1. **Annex to the SimplePay User GTC**

DATA MANAGEMENT NOTICE

The developer and provider of the SimplePay service, **OTP Mobile Ltd.** (company reg. no. 01-09-174466; seat: 1093 Budapest, Közraktár u. 30-32.; hereafter referred to as: **Simple**) informs the Customers of the data management regarding the engagement of the SimplePay service as follows, in accordance with 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 **Conclusion 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 **Compliance**)
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 továbbiakban: **Jogos érdek**)
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. Bank card data

When utilising 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. This bank card data is not processed by SimplePay, but rather by OTP Bank Plc., who provide the banking background to the SimplePay Service. Simple cannot access this data, does not store, nor forward them, the data gets recorded directly into the systems of OTP Bank Plc.

Merchant cannot access bank card data either.

1.2. Data processed by Simple per mandate from the Merchant

Simple manages the user 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, whereby Simple engages the services of data sub-processors. 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.

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	name
		telephone number
		e-mail address
		transacted amount
		IP address
		time and date of transaction
		shipping address
		billing address
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,	The Customer conducting	name

identification of Customers regarding payment transactions within the SimplePay service	payment via SimplePay, on the payment interface of the Merchant	telephone
		e-mail address
		transacted amount
		IP address
		time and date of transaction
		shipping address
		billing address
Monitoring of SimplePay transactions for the purposes of detecting and preventing fraud, and for exercising rights and claims	The Customer conducting payment via SimplePay, on the payment interface of the Merchant	name
		telephone number
		e-mail address
		transacted amount
		IP address
		time and date of transaction
		shipping address
		billing address

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 collected and stored automatically about the User when visiting the SimplePay website or using the SimplePay Service

When using the www.simplepay.hu website (**Website**), we utilise small programs called cookies and similar technologies on your device, to aid your identification, to recognize your data, so you don't have to enter them every time, and to improve user experience, to increase website security and efficacy. This data is not provided by the User, but is collected by us during your website visit:

Subject	Data category	Purpose of data management	Legal basis of data management	Duration of data management
User visiting the website	IP address	Understanding of interests, website customization	GDPR Article 6 (1) a), Consent	Duration of website visit
	Browser type	Understanding of interests, website customization	GDPR Article 6 (1) a), Consent	Duration of website visit
	Operating system	Understanding of interests, website customization	GDPR Article 6 (1) a), Consent	Duration of website visit
	Internet service provider	Website customization	GDPR Article 6 (1) a), Consent	Duration of website visit
	Timestamp	Ensuring of safety	GDPR Article 6 (1) a), Consent	Duration of website visit
	Website visit data	Understanding of interests, app customization	GDPR Article 6 (1) a), Consent	Duration of website visit

Simple logs the above data automatically upon the User's entering and leaving of the website, without any need for a dedicated action of the User. This data may not be linked with other personal data – notwithstanding cases where such is mandatory pursuant to applicable law. This data may only be accessed by Simple, as data processor.

Service Provider utilises cookies and similar technologies in order to aid identification of the User, the recognize them upon using of the Website's services, to enable Service Provider to understand the interests of Users regarding the Services and the Website, to improve user experience, and to increase Website safety and efficiency. User may control the usage of cookies within their browser settings, and by various other means.

Upon visiting the Webpage and ustilising the Services, Service Provider places cookies within User's browser and in HTML-based emails as per the regulations herein.

In general the cookie is a small file consisting of letters and numbers which is sent to the device of the User from the web server of the Service Provider. It enables for example the Service Provider to recognize the final appliance of the User when the connection is created between the web server of the Service Provider and the device. The main purpose of the cookie is to enable the Service Provider to make available individualized offers, publicity and advertisements for the User which may personalize the User's experience during the use of the Simple System and may reflect more to the personal needs of the User.

Purpose of cookies utilised by Service Provider:

a) Security: aiding and ensuring safety, moreover enabling and aiding Service Provider to detect unlawful conduct.
b) Preferences, attributes and services: cookies let Service Provider know, what language is preferred by the User, what are their communications preferences, aid the User in completing forms on the Website, making them easier to fill out.
c) Performance, analytics and research: cookies aid the Service Provider in understanding how the Website performs in various areas. Service Provider may use cookies, which rate, improve and search the Website, the products, functions, services, including when User enters the Website from other webpages, and the devices, such as User's computer or mobile device.

Types of cookies utilised by Service Provider:

a) analytics, tracking cookies;
b) session cookies, which only operate during the active session (usually the webpage visit itself);
c) permanent cookies: which help in identifying the Customer as an existing user, making it easier for them to return without having to log in again. After the Customer logs in, the permanent cookie remains in their browser, withe the webpage being able to read it.

Adobe Flash is another technology equal in function to cookies. Adobe Flash is able to store data on the User's device. Not every browser allows the removal of Adobe Flash cookies however. The Customer may restrict or block Adobe Flash cookies via the website of Adobe. If Customer restricts or blocks them, certain elements of the Website may become inaccessible.

Third party cookies:

Reputable partners aid Service Provider in analysing Webpage statistics, and analytics companies such as Google Analytics, Quantcast, Nielsen and ComScore may also place cookies on the Customer's device.

Users may disallow Google cookies on the page used for the disabling of Google ads.

On http://www.networkadvertising.org/choices/ there are further means to deny other, third party cookies from being used.

Control of cookies:

Most cookies enable Customers to control cookie usage via their settings. However, if Customer restricts the usage of cookies, this may hinder user experience, since it will no longer be customised. Customer may also stop the saving of personal settings, such as the saving of login information.

If Customer does not wish for Service Provider to use cookies when User visits the webpage, they may refuse usage under their settings page. In order to let Service Provider know that the Customer has refused usage of cookies, a denial cookie is placed on the Customer's device, thus, Service Provider will know that no cookies may be placed on the device upon the next visit of the webpage. If the Customer does not wish to receive cookies, they may change their browser settings accordingly. If no such change has been made, Service Provider will view Customer as having given consent to the sending of any kinds of cookies. The Website shall not function completely without cookies.

For further information of cookies, including types, management and removal, visit Wikipedia.org or www.allaboutcookies.org or www.aboutcookies.org.

1.4. Data managed by Simple regarding the User for purposes of customer service and complaints

Subject	Data category	Data source	Purpose of data management	Legal basis of data management	Timeframe of data management
User contacting customer services	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 from complaint filing, which is 5 years from the complaint being filed.
	e-mail address*	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 from complaint filing, which is 5 years from the complaint being filed.
	telephone number*	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 from complaint filing, which is 5 years from the complaint being filed.
	record of phonecall	from subject	User identification Quality control Consumer rights protection	GDPR Article 6 (1) f) on Lawful interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.

			Evidence on complaint contents Exercising of rights and claims		
	parameters of Customer transaction in question, not including bank card no. and security ID	from subject	Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Lawful interest	General civil law expiration time from complaint filing, which is 5 years from the complaint being filed.

Nomination 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.

1.5. Customer data managed by Simple for the purposes of sending system notifications

Simple may inform the Customer of the stoppage, error, troubleshooting, amendment, suspension or other circumstance regarding the SimplePay Service (**System notification**), and may process the Customer's data accordingly:

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 from complaint filing, which is 5 years from the complaint being filed.
	e-mail	from	User identification	GDPR Article 6 (1) f)	General civil law expiration time

	address	subject	Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	on Lawful interest	from complaint filing, which is 5 years from the complaint being filed.

1.6. Customer data managed by Simple for the 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. 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.

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

The data controller

The controller of the personal data specified under point 1.2. – 1.6 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.: 24386106-2-43
Seat: 1093 Budapest, Közraktár u. 30-32. RiverPark irodaház, K30 VII. emelet
Postal address: 1093 Budapest, Közraktár u. 30-32.
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
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 c) provision of SimplePay customer services
Borgun hf. (Ármúli 30, 108 Reykjavik, Iceland, cg. 440686-1259)	a) provision of online bank card payment service, bank card authorization, fraud monitoring
Microsoft Corporation (USA - One Microsoft Way Redmond, Washington 98052)	a) Microsoft 365 cloud service provision
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
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
Visa Europe Services LLC, incorporated in Delaware, USA, acting via its London branch office (branch No: BR007632) registered office: 1 Sheldon	a) conclusion of online bank card payments

Square, London W2 6TT, VAT Number: GB 840 111 776	
American Express Services Europe Limited, registered office: Belgrave House, 76 Buckingham Palace Road, London SW1W 9AX, United Kingdom, company reg. No: 1833139, Authority: Companies House.	a) conclusion of online bank card payments

The Rocket Science Group LLC d/b/a MailChimp is on the Privacy Shield List between the USA and the European Union, so the forwarding of data to them does not constitute forwarding to a third-party country, thus requiring no dedicated consent from the Customer.

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

János Weiner
Contact:
a) Simple offices (1093 Budapest, Közraktár u. 30-32.)
b) e-mail address: dpo@otpmobil.com
c) Postal address: 1093 Budapest, Közraktár u. 30-32.

4. To whom do we forward your personal data?

Your personal data is not forwarded to anyone except the data processors and the Merchants.

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

a) **Right of access**: they may inquire as to what employee data is managed, for what purposes, for how long, to whom do we forward them, and where the data originates from.
b) **Right of correction**: should their data change or be recorded wrong, they may request that this be rectified or corrected.
c) **Right of deletion**: in instances specified by law, they may request that we delete their stored personal data.
d) **Right of restriction:** in instances specified by law, they may request that data management be restricted regarding their personal data.
e) **Right to objection**: in instances specified by law, they may object to their personal data being managed, in which case we do not manage their personal data any further.
f) **Right to data portability**: the subject may request the porting of their personal data, in which case we hand over their stored data either to them, or directly to a data controller of their choosing, if such is technically safe.

The right to data portability request form can be downloaded from the link below: http://simplepay.hu/old/docs/201804/OTP_Mobil_Kft_adathordozhatosagi_kerelem_form.pdf

In cases of such requests, we conduct ourselves pursuant to applicable law, and will provide information on the rendered measures in one month.

We inform you, that cases of deletion requests, OTP Mobile Llc. shall – without any modifications whatsoever, except the modifications on your request for rectification – retain your aforementioned data processed for the purposes of enforcement of rights and claims, moreover for the efficient prevention, detection and handling of fraud for the general civil law limitation period of 5 years, for the purposes of enforcement of rights and claims, moreover for the efficient prevention, detection and handling of fraud. The anonymisation of data shall take place after the cessation of the pertaining legal interest.

g) **Right to revoke consent:** in cases where personal data is managed by the consent of the subject, they have the right to revoke such consent at any time, which does not affect the legality of data management conducted prior to the revocation

h) **Right of complaint:** should you have any complaints or grievances regarding our data management, you have the right to lodge a complaint by the supervisory authority:

National Authority for Data Protection and Freedom of Information
Website: http://naih.hu
Postal address: 1530 Budapest, Pf.: 5.
E-mail: ugyfelszolgalat@naih.hu
Telephone: +36 (1) 391-1400

Moreover, you may file a suit against Simple before the Municipal Court of Budapest if your personal data has been infringed upon.

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 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.

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

6.3. 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.

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.

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 an incident?

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?

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 within 30 days, as is required by GDPR. Please pay attention to the amendments of this notice, as they contain important information regarding the management of your personal data.