Annex 1 to the SimplePay Merchant GTC

Privacy policy on the data processing of Merchants' contact persons' personal data

Effective: from 22. 06. 2019

OTP Mobile Services Ltd. (seat: 1093 Budapest, Közraktár u. 30-32.; Cg. 01-09-174466; VAT No.: 24386106-2-43) hereby informs the contact persons of the Merchants about the processing of their personal data.

1. Data processing related to the SimplePay agreement for the purpose of concluding contract, communication and general case management

During the contracting with Merchants, Simple gains knowledge of the personal data of Merchant's representatives and contact personnel, moreover, if Merchant is a sole trader. Simple informs the Merchants and Merchant representatives of the processing of their data as follows.

Simple manages the personal data of sole trader Merchants pursuant to GDPR Article 6 (1) a), for the performance of a contract to which the data subject is party. Simple processes the personal data of Merchant representatives and contact personnel pursuant to GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller, which is Simple.

It is the joint legitimate interest of Simple and the Merchant for the personal data of the Merchant's representatives and contact persons to be managed, since it is necessary to conclude the contract between the Merchant and Simple, for keeping contact, and for providing contractual notifications to the Merchant. Only the essential personal data of the representative and the contact person are managed, so the fundamental rights and freedoms of the representative and the contact person are not infringed upon. and they do not preclude the legitimate interests of Simple.

The legal basis for the data management is specified below per data categories and management purposes.

Data subject	Governed data type	Purpose of data management	Legal basis of data management	Retention period
Contact person of Merchant	name	Creation and conclusion of contract Contact keeping	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract
	telephone number	Creation and conclusion of contract Contact keeping	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract
	e-mail address	Creation and conclusion of contract Contact keeping	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract
	recorded phone call	Customer service, complaint management Conclusion of contract	GDPR Article 6 (1) a) Consent of data subject	5 years from the date of the recording
Representative of Merchant	name	Creation and conclusion of contract Contact keeping	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract

	date and place of birth	Creation and conclusion of contract	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract
	mother's maiden name	Creation and conclusion of contract	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract
	position/authorization	Creation and conclusion of contract	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	5 years from the termination of contract
Sole trader Merchant	name	Creation and conclusion of contract Contact keeping Fulfilment of legal obligations Right- and claim exercising	GDPR Article 6 (1) b) Contracting and conclusion of contract GDPR Article 6 (1) c) Fulfilment of legal obligations – in case of data necessary for the fulfilment of tax law obligations: paragraphs 78. § (3), 202. § (1),of the Act CL of 2017 on the order of taxation, necessary for the fulfilment of the accounting obligations: 168-169 § of the Act C of 2000 on accounting GDPR Article 6 (1) f): Legitimate interest – in case of purposes for contact keeping and law enforcement	The documents necessary for the fulfilment of the tax obligation shall be kept for 5 years from the last day of the calendar year in which year the tax should have been reported or announced, or in case of lack of such report or announcement in which year the tax should have been paid; documents necessary for the fulfilment of the accounting obligation shall be kept for 8 years from the date of contract termination. In other cases for 5 years from the termination of the legal relationship.
	seat of the sole trader	Creation and conclusion of contract Contact keeping Invoicing Fulfilment of legal obligations Right- and claim exercising	GDPR Article 6 (1) b) Contracting and conclusion of contract GDPR Article 6 (1) c) Fulfilment of legal obligations – in case of data necessary for the fulfilment of tax law obligations: paragraphs 78. § (3), 202. § (1),of the Act CL of 2017 on the order of taxation, necessary for the fulfilment of the accounting obligations: 168-169 § of the Act C of 2000 on accounting GDPR Article 6 (1) f): Legitimate interest – in case of purposes for contact keeping and law enforcement	
	mother's maiden name	Creation and conclusion of contract Right- and claim exercising	GDPR Article 6 (1) b) Contracting and conclusion of contract GDPR Article 6 (1) f): Legitimate interest – in case of purposes for law enforcement	5 years from the termination of contract

	date and place of birth	Creation and conclusion of contract Right- and claim exercising	GDPR Article 6 (1) b) Contracting and conclusion of contract GDPR Article 6 (1) c) Fulfilment of legal obligations	5 years from the termination of contract
	sole trader registration number	Creation and conclusion of contract Fulfilment of legal obligations Right- and claim exercising	GDPR Article 6 (1) b) Contracting and conclusion of contract GDPR Article 6 (1) c) Fulfilment of legal obligations – in case of data necessary for the fulfilment of tax law obligations: paragraphs 78. § (3), 202. § (1),of the Act CL of 2017 on the order of taxation, necessary for the fulfilment of the accounting obligations: 168-169 § of the Act C of 2000 on accounting GDPR Article 6 (1) f): Legitimate interest – in case of purposes for contact keeping and law enforcement	The documents necessary for the fulfilment of the tax obligation shall be kept for 5 years from the last day of the calendar year in which year the tax should have been reported or announced, or in case of lack of such report or announcement in which year the tax should have been paid; documents necessary for the fulfilment of the accounting obligation shall be kept for 8 years from the date of contract termination. In other cases for 5 years from the termination of the legal relationship.

2. Data processing for the purpose of customer service

Simple provides customer services, to which the Merchants may turn through their contact persons with their questions and complaints. Simple processes the following personal data related to the customer services:

A	B	D	E	F
Data subject	**Data Category**	**Purpose of data management**	**Legal basis of data management**	**Duration of data management**
Contact person of the Merchant, and if the Merchant is a sole practitioner, the Merchant itself	name*	a) Identification b) Communication in course of complaint management and customer service c) Complaint management, customer service administration d) Claim and law enforcement	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.
	e-mail address*	a) Identification b) Communication in course of complaint management and customer service c) Complaint management, customer service administration d) Claim and law enforcement	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.

	Name of the Merchant represented	a) Identification b) Communication in course of complaint management and customer service c) Complaint management, customer service administration d) Claim and law enforcement	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.
	phone number	a) Identification b) Communication in course of complaint management and customer service c) Complaint management, customer service administration	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.
	recorded phone call	a) Identification b) Communication in course of complaint management and customer service c) Complaint management, customer service administration d) Quality assurance e) Consumer protection f) Proofing in a lawsuit g) Claim and law enforcement	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.
	subject of complaint	a) Complaint management b) Claim and law enforcement	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.
	Reg. No and ID card No. of the sole practitioner Merchant	a) Identification b) Communication in course of complaint management and customer service c) Complaint management, customer service administration d) Claim and law enforcement	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.

Data indicated by * are obligatory.

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: 1051 Budapest, Nádor u. 16.

Indication of legitimate interest in accordance with GDPR Article6 (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 your and our common interest, as well as the interest of the service providers of the services available within Simple Application, since the processing of these data is necessary for the enforcement of our consumer and civil rights and interests in connection with the the purchase made, service used within Simple Application. The processing of your personal data hereunder is not precluded by your right to self-determination of recorded voice, since your personal freedoms are not infringed upon, since at the very beginning of the phonecall, you are duly informed regarding the recording of audio that is to commence, leaving you ample opportunity to decide on continuing with the phonecall, or terminating it. The same services and solutions are also available via e-mail customer service, thus, you have a choice regarding the addressing of your complaint.

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

3. Data controller and data processors

The data controller

The controller of the personal data listed in clause 1 is Simple, the information of which are the following:

OTP Mobile Services Ltd.:

Seat: 1093 Budapest, Közraktár u. 30-32.
Reg. No.: 01-09-174466
Registry: Court of Registration of the General Court of Budapest
Tax No.: 24386106-2-43
Represented by: Péter Benyó Managing Director, individually

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 policy.

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:

Data processor	Data processor's activity
OTP Bank Plc. (seat: 1051 Budapest, Nádor u. 16.; company reg. no.: 01-10-041585; tax no.: 10537914-4-44)	a) provision of IT infrastructure b) accounting and bookkeeping c) document storage d) provision and support of company controlling software

Microsoft Corporation (USA - One Microsoft Way, Redmond, Washington 98052)	a) Microsoft 365 cloud services
Salesforce.com, Inc. (Salesforce Tower, 415 Mission St., San Francisco, California 94105)	Salesforce CRM system services, storing Merchant's data
XTK Kft. (seat: 1015 Budapest, Batthyány u 59. 2. em. 6.; Cg. 01-09-712431)	Introducing, supporting, maintenance and development of Salesforce CRM system,
Quadron Kibervédelmi Kft. (1051 Budapest, Sas u. 10-12.; Cg. 01-09-189206)	Cybersecurity services and consultation
Etalon-Informatika Kft. (1132 Budapest, Kresz Géza u. 53/b.; Cg. 01-09-668817)	IT infrastructure operation, system maintenance, professional support
Nconnect Hungary Kft. (2161 Csomád, Kossuth u. 79.; Cg. 13-09-140663)	IT security consultation

Information about data transfer to abroad:

Microsoft Corporation and SalesForce.com, Inc. is on the Privacy Shield List created under the decision of the European Commission based on article 45 of the GDPR and the executive order No 2016/1260; which means that the data transfer to those co'panies cannot deemed as data transfer to third countries outside of the European Union and the specific consent of the data subjects is not necessary and the data transfer to them is allowed by Article 45 of the GDPR. Those companies undertook the compliance with the GDPR.

4. Simple's data protection officer

Zsombor Sári
Contact:
a) Simple's seat (1093 Budapest, Közraktár u. 30-32.)
b) e-mail address: dpo@otpmobil.com
c) Mailing address: 1093 Budapest, Közraktár u. 30-32.

5. Data transfer

The personal data of Merchants' contact persons is not transferred by Simple to any third countries not party to the GDPR, these are only forwarded to data processors nominated under point 3. hereto.

6. Rights of Merchants' contact persons

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.

Requests and inquiries per the above are to be issued either electronically at our customer services contacts (ugyfelszolgalat@simple.hu) or via mail addressed to our postal address; in such cases, Simple conducts themselves pursuant to applicable law, and will provide information on the rendered measures in one month.

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

Consent may either be revoked electronically at our customer services contacts (ugyfelszolgalat@simple.hu) or via mail addressed to our postal address.

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.

7. Data security

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.

7.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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.

8. Processing of the personal data of the Merchant's factual owner, representative and persons with signing right for the purpose of identification and due diligence based on the anti-money laundering laws

If Simple uses Borgun hf. for providing the SimplePay services as background service provider for the purpose of authorisation, fraud monitoring, fraud prevention and bank card acceptance, Simple as the Borgun hf.'s data processor shall request the following personal data of the Merchant's representatives on behalf and for the request of Borgun hf. and shall transfer them to Borgun hf. as data controller based on the data processing agreement concluded with Borgun hf:

Data subject	Data categories
persons entitled to represent the Merchant	Name
	Address
	Mother's maiden name
	Place and date of birth
	ID Number of ID card
	Photo on the ID card
	Validity of the ID card
	Signature ont he ID card

	Gender ont he ID card (male/female)
	Citizenship
	Name of the issuer, date of issuance
	State issuing the ID card
	ID number of the address card
	Address ont he address card and date of announcement of this address
	Name of the authority issued the address card, date of issuance

Neither Simple nor Borgun hf processes and is entitled to process the personal identification number on the address card.

The purpose of the processing of the aforementioned data: identification and due diligence based on the anti-money laundering laws (due diligence and know your customer – KYC).

The Borgun hf. (Ármúli 30, 108 Reykjavik, Iceland) is the data controller of the aforementioned data, Simple requests those data as data processor of Borgun hf., for the request of and on behalf of Borgun hf and transfers them to Borgun hf.

Borgun hf. as data controller provides detailed information about the aforementioned data processing of the aforementioned personal data.

Furthermore, if the Merchant enters into a SimplePay agreement for the acceptance of American Express bankcard with Simple, Simple is obliged to transfer the following data of the Merchant's representative, persons having signing right and Merchant's factual owner to OTP Bank Nyrt (1051 Budapest, Nádor u. 16.) and through it to American Express:

Data subject	**Data categories**
Merchant's representative, factual owner and persons having signing rights	Name
	Address
	Date of birth
	ID Number of ID card
	Citizenship

The purpose of the processing of the aforementioned data: identification and due diligence based on the anti-money laundering laws (due diligence and know your customer – KYC).

Simple, OTP Bank Nyrt. and the American Express qualify as data controller of the aforementioned data. The legal basis of Simple's data processing is Article 6 (1) f) of the GDPR: legitimate interest.

Designation of the legitimate interest: Simple's legitimate interest is the due diligence of the Merchant and to identify the representatives and factual owners of the Merchant in order to prevent money-laundering which is possible with the aforementioned data.

Simple stores the aforementioned data for 5 years after the termination of the SimplePay agreement concluded with the Merchant.

(end of the document)