Annex 1 to the SimplePay Merchant GTC

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

OTP Mobile Services Ltd. (seat: 1143 Budapest, Hungária krt. 17-19.; 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.

For the request of the data subject, the data subject is entitled to receive the legitimate interest balancing tests regarding the data processing based on legitimate interest. The request shall be submitted to the customer service e-mail address.

In case of data processing based on legitimate interest, the data subject is entitled to object against the data processing; in this case the Data controller does not process his/her data further.

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

Data subject	Categories of data	Purpose of data processing	Legal basis of data processing	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	If the data are in documents necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid. If the data are in the contract concluded with the Merchant,
	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	
	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	

				the data will be stored and kept for the fulfilment of the accounting obligations for 8 years from the termination of the contract. In any other case the data shall be stored for 5 years after the termination of the contract concluded by the Merchant.
	recorded phone call	Customer service, complaint management Conclusion of contract	GDPR Article 6 (1) a) Consent of data subject	until the withdrawal of the consent, in lack of that 5 years from the termination of the contract
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	If the data are in documents necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid. If the data are in the contract concluded with the Merchant, the data will be stored and kept for the fulfilment of the accounting obligations for 8 years from the termination of the contract. In any other case the data shall be stored for 5 years after the termination of the contract concluded by the Merchant.
	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	
	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	
	position/authorization	Creation and conclusion of contract	GDPR Article 6 (1) f) for the purposes of the legitimate interests pursued by the controller	
Sole trader Merchant	name	Creation and conclusion of contract	GDPR Article 6 (1) b) Contracting and conclusion of contract	If the data are in documents necessary for the fulfilment of tax obligations, they

		Contact keeping Fulfilment of legal obligations Right- and claim exercising	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	will be stored for 5 years calculated from the last year from that calendar year in which the tax should have been reported or in the lack of reporting in which the tax should have been paid. If the data are in the contract concluded with the Merchant, the data will be stored and kept for the fulfilment of the accounting obligations for 8 years from the termination of the contract. In any other case the data shall be stored for 5 years after the termination of the contract concluded by the Merchant.
	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	GDPR Article 6 (1) b) Contracting and conclusion of contract	

		Right- and claim exercising	GDPR Article 6 (1) f): Legitimate interest – in case of purposes for law enforcement	
	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	
	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	

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,	name*	a) Identification b) Communication in course of complaint management and customer service	GDPR Article 6 (1) f) Legitimate Interest	Within the general civil law limitation period following the complaint, that is 5

and if the Merchant is a sole practitioner, the Merchant itself		c) Complaint management, customer service administration d) Claim and law enforcement		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. 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 on the ID card

	Gender on the ID card (male/female)
	Citizenship
	Name of the issuer, date of issuance
	State issuing the ID card
	ID number of the address card
	Address on the 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.

4. Data processing concerning the enforcement of the data subjects' data protection rights (see clause 9)

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)	Personal data submitted to the Data controller in connection with the data protection requests: in case of private persons, legal entities and	**Duration of data processing:** in lack of other data protection authority guidance:

	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.	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.	indefinite period of time.

5. 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 protection breaches (including documentation of steps taken related to the management of the incidents)	GDPR Article 6 (1) c) (the data processing is necessary for fulfilling 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.	Personal data of the data subjects related to the data protection incident.	**Duration of data processing:** in lack of other data protection authority guidance: indefinite period of time.

6. Data controller and data processors

The data controller

The controller of the personal data listed in clause 1, 4 and 5 is Simple, the information of which are the following:

OTP Mobile Services Ltd.:

Seat: 1143 Budapest, Hungária krt. 17-19.
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 companies 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.

7. Simple's data protection officer

Zsombor Sári
Contact:
a) Simple's seat (1143 Budapest, Hungária krt. 17-19.)
b) e-mail address: dpo@otpmobil.com
c) Mailing address: 1143 Budapest, Hungária krt. 17-19.

8. 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.

9. Rights of Merchants' contact persons

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 Data controller provides information for the individuals in accordance with the above articles about their rights and remedies related to the processing of personal data.

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

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

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

9.1 The individual's right of access

(1) The individual has the right to obtain confirmation from the Data controller whether or not personal data concerning him/her are being processed. Where the case is such, then he/she is entitled to have access to the personal data concerned and to the following information:

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

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

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

9.2 Right to rectification

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

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

(1) The individual has the right that when he/she so requests, the Data controller erase the personal data concerning him/her without delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed by the Data controller;

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

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

(3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary, among other things, for:

a) exercising the right of freedom of expression and information;
b) compliance with a legal obligation which requires processing by Union or Member State law to which the Data controller is subject;
c) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
d) the establishment, exercise or defence of legal claims.

9.4 Right to restriction of processing

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

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

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

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

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

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

9.6 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 Data controller in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Data controller, where:

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

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

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

9.7 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 Data controller will no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims.

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

9.8 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: 1125 Budapest, Szilágyi Erzsébet fasor 22/c; mailing address: 1530 Budapest, POB 5; Phone: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu).

9.9 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.

9.10 Right to an effective judicial remedy against the Data controller or the processor

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

(2) Proceedings against the Data controller or a processor shall be brought before the courts of the Member State where the Data controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the individual has habitual residence. You can find more information about the availabilities of the courts here: www.birosag.hu.

10. 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.

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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.

10.5. 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.

11. 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.

12. 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.