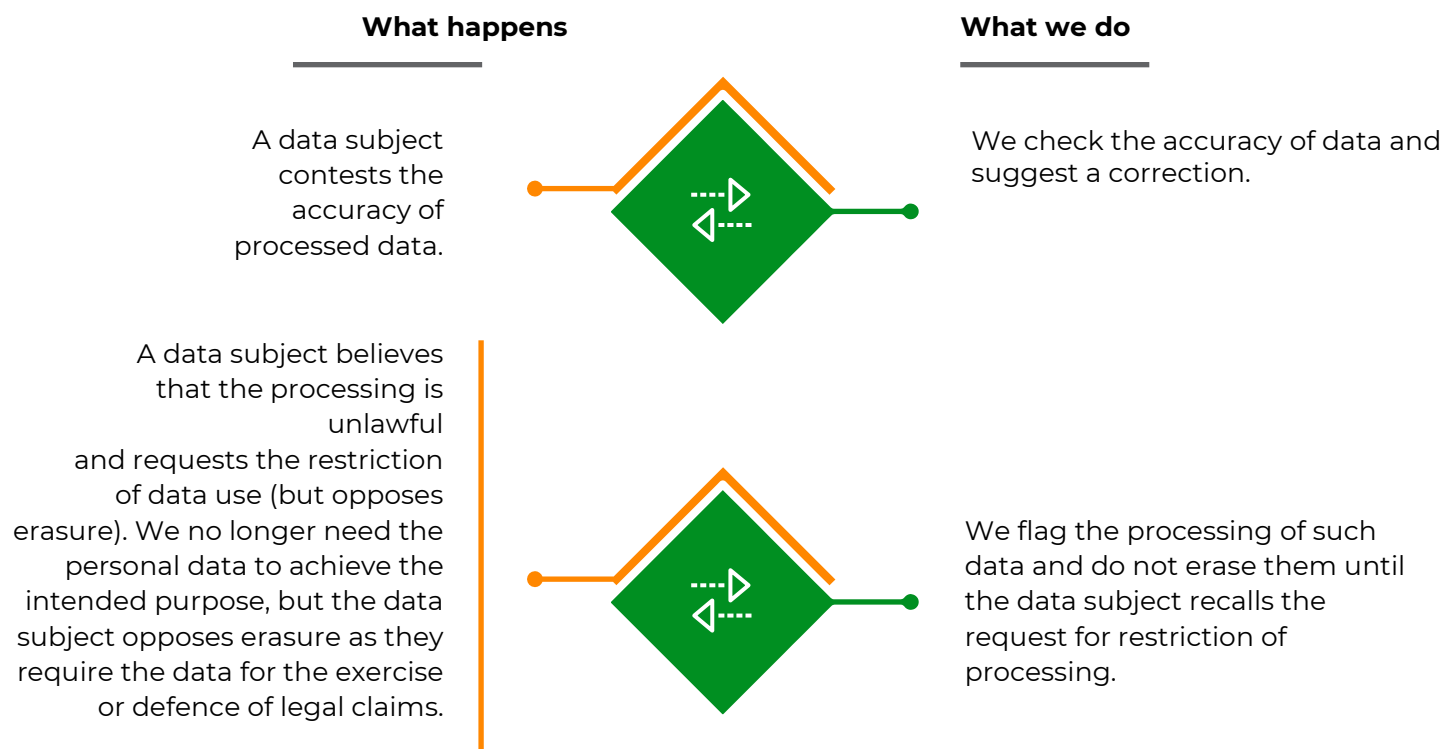
In order to stop processing personal data, we need to receive the data subject's statement which defines their wishes. We will honour such request if we establish that we are not legally bound to continue the processing despite the request.

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

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

Right to restriction of processing

Each data subject may also request us to restrict the processing of their data. The right applies in the following cases:



Right to portability

Each data subject has the right to transfer their data. We transmit data directly to the requesting data subject who is then able to transmit the data to another entity (there are no standards for secure data transfers between controllers).


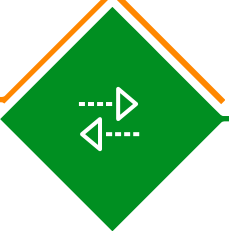

We transmit data in encrypted email messages (in the format agreed by investment companies as part of arrangements of the Chamber of Brokerage Houses). The dataset includes the data provided by the data subject as well as the data generated as a result of their actions (including transaction data). We do not disclose data which we have generated on our own (e.g. when rating creditworthiness or classifying a client to a target group of buyers of financial instruments).

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.

Right to object to processing

Each data subject has the right to object to our processing of their personal data where the data are processed in the pursuit of our legitimate interest.

The data subject must each time indicate the type of objection.

Type of 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 activities addressed to the client, including marketing activities based on profiling.
Objection on grounds relating to the data subject's particular situation (where data are processed in the pursuit of our legitimate interest).		We analyse each case and, if we find the objection to be justified, we no longer process such data.

We process each objection as soon as technically possible.

Procedure for the exercise of rights (after successful identification of the data subject):

■ eMakler service:

Right	Where can data subjects exercise the right?					
	mLinia	Chat	Branch	mFinanse	Online banking	Mobile app
Right of access	✓	✗	✗	✗	✗	✗
Right to portability	✓	✗	✗	✗	✗	✗
Right to data completion/rectification	✓	✗	✗	✓	✓	✗
Right to restriction of processing	✓	✗	✗	✗	✗	✗
Right to be forgotten/data erasure	✓	✗	✗	✗	✗	✗
Right to object to processing/profiling of data for marketing purposes	✓	✓	✗	✓	✗	✗

■ **brokerage account held with the Brokerage Bureau of mBank, mForex:**

Right	Where can data subjects exercise the right?					
	Brokerage Bureau's helpline	Chat	Branch	Online banking	Mobile app	Brokerage Service Point
Right of access	✓**	✗	✗	✗	✗	✓
Right to portability	✓**	✗	✗	✗	✗	✓
Right to data completion/rectification	✓**	✗	✗	✓	✓*	✓
Right to restriction of processing	✓**	✗	✗	✗	✗	✓
Right to be forgotten/data erasure	✓**	✗	✗	✗	✗	✓
Right to object to processing/profiling of data for marketing purposes	✓**	✗	✗	✓****	✗	✓

* only for brokerage accounts, change of contact details

** only for existing clients of the Brokerage Bureau of mBank

**** only for mForex clients

■ **Wealth Management services:**

Right	Where can data subjects exercise the right?					
	Call Centre PB	Chat	Branch	Online banking	Mobile app	Private Banking & Wealth Management Branch / Brokerage Service Point
Right of access	✗	✗	✗	✗	✗	✓
Right to portability	✗	✗	✗	✗	✗	✓
Right to data completion/rectification	✗	✗	✗	✓****	✗	✓
Right to restriction of processing	✓****/✗	✗	✓****/✗	✗	✗	✓
Right to be forgotten/data erasure	✗	✗	✗	✗	✗	✓
Right to object to processing/profiling of data for marketing purposes	✓****/✗	✗	✓****/✗	✓****	✗	✓

*** provided that the client also uses private banking services

- **Services for financial institutions:**

clients being financial institutions may exercise their rights through their employees and representatives via phone, messengers (Bloomberg, chat) or directly with employees of the Brokerage Bureau's Institutional Sales Department.





For how long do we process data?

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

- for five years where no agreement has been concluded,
- for no more than 10 years after termination of an agreement (in case of a legal dispute or for purposes of compliance with a legal obligation),
- for 90 days from the day on which a CCTV image was recorded.

We follow the principle of storage limitation which protects personal data from being processed for an unlimited period of time. When we have achieved the purpose of processing, we erase or anonymise data (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).



To what entities may we disclose data of our clients?

As regards brokerage services, financial market regulations and guidelines allow us to transmit data to other entities in order to:

- conclude and perform an agreement,
- conclude transactions or place orders/subscriptions for financial instruments,
- exercise and discharge legal rights and obligations.

In particular, we may transmit personal data to entities such as:

- **investment fund companies, insurance companies, investment companies, issuers of financial instruments** in connection with exercise of legal obligations or a client's agreement with such an entity,
- **the Ministry of Finance, the Polish Financial Supervision Authority, the relevant exchange** – regulated market and other trading venues, **the Central Securities Depository of Poland, tax offices, the National Bank of Poland, the Bank Guarantee Fund**, pursuant to applicable law,
- **entities with which we have signed agreements on provision of services for our benefit and which we have entrusted with data processing**

(e.g. investment company agents whose list is available at <https://www.mbank.pl/pdf/pb/bank/grupa/informacja-o-agentach-firmy-inwestycyjnej-wykonujacej-czynnosci-posrednictwa-na-rzecz-mbanku-sa.pdf>).



In special cases, we transfer personal data to other investment companies when we provide the service of managing portfolios of financial instruments under an authorisation granted. The list of controllers to whom we disclose personal data in order to provide that service is presented in our periodic reports concerning the service of managing portfolios of financial instruments (for financial instruments held) and on our website.



What principles do we apply when transmitting clients' 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.

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>.



Handling personal 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 should we do it?

Data subject	if we believe that the risk to the rights and freedoms is high,	immediately (where it is extremely difficult to provide the information directly, we issue a public statement).
Supervisory authority	if we believe that the rights and freedoms of natural persons may have been infringed (and the probability is greater than low)	immediately, depending on technical capacity, no later than within 72 hours from identification of the breach.



mBank's Data Protection Officer

We have appointed Anna Hermanowicz 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 Warszawa



How to lodge a complaint concerning personal data protection?

If a client believes that their data are processed in violation of GDPR, the client has the right to lodge a complaint with the personal data protection supervisor according to the procedure described on its website: <http://www.uodo.gov.pl>.



Useful documents and information

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

