PRIVACY NOTICE

Effective: from 8 September 2023

The developer and provider of the SimplePay service, **OTP Mobile Ltd**. (company reg. no. 01-09-174466; seat: 1138 Budapest, Váci út 135-139. B. ép. 5. em.; hereafter referred to as: Simple) informs the Customers of the data management regarding the engagement of the SimplePay service as follows, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation (hereafter referred to as GDPR).

The terms herein and the phrases beginning with capital letters are to be understood as those in the GTC.

1. What personal data do we manage, for how long, for what purposes and by what authorization?

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), on 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 fulfillment 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, (a hereafter 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)

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 processing concerning bank card data

When using the bank card payment function of the SimplePay Service, the User enters their bank Card data, such as the name on the Card, the card number, the expiry data, the issuing bank name, and the CVC/CVV security code on the applicable online interface. These Card data are processed by Simple as data processor of the Merchant to which Card data, OTP Bank Plc. and Borgun hf, who provides the bank card acceptance background to the SimplePay Service, ha access as independent data controllers

Merchant cannot access bank card data.

If the Customer saved or saves the Card data during the payment process for the purpose of later payments, in case of those Merchants which originally concluded a contract with the OTP Bank Plc. for the acceptance of VPOS and which later had been taken over by Simple into the SimplePay system on the basis of the joint agreement between the bank, the Merchant and the Simple, those Card data are also stored directly in the bank's system in the VPOS (Virtual Point Of Sale) belonging to the given Merchant. The bank is the data controller of those saved Card data. Simple is also processing those data as the data processor of the Merchant.

Simple may have access to those Card data saved and stored in the aforementioned bank's system during the payment with that saved Card in the process of reading of the Card data on the basis of the contract the Simple concluded with the bank storing the Card data, on behalf and in the name of the bank, as a data processor. Simple reads those Card data saved and stored in the VPOS belonging to the given Merchant in the bank's system from the VPOS originally created for the given Merchant during the Customer's payment transaction in the SimplePay Services.

1.2. Data processed by Simple as data processor for the request of the Merchant and Borgun hf.

Simple manages the user transactional data given to them by Merchant, provided by the User on the payment interface of the Merchant's webshop per the mandate from Merchant, pursuant to the provisions of the data processing agreement between Merchant and Simple. The data sub-processor of Simple is OTP Bank Plc. in this regard, who perform the authorization of the transactions, and who perform monitoring services by a mandate from Simple, for the purposes of detecting and preventing fraud.

If Simple uses Borgun hf. for card acceptance, Simple transfers the Customers' transactional data on behalf of and for the request of the Merchant to the financial institution with whom Simple entered into a card acceptance agreement and providing the authorisation, namely to Borgun hf. Borgun hf. processes the Customers' transactional data as an independent data controller based on its own data protection notice and policies. Simple qualifies as data processor of Borgun hf. in this data transfer, Simple acts on behalf of and for the request of Borgun hf. based on its data processing agreement concluded with Borgun hf.

Simple manages the following data, listed per data processors:

Nature and purpose of data processing activity	Data subject category	Data category
Conclusion, monitoring and accounting of payment transactions within the SimplePay service	The Customer conducting payment via SimplePay, on the payment interface of the Merchant, Customer paying with SoftPOS Services	Name (it is not precessed in SoftPOS)
		telephone number (it is not precessed in SoftPOS)
		e-mail address (it is not precessed in SoftPOS)
		transacted amount
		IP address (it is not precessed in SoftPOS)
		Time, date and identifier of transaction
		shipping address (it is not precessed in SoftPOS)
		billing address (it is not precessed in SoftPOS)
		Data of the bank card saved during the payment in the Merchant's webstore

		through SimplePay services (token bankcard storing): bankcard number, expiration date, CVV code, name on the bank card
		In Simple Business application: name of the product purchased by the Customer
		In case of wire transfer: Customer's (bank account owner's) name and bank account number
Sending of messages, notifications and confirmations regarding payment transactions within the SimplePay service	The Customer conducting payment via SimplePay, on the payment interface of the Merchant	name
		e-mail address
Authorization of transactions within the SimplePay service	The Customer conducting payment via SimplePay, on the payment interface of the Merchant, Customer paying with SoftPOS Services	Name (it is not processed in SoftPOS)
		Telephone (it is not processed in SoftPOS)
		e-mail address (it is not processed in SoftPOS)
		transacted amount
		IP address (it is not processed in SoftPOS)
		Time, date and identifier of transaction
		shipping address (it is not processed in SoftPOS)
		billing address (it is not processed in SoftPOS)
		Data of the bank card saved during the payment in the Merchant's webstore through SimplePay services (token bankcard storing): bankcard number, expiration date, CVV code, name on the bank card
Monitoring of SimplePay transactions for the purposes of detecting and preventing fraud, and for assessment of Chargeback and Customer's claim	The Customer conducting payment via SimplePay, on the payment interface of the Merchant, Customer paying with SoftPOS Services	Name (it is not processed in SoftPOS)
		telephone number (it is not processed in SoftPOS)
		e-mail address (it is not processed in SoftPOS)
		transacted amount (including the name, price of the products, transfer fee and discount provided)
		IP address (it is not processed in SoftPOS)
		Time, date and identifier of transaction
		shipping address (it is not processed in SoftPOS)
		billing address (it is not processed in SoftPOS)
		Comments by the Customer related to the order
		Whether the Customer is a regular, repeat customer
		Data in the document proving the hand-over by the Customer of the product ordered by the Customer
		Data in the document proving the use by the Customer of the services ordered

		by the Customer
Providing strong customer authentication, 3D Secure services in the SimplePay services during online bankcard payment	Customers paying with SimplePay in Merchant's webshop	name
		telephone number
		e-mail address
		transaction sum
		IP address
		shipping address
		billing address
		Data collected from the browser used during the online purchase of the Customer: • value of Accept http header which is the format which appears in the body of the request • name and version number of the browser and operation system, default language • browser source IP address • whether browser can run java codes • browser language • browser colour depth • browser screen heights • browser screen width • time zone of the browser
		Way of purchasing at Merchant: • as a guest, without registration • as a registered user • as a user registered with with a third party identification (Facebook, Google, other account registration)
In SoftPOS Services sending certificate on the Transaction to the Customer	Customer paying in the SoftPOS Services	Customer's e-mail address Date, time and identifier of the Transaction Amount of the Transaction Result of the Transaction

Regarding the data above, Merchant qualifies as data controller, and Merchant's data processing notice holds what data is managed by Merchant, for what purpose, per what legal basis, and for how long. Simple processes this data pursuant to the instructions of the Merchant, and does not use these for their own purposes in any way.

Should User elect on the payment interface of the Merchant to conduct their payment via their bank card registered in the Simple App, Simple shall then be held as a data processor, managing and storing the email address and name of the User that is registered within the Simple App. The recording and storage of the bank card data is done pursuant to the data processing notice of the Simple Application.

1.3. Data processed by Simple regarding the User for purposes of customer service and complaints

Subject	Data category	Purpose of data management	Legal basis of data management	Timeframe of data management
User contacting customer services	name*	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Legitimate interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.
	e-mail address*	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Legitimate interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.
	telephone number*	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Legitimate interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.
	record of phonecall	User identification Quality control Consumer rights protection Evidence on complaint contents Exercising of rights and claims	GDPR Article 6 (1) f) on Legitimate interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.
	parameters of Customer transaction in question, not including bank card no. and security ID	Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Legitimate interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.

In case of data processing based on Legitimate interest, the data subject is entitled to object against the data processing; in this case the Service Provider does not process his/her data any more.

The data subjects are entitled to request to read the interest balancing tests concerning the data processing based on legitimate interest. The request may be submitted to the e-mail address of customer service below.

Simple and OTP Bank Nyrt. provide (1051 Budapest, Nádor u. 16) customer services as joint data controllers based on the joint data controller agreement concluded between them. According to Article 26 (2) of the GDPR we hereby inform you about the material provisions of the joint data controller agreement:

- Simple and OTP Bank Nyrt. independently keep the data protection records about its own data processing activities connected to its own liability, and independently keeps the data breach records, records of requests from supervisory authorities and data subjects, records of data processors, records of data transfers.
- OTP Bank Nyrt. ensures the storage of the consent statements for the time agreed by the joint data controllers and in a way which ensures searchability.
- In case of contacting the customer services via phone or in e-mail, OTP Bank Nyrt. informs the data subjects about the data processing and OTP Bank Nyrt. is liable for preparing the text of the consent statemeIt. OTP Bank Nyrt. collects, stores the consent statements and keeps records of them.
- Simple fulfils its obligation for information providing about the data processing via this privacy notice on its website.
- Simple and OTP Bank Nyrt. publish its privacy notices prepared separately related to the joint data processing on its own and informs the data subjects on its own.
- Simple and OTP Bank Nyrt. determine the purpose and tools of data processing jointly related to the joint data processing activity according to Article 26 (1) of the GDPR.
- The data subject is entitled to exercise his/her rights against both data controller and related to both data controller.
- Simple and OTP Bank Nyrt. answer the requests received by each of them independently according to the process jointly agreed.
- Simple and OTP Bank Nyrt. fulfil the requests of data subject on rectification, erasure, restriction of the personal data, objections against the data processing and requests on data portability independently.
- Simple and OTP Bank Nyrt. independently answer the questions of the supervisory authority related to their own activity.
- Those joint data controller announces the data breach to the authority whose activity is affected by the data breach.
- Those joint data controller informs the data subjects about the data breach, whose activity is affected by the data breach. If the data breach affected both data controller, the data controllers inform the data subjects independently and separately.
- Data protection officer of the OTP Bank Nyrt is: Zoárd Gázmár, e-mail: adatvedelem@otpbank.hu, address: 1131 Budapest, Babér u. 9.

Designation of lawful interest pursuant to GDPR Article 6 (1) f): data management relating to the issuing and examination of complaint, the handling and execution thereof, including the recording of phonecalls, which is a joint interest of the Customer and the Service Provider, since the processing if this data is necessary for the usage of the Website and the SimplePay service, moreover to the exercising of concumser protection, law and civil law interests and rights relating to the payment transaction. In management of this personal data, the rights of the Customer on the recorded phonecall do not preclude others, since their personal freedoms are not infringed upon, since at the beginning of the phonecall, they receive information on the imminent recording, affording Customer the choice to terminate the call or to proceed with it. The email alternative of customer services is also available with equal means, so there is a choice there for the Customer as well

Data marked with * are mandatory to input, since in abscence of those, customer services cannot examine the given complaint.

1.4. Customer data processed by Simple for the purposes of sending system notifications

Simple send notification to the Customer in e-mail, push notification maessages, in-app messages and in any other electronic way about the break down, error, troubleshooting, suspension or other circumstance regarding the operation of the SimplePay Service, about information connected to the payment through the SimplePay service (System notification). Simple may send the System notification in a separate message or if the Customer is registered in the Simple Application, within the Simple System. Simple processes the following Customer's data for this purpose:

Subject	Data category	Data source	Purpose of data management	Legal basis of data management	Timeframe of data management
Customer	name	from subject	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Lawful interest	General civil law expiration time which is 5 years
	e-mail address	from subject or Merchant	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Lawful interest	General civil law expiration time which is 5 years

In case of data processing based on Legitimate interest, the data subject is entitled to object against the data processing; in this case the Service Provider does not process his/her data any more.

The data subjects are entitled to request to read the interest balancing tests concerning the data processing based on legitimate interest. The request may be submitted to the e-mail address of customer service below.

Designation of legitimate interest: it is the business and legal interest of the Service Provider to inform the Customer about the the break down, error, troubleshooting, suspension or other circumstance regarding the operation of the SimplePay Service, about information connected to the payment through the SimplePay service. The purpose of data processing cannot be executed in other way.

1.5. Customer data processed by Simple for sending of newsletters

The Customer may freely subscribe to electronic direct marketing messages,adverts, marketing materials and newsletters on the SimplePay Website, separate from the acceptance of the SimplePay GTC, meaning that the User may expressly consent to such materials being sent to their email address provided regarding the engagement of the SimplePay service. In case of data processing based on consent, the data subject is entitled to withdraw his/her consent at any time in the way that the Customer may unsubscribe from said media freely, at any point by selecting the "unsubscribe" option within any newsletter. In such cases, upon receipt of the notification thereof, Simple immediately deletes the email address from their database and ensures that no further messages or other direct marketing media are sent to the Customer.

Subject	Data category	Data source	Purpose of data management	Legal basis of data management	Timeframe of data management
Customer	name*	from subject	sending of newsletters	GDPR Article 6 (1) a), Consent	Until revocation of consent
	e-mail address*	from subject	sending of newsletters	GDPR Article 6 (1) a), Consent	Until revocation of consent

Data marked with * are mandatory to input, since in abscence of those, subscription to newsletters is not possible.

1.6. Personal data processed in Instalment services

Simple processes the Customer's personal data listed below in connection with the Instalment Services as the data processor of the OTP Bank Plc. and based on the outsourcing and data processing agreement concluded with OTP Bank Plc.

Data controller: OTP Bank Plc (seat: H- 1051 Budapest, Nádor u. 16.)

Subject	Data category	Data source	Purpose of data processing, data processing activity
Customer	Amount of the own contribution	Data subject (Customer)	Displaying Instalment services on SimplePay platform, providing technical platform services, sending confirmation letter ont he successful Instalment construction.
	Amount to be paid in instalments		
	Number of instalments (months)		
	Amount of the monthly instalments		
	Amount of the interest and fees		

2. Data processing concerning the enforcement of the data subjects' data protection rights (see clause 8)

The Data controller processes data when the data subjects eyercise their data protection rights concerning the data controller's data processing activity. In this case the Data controller processes the following data:

Name and purpose of data processing	Legal basis of data processing	data categories	Duration of data processing
Data processing concerning the enforcement of the data subjects' data protection rights (see clause 8)	GDPR Article 6 (1) c) (the data processing is necessary for fulfilling the legal obligation of Data controller) Legal obligation: making possible the exercising of the data subjects' rights stipulated in a GDPR Articles 15-22 and documentation of the other steps concerning the request.	Personal data submitted to the Data controller in connection with the data protection requests: in case of private persons, legal entities and other organisations turning to the Data controller the contact details of the contact persons necessary for communication with them (in particular: name, address, phone number, e-mail address), content of the request, steps concerning the request, documents concerning the request. For example: if the data subject requests in e-mail to erase all of his/her data based on the GDPR, and the Data controller fulfils this request, the Data controller will keep the e-mail about the request for erasure.	Duration of data processing: in lack of other data protection authority guidance: indefinite period of time.

3. Data processing in order to archive the consents of the data subjects to the data processing and to archive the withdrawal of those consents

Name and purpose of data processing	Legal basis of data processing	data categories	Duration of data processing
Archive the consents of the data subjects to the data processing and the withdrawal of those consents	GDPR Article 6 (1) c) (the data processing is necessary for fulfilling the legal obligation of Data controller) Legal obligation: according to Article 7 (1) of GDPR if the data processing is based on consent, the data controller must be able to certify that the data subject has granted consent to the processing of his/her personal data.	If any data processing of the Data controller is based on consent, the Data controller archives the consent. The purpose of this procedure is to certify the legality of the consent in any time. If the data subject withdraws his/her consent, the Data controller keeps the withdrawal statement (and the communication related to that). The purpose of this procedure is that the Data controller must always be be aware of that a data subject withdrew his/her consent to a given data processing.	Duration of data processing: in lack of other data protection authority guidance: indefinite period of time.

4. Data processing for the purpose of recording data protection breaches (including documentation of steps taken related to the management of the incidents)

Name and purpose of data processing	Legal basis of data processing	data categories	Duration of data processing
Data processing for the purpose of recöoring data	GDPR Article 6 (1) c) (the data processing is necessary for fulfilling	Personal data of the data subjects related to the data protection incident.	Duration of data processing: in lack of

protection breaches (including documentation of steps taken related to the management of the incidents)	the legal obligation of Data controller) Legal obligation: according to Article 33 (5) of GDPR the Data controller keeps records on data protection incidents by indicating the facts related to the data protection incident, their effects and the measures taken for remedy of the incident. This record makes the data protection authority able to control the compliance with the GDPR.		other data protection authority guidance: indefinite period of time.

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

The data controller

The controller of the personal data specified under clauses 1-4 (except clause 1.3) hereto is Simple, meaning OTP Mobile Service Llc., the company data of which are as follows:

OTP Mobile Service Limited Liability Company.
Company reg. no.: 01-09-174466
Tax no.: 24386106-2-41
Seat: 1138 Budapest, Váci út 135-139. B. ép. 5. em.
Postal address: 1138 Budapest, Váci út 135-139. B. ép. 5. em.
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 Simple, the data is accessible to the employees of Simple whose access is essential to the performance of their duties. Access authorizations is specified in a strict internal code.

Data processors

For the processing of the personal data of representative and contact persons, we engage the following companies, with whom we have entered into data processor agreements. The following data processors conduct the processing of personal data:

Name and address of data processor	Purpose of data processing	Information regarding data transfers to abroad
OTP Bank Plc. (seat: 1051 Budapest, Nádor u. 16.; company reg. no.: 01-10-041585; tax no.: 10537914-4-44)	a) provision of online bank card payment service, bank card authorization, fraud monitoring b) provision of IT infrastructure for SimplePay	There is no data transfer to abroad.
Microsoft Corporation (USA - One Microsoft Way Redmond, Washington 98052)	a) Microsoft 365 cloud service provision	Data is transferred to the USA. Legal basis of transfer: Standard Contractual Clauses (SCC) based on the Data Protection Directive 95/46/EC as approved by the Article 29 Working Party based on the model contract 2010/87/EU, by virtue of which the data processor ensures that the personal data is processed and transferred in accordance with the EU data protection provisions. The SCC is available in the Microsoft Online Services Terms.
Mastercard Europe SA company reg. no.: RPR 0448038446, seat: 198/A, Chaussée de Tervuren, 1410 Waterloo, Belgium and Mastercard International Incorporated seat: 2000 Purchase Street, Purchase, New York 10577, United States of America	a) conclusion of online bank card payments	Data is transferred to the USA. Lgal basis of transfer: Binding Corporate Rules in accordance with Article 47 of the GDPR, which are, pursuant to Article 46 (2) b), an appropriate guarantee in respect of data transfers to abroad. The Mastercard BCR is available here: mastercard-bcrs.pdf
The Rocket Science Group LLC d/b/a MailChimp seat: Georgia 675 Ponce De Leon Ave NE, Suite 5000 Atlanta, Georgia 30308	a) sending of newsletters, storage of e-mail addresses in newsletter databases	Data is transferred to the USA. Legal basis of transfer: Standard Contractual Clauses (SCC) based on the Data Protection Directive 95/46/EC as approved by the Article 29 Working Party based on the model contract 2010/87/EU, by virtue of which the data processor ensures that the personal data is processed and transferred in accordance with the EU data protection provisions.

		The MailChimp SCC is available in Annex 3 of the MailChimp Data Protection Addendum: Mailchimp Data Processing Addendum
Visa Europe Services LLC, incorporated in Delaware, USA, acting via its London branch office (branch No: BR007632) registered office: 1 Sheldon Square, London W2 6TT, VAT Number: GB 840 111 776	a) conclusion of online bank card payments	Data is transferred to the USA. Legal basis of transfer: Standard Contractual Clauses (SCC) based on the Data Protection Directive 95/46/EC as approved by the Article 29 Working Party based on the model contract 2010/87/EU, by virtue of which the data processor ensures that the personal data is processed and transferred in accordance with the EU data protection provisions.
Slack Technologies Limited (Central Park (Block G), 3rd and 4th FL, No 1, Central Park, Leopardstown, Dublin 18, Ireland)	Task management and internal communication for the employees of the Data Controller.	Slack stores the data in the U.S., so there is a data transfer to third country which Slack does on the basis of Standard Contractual Clauses (Data Processing Addendum - Legal - Slack (axdraft.com) which serves as an appropriate guarantee according to article 45 (2) point c) and d) of the GDPR. The Data Controller and the Slack entered into a data processing agreement available on the above link.

Transfer of data to independent data controllers

Simple transfers the Customer's transactional data as the data processor of Borgun hf., on behalf of and for the request of Borgun hf. (Ármúli 30, 108 Reykjavik, Iceland) for the following purposes:

- ensuring online bank card payment services, bank card acceptance
- bank card authorisation
- fraud monitoring and prevention.

6. Who is the data protection officer of Simple and what are his contact details?

Zsombor Sári
Contact:
a) Simple offices (1138 Budapest, Váci út 135-139. B. ép. 5. em.)
b) e-mail address: dpo@otpmobil.com
c) Postal address: 1138 Budapest, Váci út 135-139. B. ép. 5. em.

7. To whom do we forward your personal data?

Your personal data is not transferred to anyone except the data processors, data controllers mentioned above and the Merchants.

8. 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 – which include Employees and the people listed in Section 1 – 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 Employer 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 Employer 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 Employer 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 Employer 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.

8.1 The individual's right of access

(1) The individual has the right to obtain confirmation from the Employer 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 Employer 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 Employer provides a copy of the personal data undergoing processing to the individual. The Employer 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.

8.2 Right to rectification

The individual has the right to request that the Employer 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.

8.3 Right to erasure ('right to be forgotten')

(1) The individual has the right that when he/she so requests, the Employer 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 Employer;
(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 Employer is subject;
(f) the collection of the personal data occurred in connection with offering services regarding the information society.

(2) In case the Employer 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 Employer 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.

8.4 Right to restriction of processing

(1) The individual has the right to obtain a restriction of processing from the Employer where one of the following applies:

a) the accuracy of the data is contested by the individual, for a period enabling the Employer 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 Employer 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 Employer pending the verification whether the legitimate grounds of the Employer 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 Employer informs the individual whose request has served as grounds for the restriction based on the aforesaid, before the restriction of processing is lifted.

8.5 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Employer 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 Employer informs the individual about those recipients if he/she so requests.

8.6 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 Employer in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Employer, 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.

8.7 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 Employer 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.

8.8 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 The National Data protection and Freedom of Information Authority (website: http://naih.hu; address: H-1055 Budapest, Falk Miksa u. 9-11.; mailing address: H-1363 Budapest, POB 9; Phone: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu)

8.9 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.

8.10 Right to an effective judicial remedy against the Employer 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 Employer or a processor shall be brought before the courts of the Member State where the Employer or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the individual has habitual residence. You can find more information about the availabilities of the courts here: www.birosag.hu.

9. 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.

9.1. 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 Service Provider.

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.

9.2. 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 defense against illegal connection and eavesdropping per an adequate security level.

9.3. Data security in software development and programming

In development of the Simple Application, 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. például 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.

9.4. 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.

9.5. 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.

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.

10. What procedure do we follow upon an incident?

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

11. When and how do we amend this notice?

Should the scope of data, or the circumstances of data management be subject to change, this notice shall be amended and published on www.simplepay.hu. Please pay attention to the amendments of this notice, as they contain important information regarding the management of your personal data.