**PRIVACY NOTICE**
**regarding data processing related to the purchase of e-vignette through OTP MobilBank**

SimplePay Plc. (Company reg. no. 01-10-143303; seat: 1138 Budapest, Váci út 135-139. B. ép. 5. em.; hereinafter referred to as Reseller) hereby informs the Users about the data processing related to the sale of e-vignette purchased through OTP MobilBank service as follows, in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council on the General Data Protection Regulation (hereinafter referred to as GDPR).

The terms herein and the phrases beginning with capital letters are to be understood as those in the General Terms and Conditions on the purchase of e-vignette (hereinafter: GTC)

The Reseller is entitled to modify the present Privacy Notice in any time. The present Privacy Notice enters into effect upon publishing.

**1. What personal data do we process, for how long, for what purposes and based on what legal basis?**

The legal bases for our data processing are the following:

a) GDPR Article 6 (1) a) where the processing is based on the informed consent of the data subject (hereafter referred to as **Consent**)
b) GDPR Article 6 (1) b) where processing is necessary for the performance of a contract to which the data subject is party (hereafter referred to as **Fulfilment of Contract**)
c) GDPR Article 6 (1) c) where data processing is necessary for the fulfilment of or compliance with a legal obligation of the data controller (e.g. obligations with tax statues – hereafter referred to as **Legal obligation**)
d) GDPR Article 6 (1) f) where data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, (hereinafter referred to as: **Legitimate Interest**)
e) the data processing authorization afforded by Article 13/A of Act CVIII of 2001 on Electronic Commerce and on Information Society Services, where data controllers are authorized to process the natural identification data and home address of the recipients without the need for consent, as required for contracts for information society services, for defining their contents, for subsequent amendments and for monitoring performance of these contracts, for invoicing the relevant fees, and for enforcing the claims arising out of or in connection with such contracts., moreover, where data controllers are authorized to process natural identification data and home address for the purposes of invoicing for the fees payable under the contracts for the provision of information society services to the extent related to the use of information society services, and information relating to the date, the duration and the place of using the service. (hereafter referred to as **E-Commerce Act**)

The legal basis for the data processing is specified below, per data categories and by reference to the elements of the above list.

**1.1. Data processed regarding e-vignette purchase**

| A | B | C | D | E | F |
|---|---|---|---|---|---|
| **Data subject** | **Data category** | **Data origin** | **Purpose of data processing** | **Legal basis of processing** | **Duration of data processing** |
| User registered with OTP MobilBank, buying e-vignette | vehicle license plate* | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b): GDPR Article 6 (1) c) Fulfilment of legal billing and tax obligation<br><br>In case of processing purposes of column D/b): GDPR Article 6 (1) c) Fulfilment of legal obligation - Invoicing<br><br>In case of processing purposes of column D/c): GDPR Article 6 (1) f) - Legitimate interest | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |

| | | | | | |
|---|---|---|---|---|---|
| | vehicle's country denomination* | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b): GDPR Article 6 (1) c) Fulfilment of legal billing and tax obligation<br><br>In case of processing purposes of column D/c): GDPR Article 6 (1) f) - Legitimate interest | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |
| | type of vehicle* | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid. |

| | | | | | |
|---|---|---|---|---|---|
| | | | c) Enforcement of claims and rights | In case of processing purposes of column D/b):<br>GDPR Article 6 (1) c) Fulfilment of legal billing and tax obligation<br><br>In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |
| | data of the purchased e-vignette (type, period of validity) * | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b):<br>GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b):<br>GDPR Article 6 (1) c) Fulfilment of legal billing and tax obligation | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general |

| | | | | | |
|---|---|---|---|---|---|
| | | | | In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after termination of the registration (general term of statute of limitation). |
| | name | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights<br>d) User identification<br>e) Ensuring communication | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b): GDPR Article 6 (1) c) Fulfilment of legal obligation – in case of data necessary for the fulfilment of taxation obligations Act CL of 2017 on the Rules of Taxation Sections 78 (3) and 202 (1) shall apply. If the data are necessary for the fulfilment of the accounting obligations, Act C of 2000 on Accounting sections 168-169 shall apply.<br><br>In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | In any other case the data shall be stored for 5 years after termination of the registration (general term of statute of limitation). |
| | transaction ID | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |
| | billing information: name and address | OTP Bank Plc. | a) Concluding the contract, determination of its content, | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have |

| | | | | | |
|---|---|---|---|---|---|
| | | | modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights | In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b):<br>GDPR Article 6 (1) c) Fulfilment of legal billing and tax obligation<br><br>In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |
| | e-mail address | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights, fraud prevention and management,<br>d) User identification, | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b): GDPR Article 6 (1) c) Fulfilment of legal obligation – in case of data necessary for the fulfilment of taxation obligations | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years. |

| | | | | | |
|---|---|---|---|---|---|
| | | | e) Ensuring communication | Act CL of 2017 on the Rules of Taxation Sections 78 (3) and 202 (1) shall apply. If the data are necessary for the fulfilment of the accounting obligations, Act C of 2000 on Accounting sections 168-169 shall apply.<br><br>In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |
| | amount paid for the purchase of e-vignette | OTP Bank Plc. | a) Concluding the contract, determination of its content, modification, completion thereof<br>b) Invoicing of contractual fees<br>c) Enforcement of claims and rights | In case of processing purposes of column D/a) and b): Article 13/A E-commerce Act<br><br>In case of processing purposes of column D/a) and b): GDPR Article 6 (1) b) Conclusion of Contract<br><br>In case of processing purposes of column D/b):<br>GDPR Article 6 (1) c) Fulfilment of legal billing and tax obligation<br><br>In case of processing purposes of column D/c):<br>GDPR Article 6 (1) f) - Legitimate interest | If the data are necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid.<br><br>If the data are necessary for the fulfilment of the accounting obligations, the retention period is 8 years.<br><br>Data processed for the purpose of enforcement of claims and rights, fraud prevention and fraud management purposes will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings.<br><br>In any other case the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation). |

Data marked with * are mandatory to fill in, without these data the e-vignette purchase function is not possible.

The Reseller is the data controller.

**Presentation of legitimate interest**: in case of data processing for the purpose of enforcement of claims and rights, the Reseller processes and uses the Users' aforementioned personal data in legal disputes arising from the contract concluded between the User and the Reseller for the Service, in litigation, out-of-court proceedings, other court or authority proceedings as evidence. The Reseller processes those data that in case of any legal dispute between the User and the Reseller in connection with the contract, the Reseller can use them for the purpose of evidence. The Reseller is entitled to exercise its right within the general term of statute of limitation. The data processing therefore is necessary for the protection of the Reseller's rights and legal interests. The purpose of data processing cannot be fulfilled in any other way.

The User is entitled to object to the data processing based on the aforementioned legitimate interest in an e-mail sent to the Reseller's customer service: ugyfelszolgalat@simple.hu

### 1.2. Data processing relating to customer service

#### 1.2.1. Data processing relating to the Reseller's costumer service

| A | B | C | D | E | F |
|---|---|---|---|---|---|
| **Subject** | **Data Category** | **Data origin** | **Purpose of data processing** | **Legal basis of data processing** | **Duration of data processing** |
| User registered within OTP MobilBank service and turning to the | name* | OTP Bank Plc. | a) User identification<br>b) Communication with the User in course of complaint management<br>c) Complaint management | GDPR Article 6 (1) f) Legitimate Interest | Within the general civil law limitation period following the complaint, that is 5 years from the submission of the complaint.<br><br>Data processed for the purpose of enforcement of claims and rights will be |

| | | | | | |
|---|---|---|---|---|---|
| customer service | | | d) Enforcement of claims and rights | | retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings. |
| | e-mail address* | OTP Bank Plc. | a) User identification<br>b) Communication with the User in course of complaint management<br>c) Complaint management<br>d) Enforcement of claims and rights | GDPR Article 6 (1) f) Legitimate Interest | Within the general civil law limitation period following the complaint, that is 5 years from the submission of the complaint.<br><br>Data processed for the purpose of enforcement of claims and rights will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings. |
| | recorded phone call | OTP Bank Plc. | a) User identification<br>b) Protection of consumers' rights<br>c) Proof of the content of the complaint<br>d) Enforcement of claims and rights | GDPR Article 6 (1) f) Legitimate Interest | For 5 years from the date of the complaint. |
| | subject of complaint | OTP Bank Plc. | a) Complaint management<br>b) Enforcement of claims and rights | GDPR Article 6 (1) f) Legitimate Interest | Within the general civil law limitation period following the complaint, that is 5 years from the submission of the complaint.<br><br>Data processed for the purpose of enforcement of claims and rights will be retained for a general limitation period of 5 years from the date of the successful |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings. |
| | details of transaction in question | OTP Bank Plc. | a) Complaint management<br>b) Enforcement of claims and rights | GDPR Article 6 (1) f) Legitimate Interest | Within the general civil law limitation period following the complaint, that is 5 years from the submission of the complaint.<br><br>Data processed for the purpose of enforcement of claims and rights will be retained for a general limitation period of 5 years from the date of the successful transaction, provided that if civil, criminal, administrative or other official proceedings are initiated during this period, the data will be retained until the final conclusion of such proceedings. |

Data marked with * are mandatory to fill in.

The Reseller is the data controller.

**Indication of legitimate interest** in accordance with GDPR Article 6 (1) f): the data processing within the scope of making a complaint, examination, settlement and management of the complaint, including the recording of phone calls, is the interest of the Reseller, since the processing of these data is necessary for the enforcement of our consumer and civil rights and interests in connection with the purchase made and service used within OTP MobilBank.

The User is entitled to object against the data processing based on the aforementioned legitimate interest in an e-mail sent to the Reseller's customer service: ugyfelszolgalat@simple.hu.

Upon his/her request, the User is entitled to receive the legitimate interest balancing tests concerning the aforementioned data processing based on legitimate interest; he/she may submit his/her request in an e-mail to be sent to Reseller's customer service.

**2. Who processes your personal data, and who has access to them?**

**The data controller**

The data controller of the personal data specified in clauses 1. is the Reseller, meaning SimplePay Plc., the company data of which are as follows:

**SimplePay Private Company Limited by Shares.**
Company reg. no.: 01-10-143303
Tax no.: 32835155-2-44
Seat: 1138 Budapest, Váci út 135-139. B. ép. 5. em.
Postal address: 1138 Budapest, Váci út 135-139. B. ép. 5. em.
Represented by: Péter Bese CEO, individually
E-mail address: ugyfelszolgalat@simple.hu
Telephone: 06 1 3666 611
06 70 3666 611
06 30 3666 611
06 20 3666 611

On behalf of the Reseller, the data is accessible to the employees of the Reseller whose access is essential to the performance of their duties. Access authorizations are specified in a strict internal policy.

**Data processors**

For the processing and storage of the personal data we engage the following companies, with whom we have entered into data processor agreements and to whom we forward your data necessary for the fulfilment of the aforementioned purposes. The following data processors conduct the processing of personal data:

| **Data processors' name and address** | **Purpose of data processing** |
|---|---|
| **Microsoft Corporation** (USA - One Microsoft Way Redmond, Washington 98052) | a) provider of Microsoft 365 cloud service |
| **N-Ware Kft.** (Billzone.eu, 1139 Budapest, Gömb utca 26., Company reg. no.: 01 09 921789, VAT number: 14825679-2-41) | a) electronic billing and sending service |

**3. Who is the data protection officer of OTP MobilBank and what are his contact details?**

**Zsombor Sári**
Contact:
a) The Reseller's offices (1138 Budapest, Váci út 135-139. B. ép. 5. em.)
b) e-mail address: dpo@simplepay.com
c) Postal address: 1138 Budapest, Váci út 135-139. B. ép. 5. em.

**4. To whom do we transfer your personal data?**

Your personal data are transferred to the following individual data controller recipients based on our agreement concluded with them (beside of the aforementioned data processors):

| **Recipient of data transfer** | **Category of transferred data** |
|---|---|
| **Nemzeti Mobilfizetési Zártkörűen Működő Részvénytársaság** (1027 Budapest, Kapás utca 6-12. Company reg. no.: 01 10 047569; VAT number: 24151667-2- 4) | In case of purchase of e-vignette, the following data are transferred: vehicle's license plate, vehicle's country denomination, type of the vehicle, data of the purchased e-vignette (type, period of validity). |
| **OTP Bank Plc**. (seat: 1051 Budapest, Nádor u. 16.; Company reg. no.: 01-10-041585; VAT number: 10537914-4-44) | Vehicle's license plate, vehicle's country denomination, type of the vehicle, data of the purchased e-vignette (type, period of validity), name, transaction ID, billing information: name and address, e-mail address, amount paid for the purchase of e-vignette, in case of a phone call with the customer service the recorded phone call, subject of complaint, details of transaction in question. |

The aforementioned entities are independent data controllers of the data transferred to them.

**5. What rights do you have regarding the processing of your data, and how can you exercise them?**

The detailed rights and remedies of the individuals are set forth in the applicable provisions of the GDPR (especially in articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79, 80, and 82 of the GDPR). The summary set out below describes the most important provisions and the Controller provides information for the individuals in accordance with the above articles about their rights and remedies related to the processing of personal data.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the individual, information may also be provided orally, provided that the identity of the individual is proven by other means.

The Controller will respond without unreasonable delay and by no means later than within one month of receipt to the request of an individual whereby such person exercises his/her rights about the measures taken upon such request (see articles 15-22 of the GDPR). This period may be, if needed, extended by further two months in the light of the complexity of the request and the number of requests to be processed. The Controller notifies the individual about the extension also indicating its grounds within one months of the receipt of the request. Where the request has been submitted by electronic means, the response should likewise be sent electronically unless the individual otherwise requests.

In case the Controller does not take any measure upon the request, it shall so notify the individual without delay but by no means later than in one month stating why no measures are taken and about the opportunity of the individual to lodge a complaint with the data protection authority and to file an action with the courts for remedy.

**5.1. The individual's right of access**

(1) The individual has the right to obtain confirmation from the Controller whether or not personal data concerning him/her are being processed. Where the case is such, then he/she is entitled to have access to the personal data concerned and to the following information:
   a) the purposes of the processing;
   b) the categories of personal data concerned;
   c) the recipients or categories of recipient to whom the personal data have been or will be disclosed including especially recipients in third countries and/or international organisations;
   d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   e) the right of the individual to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the individual, or to object to such processing;
   f) the right to lodge a complaint with a supervisory authority;
   g) where the personal data are not collected from the individual, any available information as to their source;
   h) whether automated decision making (Section (1) and (4) of article 22 of the GDPR) is applied including profiling, and in such case, at least information in comprehensible form about the applied logic and the significance of such data processing and the expectable consequences it may lead to for the individual.

(2) Where personal data are forwarded to a third country, the individual is entitled to obtain information concerning the adequate guarantees of the data transfer.

(3) The Controller provides a copy of the personal data undergoing processing to the individual. The Controller may charge a reasonable fee based on administrative costs for requested further copies. Where the individual submitted his/her request in electronic form, the response will be provided to him/her by widely used electronic means unless otherwise requested by the individual.

**5.2. Right to rectification**

The individual has the right to request that the Controller rectify inaccurate personal data which concern him/her without undue delay. In addition, the individual is also entitled to have incomplete personal data completed e.g. by a supplementary statement or otherwise.

**5.3. Right to erasure ("right to be forgotten")**

(1) The individual has the right that when he/she so requests, the Controller erase the personal data concerning him/her without delay where one of the following grounds applies:
   a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed by the Controller;

b) the individual withdraws consent on which the processing is based, and no other legal ground subsists for the processing;
c) the individual objects to the processing and there are no overriding legitimate grounds for the processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject;
f) the collection of the personal data occurred in connection with offering services regarding the information society.

(2) In case the Controller has made the personal data public and then it becomes obliged to delete it as aforesaid, then it will, taking into account the available technology and the costs of implementation, take reasonable steps including technical steps in order to inform processors who carry out processing that the individual has initiated that the links leading to the personal data concerned or the copies or reproductions of these be deleted.

(3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary, among other things, for:
a) exercising the right of freedom of expression and information;
b) compliance with a legal obligation which requires processing by Union or Member State law to which the Controller is subject;
c) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
d) the establishment, exercise or defence of legal claims.

**5.4. Right to restriction of processing**

(1) The individual has the right to obtain a restriction of processing from the Controller where one of the following applies:
a) the accuracy of the data is contested by the individual, for a period enabling the Controller to verify the accuracy of the personal data;
b) the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead;
c) the Controller no longer needs the personal data for the purposes of the processing, but the individual requires them for the establishment, exercise or defence of legal claims;
d) the individual has objected to processing based on the legitimate interest of the Controller pending the verification whether the legitimate grounds of the Controller override those of the individual.

(2) Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with the consent of the individual or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(3) The Controller informs the individual whose request has served as grounds for the restriction based on the aforesaid, before the restriction of processing is lifted.

**5.5. Notification obligation regarding rectification or erasure of personal data or restriction of processing**

The Controller will communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller informs the individual about those recipients if he/she so requests.

**5.6. Right to data portability**

(1) The individual has the right to receive the personal data concerning him/her, which he/she has provided to the Controller in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Controller, where:

a) the processing is based on consent or on a contract; and
b) the processing is carried out by automated means.

(2) In exercising the right to data portability pursuant to paragraph 1, the individual shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

(3) Exercising the aforesaid right shall not contravene to provisions concerning the right to erasure ('right to be forgotten') and, further, this right shall not harm the rights and freedoms of others.

**5.7. Right to object**

(1) The individual has the right to object, on grounds relating to his/her particular situation, at any time to processing of personal data concerning him/her for the purposes of legitimate interests. The Controller will no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims.

(2) Where personal data are processed for scientific or historical research purposes or statistical purposes, the individual, on grounds relating to his/her particular situation, has the right to object to processing of personal data concerning him/her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

**5.8. Right to lodge a complaint with a supervisory authority**

The individual has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his/her habitual residence, place of work or place of the alleged infringement if he/she considers that the processing of personal data relating to him/her infringes the GDPR. In Hungary, the competent supervisory authority is the National Data protection and Freedom of Information Authority (website: http://naih.hu; address: 1055 Budapest, Falk Miksa u. 9-11; Mailing address: 1363 Budapest, PO box 9; Phone: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu)

**5.9. Right to an effective judicial remedy against a supervisory authority**

(1) The individual has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him/her.

(2) The individual has the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform him/her within three months on the progress or outcome of the complaint lodged.

(3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

**5.10. Right to an effective judicial remedy against the Controller or the processor**

(1) The individual, without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, has the right to an effective judicial remedy where he/she considers that his/her rights under the GDPR have been infringed as a result of the processing of his/her personal data in non-compliance with the GDPR.

(2) Proceedings against the Controller or a processor shall be brought before the courts of the Member State where the Controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the individual has habitual residence. These kinds of proceedings are in the competence of the regional courts in Hungary. The individual may initiate the lawsuit before the reginal court competent according to their place of residence or place of stay, at their discretion. You can find more information about the availabilities of the courts here: www.birosag.hu.

**6. How do we ensure the safety of your data?**

We follow an extensive information security ruleset regarding the provision of safety concerning the data and information under our governance, the knowing and following of which is mandatory for all our staff.

Our staff is regularly trained and coached in matters of data and information security.

**6.1. Data security in IT infrastructure**

We store personal data on our central server, to which only a select and close employee group have access, per strict access control rules. We regularly test and check our IT systems in order to ensure and maintain data and information security.

We fulfil data security obligations by complying with the PCI DSS certificate, which entails enacting the strictest banking security regulations regarding our systems and our data governance.

Office workstations are password protected, third-party storage devices are restricted and may only be used following approval.

Protection against malicious software is provided regarding all of the systems and system elements of the Company.

During the planning, development, testing and operation of programs, applications and tools, we address security functions separately and with emphasis.

When allocating authorisations to our IT systems, we pay close attention to the protection of data (e.g. passwords, authorisations) affecting these systems.

**6.2. Data security in communications**

Regarding electronically forwarded messages and data; we conduct ourselves regarding our Key Management bylaws. In order to comply with the principle of safe transfer of data, we ensure the integrity of both the data of the controller and the user. For the prevention of data loss and damage, we use error detecting and correcting procedures. The application's passes, authorization data, safety parameters and other data may only be forwarded under encryption We use network endpoint-to-endpoint authorization checking in order to ensure accountability and auditability.

Our implemented security measures detect unauthorized modifications, embedding and repetitive broadcasting. We prevent data loss and damage by fault detecting and correcting procedures and we ensure the prevention of deniability.

Regarding the network used for data transmission, we provide defence against illegal connection and eavesdropping per an adequate security level.

**6. 3. Data security in software developing and programming**

We implement the measures of data safety and security even into the planning stage, which we uphold during the entire course of development.

We separate the development environment from the live one, as well as development data from live data, and we depersonalise personal data in development, where possible.

We keep the requirements of safe coding in development, we use platform- and programming language-dependant technologies to avoid frequent damage risks, moreover, we follow the latest industry best practices regarding code examination (e.g. OWASP Top 10 Guide, SANS CWE Top 25, CERT Secure Coding).

We constantly follow procedures to identify newfound vulnerabilities, we regularly coach our developers regarding data security, and we standardise our programming techniques to avoid typical errors.

The checking of completed code is conducted pursuant to the principles of safe coding and documented with alteration tracking procedures in order to ensure proper documentation.

**6.4. Data security in document management**

We comply with data security requirements in document management as well, which we stipulate in document management by-laws. We manage documents by pre-set access and authorization levels, based on the level of confidentiality regarding the documents. We follow strict and detailed rules regarding the destruction of documents, their storage and handling at all times.

**6.5. Physical data security**

In order to provide physical data security, we ensure our physical barriers are properly closed and locked, and we keep strict access control regarding our visitors at all times. The office premises are secured and protected 24/7.

Our paper documents containing persona data are stored in a closed locker that is fire- and theft-proof, to which only a select few have authorised access.

The rooms where storage devices are placed in have been made to provide adequate protection against unauthorised access and breaking and entering, as well as fire and environmental damage. Data transit, as well as the storage of backups and archives is done in these confined locations.

Backup data storage units are stored in a reliably locked area, with containers having a minimum of 30 minutes' fireproofing time.

**7. What procedure do we follow upon a data breach?**

Pursuant to applicable law, we report incidents to the supervisory authority within 72 hours of having gained knowledge thereof, and we also keep records of them. In cases regulated by applicable law, we also inform subjects of the incidents, where necessary.

**8. When and how do we amend this notice?**

If the scope of the processed data or other circumstances of data processing change, we will modify this privacy notice in accordance with GDPR requirements and publish it in the OTP MobilBank service. Please make sure to carefully read any changes to the privacy notice, as it contains important information about the processing of your personal data.