Data Protection Briefly and Clearly
Guide to Understanding the Rules of Data Protection and the GDPR

What does GDPR mean?

GDPR is the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council, which is applicable in the Member States of the European Union, consequently in Hungary as well, starting from 25 May 2018. The GDPR protects the personal data of natural persons, and also provides for the free flow of information between the Member States.

When should and when should not be the GDPR applied?

The **GDPR must be applied by all entities** that have a place of business in the European Union, and handle or process personal data, regardless whether the processing itself takes place in the territory of the EU or not.

The **GDPR need not be applied** if the processing of personal data takes place in the scope of some personal or home activity (e.g. storage of addresses or photos), or if the data does not concern natural persons, but legal entities.

What is personal data?

Personal data is *"any information relating to an identified or identifiable natural person",* i.e. personal data can be practically anything that can be linked to a natural person. For example: name, e-mail address, IP address, security camera footage, transaction details. Identification can be direct as well as indirect (and may as well be based on a combination of several data, or implemented in several steps). Data shall remain personal data as long as their link to the natural person can be restored. **For example,** if the Bank is able to identify the customer on the basis of the account number, the account number shall qualify as personal data as long as the link between the customer and the account number exists.

What are special categories of personal data?

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As a general rule, it is forbidden to process special categories of personal data; however, the GDPR provides for numerous exemptions, for example special categories of personal data may be processed subject to the express consent of the data subject, in the employment context, or in the field of social protection or health care, at the special terms and conditions specified in the GDPR. The Bank processes special categories of personal data concerning the data subject only and exclusively in predefined cases, and subject to specific conditions.

What does data processing mean?

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as data collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Distinction between controller and processor

Aspects of the distinction between controller and processor:

Controller	Processor
Determines—independently or jointly with others—the purpose and means of the processing of personal data.	**Processes** personal data **on behalf of the controller** as a quasi executor.
Makes decisions, and **determines** the purpose and means of the processing of the data.	Processes the data for the controller's **benefit**, in the way determined by the controller.

Who is the data subject?

The data subject is the natural person to whom the personal data relate, i.e. any **identified** or **identifiable** natural person. The Bank in particular processes the personal data of Customers, Contributors, One-time Data Subjects and Prospective Customers.

Basic principles

The Bank processes personal data at all times in accordance with the following basic principles set out in the GDPR:

- **Principle of lawfulness, fairness and transparency:**
  - processing takes place in accordance with legal requirements, and serves some legitimate purpose;
  - the data subject is informed properly and all-inclusively about the processing;
  - clear and understandable information is provided regarding who, for what purpose and on what legal basis the personal data are processed by, and where and for how long they are stored.
- **Principle of purpose limitation:**
  - the data are processed for some specified, clear and legitimate (lawful) purpose, i.e. only such data can be processed as are indispensable for the implementation of the purpose of the processing.
- **Principle of storage limitation:**
  - the duration of the storage of the data must be determined in advance, and after the lapse of this period the data must be actually erased or destroyed, which means that personal data must be stored in a form that makes the identification of the data subject possible only for as long as this is necessary for the achievement of the purpose of the processing of the personal data, except if the data are processed for the purpose of:
    - archiving in the public interest;
    - scientific and historical research;
    - statistics,

    also having regard to the implementation of adequate technical and organisational measures serving the protection of the rights and freedoms of the data subjects.
- **Principle of integrity and confidentiality:**
  - appropriate security of the personal data must be ensured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (e.g. firewall, antivirus software).

- **Principle of data minimisation:**
  - only as many personal data can be processed as are absolutely necessary to achieve the purpose of the processing.
- **Principle of accuracy:**
  - personal data must be accurate and, where necessary, kept up to date (personal data that are inaccurate must be erased or rectified without delay).
- **Principle of accountability:**
  - the controller or the processor shall be liable for compliance with the above principles, and must be able to provide documentary evidence to certify this, which means that all instances of data processing must be documented, and upon request the documents should be released to the data protection authority or the data subject.

What are the legal bases of processing, on what legal basis can personal data be processed?

Some proper legal basis is needed to meet the principle of lawfulness of data processing. For lawful processing at least one of the following criteria must be met:

- the data subject has given his/her **consent** to the processing of his/her personal data;
  - such consent must be given freely and on an informed basis;
- processing is necessary for the **performance of a contract** to which the data subject is a party;
  - or it is necessary in order to take steps at the data subject's request prior to entering into the contract;
- processing is necessary for the performance of some **legal obligation**;
  - the obligation to process the data is prescribed for the controller by the law;
- processing is necessary to protect the data subject's **vital interests**;
  - processing takes place in order to protect the data subject's life or the interests of some other natural person;
- processing is necessary for the performance of the some **public interest task**;
  - if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the enforcement of the controller's or a third party's **legitimate interest**;
  - unless the data subject's interests, fundamental rights and freedoms override the controller's interests. A balance of interests test[1] must be conducted to decide this.

What is a personal data breach?

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What should be done in the case of a personal data breach?

In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. A register must be kept on personal data breaches.

[1] The balance of interests test is a three-step process where the controller's legitimate interest is identified, as well as the data subject's interest and the principle concerned as the counterpoint of weighting, then after the weighting is done it is decided whether the right of the data subject overrides the controller's legitimate interest or not, i.e. whether or not the personal data can be processed.

Does the data subject have rights, and if yes, what are these?

Yes; everything that appears as an obligation on the side of the controllers and processors will ensure rights in the data subjects' side:

- **Right to transparent information**
  - the data subject should get information on the fact and purpose of the processing, and other factors;
- **Right of access**
  - the data subject, if the processing of his/her data is in progress, should have access to information concerning the processing of his/her data;
- **Right to rectification**
  - upon the data subject's request, the controller should rectify or clarify any imprecise personal data relating to the data subject;
- **Right to erasure, right to be forgotten**
  - upon the data subject's request (under certain conditions) the controller should without undue delay erase the personal data concerning the data subject;
- **Right to restriction of processing**
  - under certain conditions the data subject has the right to obtain from the controller restriction of processing;
- **Right to object**
  - under certain conditions, on grounds relating to his or her particular situation, the data subject may object to the processing of his or her personal data;
- **Right to data portability**
  - the data subject has the right under certain conditions to get his/her personal data that he/she has made available to the controller, and to transmit these to another controller;
- **Automated processing**
  - under certain conditions the data subject has the right not to be subject to solely automated processing—i.e. one free from human interference—which produces legal effects concerning the data subject or would significantly affect him/her.

What can the data subject do if he/she objects to the processing of his/her personal data?

The data subject may file a complaint or pursue remedies:

- At the controller's Data Protection Officer;
- At the supervisory authority, i.e. the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) (registered office: 1055 Budapest, Falk Miksa utca 9-11., mailing address: 1363 Budapest, Pf. 9, telephone: +36-1-391-1400, fax: +36-1-391-1410, e-mail: ugyfelszolgalat@naih.hu);
- Before a court of the Member State where the supervisory authority is located if the supervisory authority does not handle a complaint or does not inform the data subject within 3 months on the progress or outcome of the complaint lodged;
- Directly before a court (http://birosag.hu/ugyfelkapcsolati-portal/illetekessegkereso).

You can find further more detailed information about data processing in the Bank's website under the heading "Data Processing".