GDPR Pack

for mBank S.A. Private Banking
and Brokerage Office clients

Table of contents

GDPR – General

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

Its full name is: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

What is the purpose of GDPR?

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

Glossary:

Controller – means the person or entity which (alone or jointly with others) determines the purposes and means of the processing of personal data. mBank S.A. with its seat in Warsaw is a personal data controller.

Automated decision-making – means decision-making without human intervention based on models and algorithms developed in IT systems.

Personal data – tmeans any information relating to an identified or identifiable natural person, including: first name and surname, client ID, contact details, date of birth, tax ID (NIP), personal ID (PESEL), credit history, bank account number, visual monitoring image, etc.

Data subject – means a Private Banking or Brokerage Office client, a prospective Private Banking or Brokerage Office client, a natural person related to a client, e.g., a client's representative, proxy, beneficiary, beneficial owner.

Processor – means a person or entity which processes personal data on behalf of and for the controller.

Profiling – means automated processing of personal data which uses personal data to evaluate certain personal aspects relating to a client.

Processing – means any operation on personal data, either automated or manual. We process data whenever we collect, record, organise, structure, store, adapt or alter, retrieve, consult, use, disclose (e.g. transmit), disseminate, align or combine, restrict, erase or destroy data.

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

How do we communicate with data subjects?

We communicate with data subjects on all matters, including personal data, via our website, transaction service, by email, phone and mail, and at our branches:

- Private Banking & Wealth Management Branches – to the extent of private banking and wealth management services (the list of branches is available at https://www.mbank.pl/placowki-bankomaty/#private-banking_placowki);
- Punkty Usług Maklerskich – w zakresie usług Biura maklerskiego mBanku (lista placówek dostępna jest na stronie www.mdm.pl/ui-pub/site/kontakt/punkty_uslug_maklerskich).

The agreement with each data subject specifies the agreed forms of communication.

mBank's contact details:
ul. Prosta 18, 00-850 Warsaw
phone: (22) 829-00-00,
fax (22) 829-00-33

www.mbank.pl

How to call mLine?

mLinia dostępna jest 24h/dobę 7 dni w tygodniu

- **801 300 800** – z telefonów komórkowych i stacjonarnych z całego świata;
- **+48 42 6 300 800** – z telefonów stacjonarnych na całym świecie;
- **783 300 800** – z telefonów komórkowych.

GDPR principles

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

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

How do we process personal data

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;
- PESEL, date, city and country of birth, birth name, mother's birth name, father's and mother's first names, marital status, citizenship, mailing address, address of residence or registered address, country of residence, tax identifier (NIP) or tax identification in a jurisdiction other than Poland (TIN), gender, email, phone number, education, profession and occupation;
- data disclosed in identification documents (identification card or its copy, e-ID, passport or its copy, residence permit or its copy), series and number of the identification document, date of issue and expiry date;
- financial data (bank account number or investment 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);
- client identifier (client ID);
- image recorded by the bank's monitoring systems when establishing the business relationship;
- data concerning our communications;
- the client's location data, 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 necessary to offer our services.

We may process personal data provided that:

- **the data subject has given his or her consent:** we process data on that basis for the purposes of marketing of products and services of providers other than the bank and our group members (marketing of services of the bank and our group members requires no consent);
- **we process applications and perform agreements between us and the data subject, including whenever we**:
  - determine creditworthiness to process a loan application;
  - process applications for bank products;
  - present recommendations, research, other research and information materials, periodic reports and confirmations,
  - process complaints;
  - communicate with the client's proxy or representative;

- **we comply with a legal obligation:**
  - we process data on that basis in particular to prevent fraud and protect security of transactions. We are subject to specific legal obligations under the Banking Law; the Act on Anti-Money Laundering and Combatting the Financing of Terrorism; the Act on Trading in Financial Instruments; the 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);
  - we assess the adequacy and suitability of offered services and financial instruments, including the classification of clients according to target groups of buyers of financial instruments;
- **for the purposes of our legitimate interests (as a controller),** i.e. whenever we:
  - develop an adequate and secure risk model for a loan portfolio and rate creditworthiness;
  - provide banking system functionalities based on profiling, including in electronic banking systems (transaction service, mobile application), customised to the needs of each client;
  - 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/informacje-wymagane-przepisami-prawa/);
  - present an individual marketing offer;
  - establish, enforce or defend claims;
  - generate statistics and reports;
  - develop our statistical models and operational risk assessments;
  - survey customer satisfaction;
  - develop or modify our offer and the bank's operating plans and strategy;
  - sell debt;
  - keep data records;
  - prevent and detect crime (protect security).

Special personal data:

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

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

Processing children's data:

We offer no special Private Banking or Brokerage Office products to children and young people. We may process children's data where a child is named as a beneficiary of a bank account or a pension savings account (IKE or IKZE) or acquires financial instruments through inheritance or donation. To protect the rights of children, we always ask the consent of the parents (or legal guardians) for children to use such services.

Where do we get the data we process?

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

We may also use data transmitted by other controllers (e.g. Biuro Informacji Kredytowej S.A., the Polish Financial Supervision Authority, the Ministry of Finance, law enforcement services), data we source from public databases (e.g. Central Business Register CEIDG), and data we receive from our clients in the performance of legal obligations.

We may receive clients' data from other financial institutions which serve such clients and open a brokerage account for the client with our Brokerage Office.

Automated decision-making

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

For example, in Private Banking, we use automated decision-making to grant loans. We automatically rate the client's creditworthiness, credit history, and relations 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:

- the system Bankowy Rejestr 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 loan application and later when we issue our decision. Clients may appeal against such decisions via the mLine or at a Private Banking & Wealth Management Branch.

Our Brokerage Office services use no automated decision-making.

Data profiling

Data profiling means that we use algorithms or mathematical models to analyse clients' features, preferences, and future behaviour. We use the appropriate (technical and organisational) measures to mitigate the risk of error in profiling. We use best efforts to ensure that our assessment is objective and our processes are non-discriminatory. Our statistical models comply with the good practice of the banking industry (including Recommendation W of the Polish Financial Supervision Authority KNF).
Our profiling uses data provided by the client as well as data maintained in our IT systems (e.g. transaction history).

Why do we use profiling?

We use profiling to discharge our legal obligations:

- we protect the security of assets and transactions;
- we prevent money laundering and financing of terrorism, we develop models to recognise such crime;
- we decide which products and services do not match the needs of customer groups and we do not offer them in order to protect clients from misselling of financial products;
- we monitor the quality of granted loans in order to manage the risk of retail credit exposures effectively;
- we prevent the offering of financial products or services of the Brokerage Office which are not suitable for a client; we alert clients who want to purchase financial products or services which we believe are not suitable or where the client is not in the target group considering the client's investment profile.

We use profiling whenever necessary to conclude or perform a contract:

When a client applies for a loan or for modification of the terms of a loan, we rate the client's creditworthiness in order to ensure an appropriate and secure risk profile of the bank. For that purpose, we may issue queries to third-party databases.

We use profiling to pursue our legitimate interests:

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

Obligation to inform data subjects

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

When do we provide information?

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

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

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

How do we provide information?

We may provide information:

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

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

Right to access data

Each data subject has the right to be informed by the bank whether we process his or her personal data. Such requests may be lodged with the mLine or at a Private Banking & Wealth Management Branch. We will send our reply to the address maintained in our database.

The data subject has the right to know:

- why we process specific data;
- what data we process;
- to what recipients or categories of recipients we have disclosed (or may disclose) data, in particular recipients in countries outside the European Economic Area or international organisations;
- how long we are planning to process data (if that can be established) or the criteria on the basis of which we define that period.

Right to rectification

Each data subject may request that we immediately rectify his or her inaccurate personal data or complete his or her incomplete personal data. Depending on the type of data, rectification may be requested at a Private Banking & Wealth Management Branch, via the transaction system or the mobile application.

Right to erasure (right to be forgotten)

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

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

To stop processing personal data, we need to receive the data subject's request which defines the data subject's wishes. We will execute such request if, in our opinion, we have no reasonable legal basis not to do so.

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 request us to restrict the processing of his or her data. The right applies if the data subject:

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

Right to portability

Each data subject has the right to transmit his or her data. We transfer data directly to the requesting data subject as necessary 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 banks in the Polish Bank Association ZBP or by investment firms in the Chamber of Brokerage Houses IDM). The dataset includes data provided by the data subject and data generated as a result of his or her actions (including transaction data). We do not disclose data which we have generated (e.g. when rating creditworthiness or classifying the client in a target group of purchasers 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.

The right to object

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

Objection	What we do
Objection to marketing based on profiling.	We no longer prepare and present offers customised to the client's needs and situation.
Objection to marketing of products and services of the bank and members of our group.	We no longer engage in any marketing addressed to the client, including marketing based on profiling.
Objection to functions of the bank's systems based on profiling.	We deactivate those functions of our electronic banking systems (transaction system, mobile application) which are based on profiling (advanced transaction history, payment assistant, etc.).
Objection to the development of the bank's appropriate and safe risk profile by rating the clients' creditworthiness, including querying third-party databases.	The client may only object due to his or her special situation (and should describe it). We analyse each case and, if we find the objection to be reasonable, we no longer process such data for that purpose.
Objection for reasons of the data subject's special situation (with regard to data processing based on legitimate interest).	We analyse each case and, if we find the objection to be reasonable, we no longer process such data.

We process any objection as soon as technically possible.

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

- Private Banking services:

Right	Where can data subjects exercise the right?					
	PB call centre	Chat	Branch	Transaction service	Mobile app	Private Banking & Wealth Management Branch
Right of access	no	no	no	no	no	yes
Right to portability	no	no	no	no	no	yes
Right of rectification	no	no	no	yes*	yes*	yes
Right of restriction of processing	yes	no	yes	no	no	yes
Right of erasure (right to be forgotten)	no	no	no	no	no	yes
Right to object to data processing/ profiling for purposes of marketing	yes	no	yes	no	no	yes

*applicable to part of the customer's data

- Wealth Management services:

Right	Where can data subjects exercise the right?					
	centrum telefoniczne PB	Chat	Placówka banku	Serwis transakcyjny	Aplikacja mobilna	Oddział Bankowości Prywatnej &Wealth Management / Punkt Usług Maklerskich
Right of access	no	no	no	no	no	**yes**
Right to portability	no	no	no	no	no	**yes**
Right of rectification	no	no	no	**yes*/no**	**yes*/no**	**yes**
Right of restriction of processing	**yes*/no**	no	**yes*/no**	no	no	**yes**
Right of erasure (right to be forgotten)	no	no	no	no	no	**yes**
Right to object to data processing/ profiling for purposes of marketing	**yes*/no**	no	**yes*/no**	no	no	**yes**

*provided that the client also used private banking services

- eMakler services:

Right	Where can data subjects exercise the right?					
	mLine	Chat	Branch	mFinanse	Transaction service	Mobile app
Right of access	yes	no	no	no	no	no
Right to portability	yes	no	no	no	no	no
Right of rectification	yes	no	no	yes	yes	no
Right of restriction of processing	yes	no	no	no	no	no
Right of erasure (right to be forgotten)	yes	no	no	no	no	no
Right to object to data processing/ profiling for purposes of marketing	yes	tak yes	no	yes	no	no

- mBank Brokerage Office investment accounts, mForex:

Right	Where can data subjects exercise the right?					
	Infolinia Biura maklerskiego	Chat	Placówka banku	Serwis transakcyjny	Aplikacja mobilna	Punkt Usług Maklerskich
Right of access	no	no	no	no	no	yes
Right to portability	no	no	no	no	no	yes
Right of rectification	no	no	no	yes	yes*	yes
Right of restriction of processing	yes**	no	no	no	no	yes
Right of erasure (right to be forgotten)	no	no	no	no	no	yes
Right to object to data processing/ profiling for purposes of marketing	yes**	no	no	yes***	no	yes

* only for brokerage accounts, change of contact details
** only for existing clients of mBank Brokerage Office
*** only for mForex clients

- services for Financial Institutions: the right may be exercised by phone, messenger (Bloomberg, chat) or directly with employees of mBank Brokerage Office Institutional Sales Department.

For how long do we process data?

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

- six months if we conclude no agreement concerning Private Banking deposit services or Brokerage Office services;
- five years if we conclude no agreement concerning Private Banking lending services;
- 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).

We follow the principle of storage limitation which protects data from processing for an unlimited period of time. When we have achieved the purpose of processing, we erase or anonymise data, which means that such data may no longer be recovered.

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

Private Banking services

According to the regulations, 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 such data to institutions including:

- **Biuro Informacji Kredytowej,** for more information, visit https://www.mbank.pl/pdf/rodo/klauzula-informacyjna-bik.pdf;
- **Ministry of Finance,** (we send monthly transaction logs to the General Inspector of Financial Information GIIF in accordance with the anti-money laundering and financing of terrorism regulations);
- **the Office of Competition and Consumer Protection (UOKiK), the Financial Supervision Authority (KNF), the Financial Ombudsman, the National Revenue Administration (KAS),** in accordance with applicable regulations;
- **our outsourcing contractors under the Banking Law** (in particular, our lending 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 the consent of the data subject);
- **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).

Brokerage Office services

According to financial market regulations and guidelines, we may transfer 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.

We may in particular transfer personal data to entities including:

- investment fund companies, insurers, investment firms, issuers of financial instruments in connection with compliance with a legal obligation or a client's agreement with such entity;
- other institutions authorised by law to collect data in connection with our brokerage activities (including mainly the Ministry of Finance, the Polish Financial Supervision Authority, the relevant exchange – regulated market or trading venue, the Central Securities Depository of Poland KDPW, tax offices);
- entities which sign an agreement with mBank to provide services to us and to process data on our behalf (e.g., investment firm 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).

As a special case, we transfer personal data to other investment firms when we provide the service of managing portfolios of financial instruments according to an authorisation granted. The list of controllers to whom we transfer personal data to provide that service will be presented in our regular reports concerning the service of managing portfolios of financial instruments (for financial instruments held) and on our website.

Data transmission outside Poland

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

We may transfer personal data to other third countries without the consent of Poland's personal data protection supervisor provided that our agreements with entities in such countries include special solutions provided by law or approved by Poland's personal data protection supervisor.

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

Handling data breaches

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

Whom do we notify of a breach and when?

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

mBank's Data Protection Officer

We have appointed Agata Rowińska as our Data Protection Officer.

Contact details of the Data Protection Officer:

- email: inspektordanychosobowych@mbank.pl
- mailing address:

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

How to lodge a complaint concerning personal data protection?

If a client believes that his or her 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 at https://www.uodo.gov.pl. Poland's data protection supervisor is the President of the Personal Data Protection Office (UODO).

Useful documents and information

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