

## PRIVACY POLICY ON THE DATA PROCESSING OF MERCHANTS' CONTACT PERSONS' PERSONAL DATA

Effective: 22 June 2026.

**SimplePay Private Company Limited by Shares** (Registered seat: 1138 Budapest, Váci út 135-139. B. building, 5th floor; Company reg. no.: 01-10-143303; tax number: 32835155-2-44, hereinafter referred to as "Simple" or "Controller") hereby informs the contact persons of Merchants contracted for the SimplePay service about the processing of their personal data in this privacy notice.

### 1. **Data processing related to the SimplePay agreement for the purpose of communication, general case management, and in case of sole traders, data processing for the purpose of concluding contract**

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, also of the personal data of the Merchant. Simple informs the Merchants, the Merchant's representatives and these contact personnel of the processing of their data as follows.

Simple manages the personal data of sole trader Merchants pursuant to GDPR Article 6 (1) b), 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, or by a third party.

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 in full 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 or a third party	If the data are in documents necessary for the fulfilment of tax obligations, they will be stored for 5 years calculated from the last

Data subject	Categories of data	Purpose of data processing	Legal basis of data processing	Retention period
	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 or a third party	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.
	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 or a third party	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.
	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 or a third party	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.
	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 or a third party	
	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 or a third party	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.
	position/ authorization	Creation and conclusion of contract	GDPR Article 6 (1) f) for the purposes of the legitimate	

Data subject	Categories of data	Purpose of data processing	Legal basis of data processing	Retention period
			interests pursued by the controller or a third party	In any other case the data shall be stored for 5 years after the termination of the contract concluded by the Merchant.
Sole trader Merchant	name	Creation and conclusion of contract Contact keeping Fulfilment of legal obligations Right- and claim exercising	<p>GDPR Article 6 (1) b) Contracting and conclusion of contract</p> <p>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</p> <p>GDPR Article 6 (1) f): Legitimate interest – in case of purposes for contact keeping and law enforcement</p>	<p>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.</p> <p>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.</p> <p>In any other case the data shall be stored for 5 years after the termination of the contract concluded by the Merchant.</p>
	seat of the sole trader	Creation and conclusion of contract Contact keeping Invoicing Fulfilment of legal obligations Right- and claim exercising	<p>GDPR Article 6 (1) b) Contracting and conclusion of contract</p> <p>GDPR Article 6 (1) c) Fulfilment of legal obligations – in case of data</p>	

Data subject	Categories of data	Purpose of data processing	Legal basis of data processing	Retention period
			<p>necessary for the fulfilment of tax law obligations: paragraphs 78. § (3), 202. § (1), of the Act CL of 2017 on the order of taxation,</p> <p>necessary for the fulfilment of the accounting obligations: 168-169 § of the Act C of 2000 on accounting</p> <p>GDPR Article 6 (1) f): Legitimate interest – in case of purposes for contact keeping and law enforcement</p>	
	mother's maiden name	<p>Creation and conclusion of contract</p> <p>Right- and claim exercising</p>	<p>GDPR Article 6 (1) b) Contracting and conclusion of contract</p> <p>GDPR Article 6 (1) f): Legitimate interest – in case of purposes for law enforcement</p>	
	date and place of birth	<p>Creation and conclusion of contract</p> <p>Right- and claim exercising</p>	<p>GDPR Article 6 (1) b) Contracting and conclusion of contract</p> <p>GDPR Article 6 (1) c) Fulfilment of legal obligations</p>	
	sole trader registration number	<p>Creation and conclusion of contract</p> <p>Fulfilment of legal obligations</p> <p>Right- and claim exercising</p>	<p>GDPR Article 6 (1) b) Contracting and conclusion of contract</p> <p>GDPR Article 6 (1) c) Fulfilment of legal obligations –</p>	

Data subject	Categories of data	Purpose of data processing	Legal basis of data processing	Retention period
			<p>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</p> <p>GDPR Article 6 (1) f): Legitimate interest – in case of purposes for contact keeping and law enforcement</p>	
	Tax ID of the sole trader	<p>Creation and conclusion of contract            Fulfilment of legal obligations</p>	<p>GDPR Article 6 (1) b)            Contracting and conclusion of contract</p> <p>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</p>	

Data subject	Categories of data	Purpose of data processing	Legal basis of data processing	Retention period
			of 2000 on accounting	
	Annual payment volume of the sole trader	Calculation of the contractual fee	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	E-mail address	Creation and conclusion of contract Communication	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	Phone number	Creation and conclusion of contract Communication	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	Range of activity (MCC code)	Creation and conclusion of contract	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	Address of the physical store in case of Simple Business Services	Creation and conclusion of contract	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	URL address of the online store in case of SimplePay Services	Creation and conclusion of contract	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	Merchant ID	Identification of the Merchant, settlement based on the agreement	GDPR Article 6 (1) b) Contracting and conclusion of contract	
	Device ID of the mobile device connected to the SoftPOS Endpoint in case of SoftPOS Services	Settlement based on the agreement	GDPR Article 6 (1) b) Contracting and conclusion of contract	

## 2. Data processing for the purpose of customer service and Service Desk

Simple provides customer services via phone, e-mail and Service Desk online portal, to which the Merchants may turn through their contact persons with their questions, requests, submissions and complaints. Furthermore, Simple provides an AI-based chatbot interface

available on its website for Merchants using the SimplePay Service pursuant to the general terms and conditions applicable to the SimplePay Service (SimplePay Service GTC, available at: <https://simplepay.hu/kereskedo-aszf/>) and their contact persons, for inquiries related to general information about merchant services, contact initiation, recording of callback requests, as well as preparation of registration. While using the chatbot, Simple processes the data of Merchants and their contact persons specified in Section 1 to the extent necessary to respond to the inquiry. Simple processes the following personal data related to the customer services:

A	B	C	D	E
Data subject	Data Category	Purpose of data processing	Legal basis of data processing	Duration of data processing
Contact person of the Merchant, and if the Merchant is a sole practitioner, the Merchant itself	name* (in phone, e-mail, chatbot and Service Desk customer services)	a) Identification b) Communication in course of complaint, submission, request management and customer service c) Complaint, submission, request 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* (in phone, e-mail, chatbot and Service Desk customer services)	a) Identification b) Communication in course of complaint, submission, request management and customer service c) Complaint, submission, request 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* (in phone, e-mail, chatbot and Service Desk customer services)	a) Identification b) Communication in course of complaint, submission, request management and customer service c) Complaint, submission, request 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.

A	B	C	D	E
Data subject	Data Category	Purpose of data processing	Legal basis of data processing	Duration of data processing
	phone number* (in phone, e-mail and Service Desk customer services)	<ul style="list-style-type: none"> <li>a) Identification</li> <li>b) Communication in course of complaint, submission, request management and customer service</li> <li>c) Complaint, submission, request management, customer service administration</li> </ul>	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 (only in phone customer service)	<ul style="list-style-type: none"> <li>a) Identification</li> <li>b) Communication in course of complaint, submission, request management and customer service</li> <li>c) Complaint, submission, request management, customer service administration</li> <li>d) Quality assurance</li> <li>e) Consumer protection</li> <li>f) Proofing in a lawsuit</li> <li>g) Claim and law enforcement</li> </ul>	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 and description of complaint, submission and request* (in phone, e-mail and Service Desk customer services)	<ul style="list-style-type: none"> <li>a) Complaint, submission, request management</li> <li>b) Claim and law enforcement</li> </ul>	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.
	Information voluntarily provided during a conversation with the chatbot	<ul style="list-style-type: none"> <li>a) Tracking of case management</li> <li>b) Quality assurance</li> <li>c) Error handling</li> <li>d) Claim and law enforcement</li> </ul>	GDPR Article 6 (1) f) Legitimate Interest	Within the general civil law limitation period following the closure of the conversation, that is 5 years from the closure of the conversation.

A	B	C	D	E
Data subject	Data Category	Purpose of data processing	Legal basis of data processing	Duration of data processing
	password (only in Service Desk)	Registration in Service Desk system, identification	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 (Only in phone and e-mail customer service)	a) Identification b) Complaint, submission, request management, customer service administration c) 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 processes the personal data in Service Desk service.

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 statement. 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](mailto: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, submissions, requests, examination, settlement and management of the complaint, submissions, requests 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 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 phone call, you are duly informed regarding the recording of audio that is to commence, leaving you ample opportunity to decide on continuing with the phone call, or terminating it. The same services and solutions are also available via e-mail customer service and in Service Desk service, thus, you have a choice regarding the addressing of your complaint, submissions, requests.

**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](mailto: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:

<b>Data subject</b>	<b>Data categories</b>
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.

**4. Data processing concerning the enforcement of the data subjects’ data protection rights (see clause 12)**

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

Legal basis of data processing	Data categories	Duration of data processing
<p>GDPR Article 6 (1) c) (the data processing is necessary for fulfilling the legal obligation of Data controller)</p> <p><b>Legal obligation:</b> 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.</p>	<p>Personal data submitted to the Data controller in connection with the data protection requests: in case of private persons, legal entities and other organisations turning to the Data controller the contact details of the contact persons necessary for communication with them (in particular: name, address, phone number, e-mail address), content of the request, steps concerning the request, documents concerning the request. For example: if the data</p>	<p>Lacking other data protection authority guidance: indefinite period of time.</p>

	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.	
--	--	--

**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 Processing	Legal basis of data processing	Data categories	Duration of data processing
Recording data protection incidents (including documentation of steps taken in connection with incident management)	<p>GDPR Article 6 (1) c) (the data processing is necessary for fulfilling the legal obligation of Data controller)</p> <p><b>Legal obligation:</b> 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.</p>	Personal data of the data subjects related to the data protection incident.	Lacking other data protection authority guidance: indefinite period of time.

**6. Data processing for the purpose of sending IT circular letters**

Simple sends information in e-mail about the use, set up of SimplePay system, integration with the Merchant's IT system to the IT contact persons of Merchants who have been already entered into a SimplePay contract with Simple, and who have been already used the SimplePay sandbox but not entered into a SimplePay contract yet and who are interested in the SimplePay services. The IT circular letter does not contain any marketing content or advertisement.

Simple processes the following personal data in connection with IT circulate letters:

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
Contact person of Merchant	Name E-mail address	Creating the integration between SimplePay	GDPR article 6 (1) f): Legitimate interest, which is	Until the termination of the Merchant's contract

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
concluded SimplePay contract		system and the Merchant's IT system, supporting the IT contact persons of the Merchant with technical information in order to fulfil the contract	the following: It is the legitimate business interest of SimplePay Zrt. and the Merchant to connect the SimplePay system with the Merchant's IT system pursuant to the SimplePay contract and to initiating transactions through this connection and to provide the Merchant's IT professionals with up-to-date information. Furthermore, during the contract, it is the legitimate business interest of SimplePay Zrt. and the Merchant to inform the Merchant about all technical change in order to modify its systems accordingly.	
Contact persons of Merchants without SimplePay contract but using SimplePay sandbox and aiming to join SimplePay system	Name E-mail address	Creating the integration between SimplePay system and the Merchant's IT system, supporting the IT contact persons of the Merchant with technical information in order to conclude the contract and to find the appropriate	GDPR article 6 (1) f): Legitimate interest, which is the following: It is the legitimate business interest of SimplePay Zrt. and the Merchant to find and test the appropriate technical solution for the integration between SimplePay system and the	Until the termination of the Merchant's contract. If the contract will not be concluded, for 1 year.

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
		technical solution for the integration.	Merchant's IT system, and to provide the IT professionals of the Merchant with up-to-date technical information. Without that the Merchant is not able to decide on the integration and conclusion of the contract.	
Contact person of the Merchant without SimplePay contract and without using SimplePay sandbox who is interested in the SimplePay services	Name E-mail address	Providing the Merchant with information about the technical conditions of integration to the SimplePay system in order to support the decision making process of the Merchant.	GDPR article 6 (1) a): Consent	Until withdrawing consent

The data subject is entitled to object against the data processing based on legitimate interest at any time.

Simple provides the data subjects with the legitimate interest balancing tests for request in case of data processing based on legitimate interest.

In case of data processing based on consent, the data subject is entitled to withdraw his/her consent at any time in an e-mail sent to Simple: [ugyfelszolgalat@simple.hu](mailto:ugyfelszolgalat@simple.hu), or via mail sent to Simple or by clicking to the unsubscribe button in the IT circulate letter.

Granting consent is not precondition of entering into SimplePay contract, withdrawing consent has no legal effect on the effect of the SimplePay contract.

In case of data processing based on consent, Simple registers the data subject's consent according to article 6 (1) c) of the GDPR as legal obligation, for the purpose of which Simple processes the name and the consent of the data subject until the consent has been withdrawn. The purpose of this data processing is to register consents, legal basis is GDPR article 6 (1) c): fulfilment of legal obligation.

## 7. Sending educational materials to Merchants

Simple may send, by e-mail, informational and educational materials, presentations, webinar invitations and videos (hereinafter collectively “Educational Materials”) to the contact persons designated by already contracted Merchants, relating to the operation of their webshops affected by the SimplePay service. These Educational Materials may support the development of the Merchants’ webshops and companies, especially, but not exclusively, in general marketing, sales, e-commerce, organizational psychology topics. Educational Materials may also cover legal, tax, economic, and other professional issues of webshop operation, presented by Simple and external experts engaged by Simple. The Educational Materials sent under this point do not contain advertisements.

Simple processes the following personal data related to sending educational materials:

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
Contact person of Merchant who concluded a SimplePay contract	Name E-mail address	Informing the Merchant through their contact persons about the legal, taxation, professional information. Sending Educational Materials and educating the Merchants, helping Merchants in operation their webshop lawfully and effectively.	GDPR article 6 (1) f): Legitimate interest, which is the following: It is the legitimate business interest of Simple and the Merchant that the webshop of Merchants contracted for SimplePay services operates lawfully, professionally and that Simple helps in it with providing information in legal, taxation, economical, logistical and other professional issues and to educate the Merchants by which the webshops will operate in a more customer friendly and secure way.	Until the termination of the Merchant’s contract

The data subject is entitled to object against the data processing based on legitimate interest at any time.

Simple provides the data subjects with the legitimate interest balancing tests for request in case of data processing based on legitimate interest.

**8. Sending educational materials, and payment strategy materials and relating electronic direct marketing messages, advertisement and offers**

Simple sends to the Merchants' contact persons – upon their consent – educational materials related to the lawful, effective and professional operation of the webshop which electronic messages contains direct marketing, advertisement content and offers.

Furthermore, the Simple sends payment strategy material related to the payment methods on the Merchant's webshop to the Merchant's contact person and related to which the Simple reaches out the Merchant's contact person with offer for entering into a SimplePay agreement. The Merchant first answers the questions raised by Simple on the Simple's dedicated webshop by entering the Merchant's company name and tax ID and the name, e-mail address and phone number of the Merchant's contact person and submits this to Simple. Simple sends the payment strategy materials related to the Merchant and based on the Merchant's answers to the e-mail address of the Merchant's contact person. After that with the consent of the Merchant's contact person, Simple may call the Merchant's contact person and may provide a SimplePay offer to him/her.

Simple processes the following personal data related to this data processing:

<b>Data subject</b>	<b>Data category</b>	<b>Purpose of data processing</b>	<b>Legal basis of data processing</b>	<b>Retention period</b>
In case of educational materials: Merchant's contact person without SimplePay contract but who is interested in SimplePay services	Name E-mail address	Sending educational materials to the Merchant to its contact person which contain electronic direct marketing, offers, promotions, advertisements.	GDPR art. 6 (1) point a): consent.	Until revocation of consent.
In case of payment strategy materials: Merchant's contact person without SimplePay contract who answered the questions raised by	Name E-mail address Phone number	Sending payment strategy materials to the Merchant's contact person related to the payment solutions in the Merchant's webshop and contacting the Merchant's contact persons via phone or e-mail related to this with sending electronic direct	GDPR art. 6 (1) point a): consent.	Until revocation of consent.

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
Simple related to the payments and submitted them to Simple in order to receive the payment strategy materials		marketing content including offers, promotions, advertisements.		

In case of data processing based on consent, the data subject is entitled to withdraw his/her consent at any time by clicking to the unsubscribe or revocation button in the letter or upon the choice of the data subject, in an e-mail sent to Simple: [ugyfelszolgalat@simple.hu](mailto:ugyfelszolgalat@simple.hu), or via mail sent to Simple.

Granting consent is not precondition of entering into SimplePay contract, withdrawing consent has no legal effect on the effect of the SimplePay contract.

In case of data processing based on consent, Simple registers the data subject's consent according to article 6 (1) c) of the GDPR as legal obligation, for the purpose of which Simple processes the name and the consent of the data subject until the consent has been withdrawn. The purpose of this data processing is to register consents, legal basis is GDPR article 6 (1) c): fulfilment of legal obligation.

## 9. Sending direct marketing messages

Simple sends marketing messages containing newsletters, promotions, offers, advertisements, promotions, advertisements, and advertisements to the contact persons of Merchants who have given their consent, by direct solicitation via e-mail and other electronic communication channels. These newsletters will also be sent to the contacts of Merchants who have contracted with Simple, wish to contract with Simple, are interested in Simple's services and are potential customers for Simple, provided that they have given their consent.

Simple processes the following personal data in this context:

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
Contact person of the Merchant	Name, e-mail address	Sending marketing messages containing newsletters, promotions, offers, advertisements, advertisements to the Merchant through its designated contact person by direct mail by electronic means.	GDPR art. 6 (1) point a): consent.	Until revocation of consent.

In case of data processing based on consent, the data subject is entitled to withdraw his/her consent at any time by clicking to the unsubscribe or revocation button in the letter or upon the choice of the data subject, in an e-mail sent to Simple: [ugyfelszolgalat@simple.hu](mailto:ugyfelszolgalat@simple.hu), or via mail sent to Simple.

Granting consent is not precondition of entering into SimplePay contract, withdrawing consent has no legal effect on the effect of the SimplePay contract.

In case of data processing based on consent, Simple registers the data subject's consent according to article 6 (1) c) of the GDPR as legal obligation, for the purpose of which Simple processes the name and the consent of the data subject until the consent has been withdrawn. The purpose of this data processing is to register consents, legal basis is GDPR article 6 (1) c): fulfilment of legal obligation.

#### 10. **Sending conference and event invitations, participation offers, coupons**

Simple sends to the contact persons provided by its contracted Merchants, legal entities, invitations to conferences and events organized by Simple, as well as participation offers and coupons in the form of electronic mail to promote events and latest news about e-commerce and business activities related to the contracted Merchants.

Simple processes the following data in this context:

<b>Data subject</b>	<b>Data category</b>	<b>Purpose of data processing</b>	<b>Legal basis of data processing</b>	<b>Retention period</b>
Contact person of Merchant who concluded a SimplePay contract	Name Email address	Conference, event organised by the Controller and promotion of the Controller's activities	GDPR art. 6 (1) point f): legitimate interest, which is the following: It is in the legitimate interest of the Controller to inform the Merchants about the latest news related to e-commerce and the business activities affecting them, and to invite partners to conferences and events on this topic organised by the Controller through their contacts by sending them an email, to send them discounted participation offers, coupons and to promote these conferences and events.	1 month after the date of the conference or event

The data subject has the right the object, which can be exercised by sending a letter to the email address of the customer service or by post.

**11. Business development inquiries, business and other cooperation-related value propositions, and the sending of related questionnaires**

The Data Controller sends business development inquiries, business and other (e.g. sweepstakes-related) cooperation-related value propositions, as well as related questionnaires to the contact persons of the Merchants.

Simple processes the following data in this context:

Data subject	Data category	Purpose of data processing	Legal basis of data processing	Retention period
Contact person of Merchant who concluded a SimplePay contract	Upon sending the inquiry, offer, questionnaire:  Name Email address	Sending business development offers and questionnaires	GDPR art. 6 (1) point f): legitimate interest, which is the following:  The Data Controller has a legitimate business interest, in connection with the SimplePay contract concluded with the Merchant, to send inquiries and offers to the Merchant for the development and expansion of business cooperation, and to request feedback from the Merchants regarding the business relationship and the SimplePay service for the purpose of developing the relationship and the SimplePay service. The Data Controller also has a legitimate interest in maintaining an up-to-date merchant e-mail address database for the purpose of the aforementioned inquiries.	Until the termination of the Merchant's contract
	Upon completing the questionnaire:  Email address			

The data subject has the right the object, which can be exercised by sending a letter to the email address of the customer service or by post.

## 12. Data controller and data processors

The data controller

The controller of the personal data listed in clause 1, 4 and 5 - 8 is Simple, the information of which are the following:

### SimplePay Zrt.:

Seat: 1138 Budapest, Váci út 135-139. B. ép. 5. em.

Reg. No.: 01-10-143303

Registry: Court of Registration of the General Court of Budapest

Tax No.: 32835155-2-44

Represented by: Péter Bese 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	Information regarding data transfer to abroad
<b>OTP Bank Plc.</b> (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	There is no data transfer to abroad.
<b>Microsoft Corporation</b> (USA - One Microsoft Way, Redmond, Washington 98052)	Microsoft 365 cloud services	Data is transferred to the USA.  Legal basis of transfer: During the transfer of data to the USA, Microsoft ensures the adequate protection of personal data through its certification obtained under the Data Privacy Framework adopted by Commission Implementing Decision (EU) 2023/1795 of the European Commission. Further information: <a href="https://www.dataprivacyframework.gov/">https://www.dataprivacyframework.gov/</a> .

Data processor	Data processor's activity	Information regarding data transfer to abroad
<b>Salesforce.com, Inc.</b> (Salesforce Tower, 415 Mission St., San Francisco, California 94105)	Salesforce CRM system services, storing customer data, Provision of Salesforce Agentforce chatbot services	Data is transferred to the USA.  Legal basis of transfer: During the transfer of data to the USA, Salesforce ensures the adequate protection of personal data through its certification obtained under the Data Privacy Framework adopted by Commission Implementing Decision (EU) 2023/1795 of the European Commission. Further information: <a href="https://www.dataprivacyframework.gov/">https://www.dataprivacyframework.gov/</a> . Further information: <a href="https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/Agreements/data-transfer-mechanisms-FAQ.pdf">https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/Agreements/data-transfer-mechanisms-FAQ.pdf</a> .
<b>Twilio Inc.</b> (101 Spear Street, 5th floor, San Francisco, CA 94105, USA)	a) Sending newsletters, storing e-mail addresses in newsletter database, b) Sending system messages, storing e-mail addresses in mailing system database	Data is transferred to the USA.  Legal basis of transfer: During the transfer of data to the USA, Twilio ensures the adequate protection of personal data through its certification obtained under the Data Privacy Framework adopted by Commission Implementing Decision (EU) 2023/1795 of the European Commission. Further information: <a href="https://www.dataprivacyframework.gov/">https://www.dataprivacyframework.gov/</a> .
<b>XTK Kft.</b> (seat: 1015 Budapest, Batthyány u 59. 2. em. 6.; Cg. 01-09-712431)	Introducing, supporting, maintenance and development of Salesforce CRM system,	There is no data transfer to abroad.
<b>Etalon-Informatika Kft.</b> (1132 Budapest, Kresz Géza u. 53/b.; Cg. 01-09-668817)	IT infrastructure operation, system maintenance, professional support	There is no data transfer to abroad.
<b>nConnect Hungary Kft.</b> (2161 Csomád, Kossuth u. 79.; Cg. 13-09-140663)	IT security consultation	There is no data transfer to abroad.

Data processor	Data processor's activity	Information regarding data transfer to abroad
<p><b>CircleBlue Pay, s.r.o.</b> (Mostecká 273/21, Malá Strana, 118 00 Praha 1) <b>CIRCLEBLUE d.o.o.</b> (Zagrebacka cesta 143a, 10000, Zagreb, Croatia)</p>	<p>Maintenance, support of SoftPOS mobile application and software, providing SoftPOS switching services</p>	<p>There is no data transfer to abroad.</p>
<p><b>Slack Technologies Limited</b> (Salesforce Tower 60 R801, North Dock, Dublin, Ireland )</p>	<p>Task management and internal communication for the employees of the Data Controller.</p>	<p>Data is transferred to Australia, India, South Korea and the USA, in which case the legal basis of the transfer is as follows: Slack applies the standard contractual clauses pursuant to Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as approved by the European Commission ("Standard Contractual Clauses" or "SCC"). A copy of the Data Processing Addendum (DPA) incorporating the Standard Contractual Clauses is <a href="https://slack.com/terms-of-service/data-processing">available here: https://slack.com/terms-of-service/data-processing</a>.</p> <p>Data is also transferred to Canada and Japan, in which case the legal basis of the transfer is as follows: Commission Decision (2002/2/EC) of the European Commission <i>on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act</i>, available at: <a href="https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002D0002">https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002D0002</a>; and Commission Implementing Decision (EU) 2019/419 <i>on the adequate protection of personal data provided by Japan under the Act on the Protection of Personal Information</i>, available at: <a href="https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0419">https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0419</a>.</p>
<p><b>OTRS Hungary Ltd.</b> (1062 Budapest, Váci út 1-3. 3. em. 318. ajtó; Cg 01-09-326618)</p>	<p>Providing Service Desk software solution</p>	<p>There is no data transfer to abroad.</p>

Data processor	Data processor's activity	Information regarding data transfer to abroad
<b>Survey Monkey Europe UC</b> (70 Sir John Rogerson's Quay Dublin 2 D02 R296 Ireland)	Providing questionnaire application in which e-mail address, name and the answers of the questions as personal data are processed	There is no data transfer to abroad.
<b>CMO24 Hungary Plc.</b> 1133 Budapest, Véső utca 3. Reg. No.: 01-10-143424	Intermediary of contract: contact persons' name, e-mail address, phone number, sole practitioner's name, tax ID.	There is no data transfer to abroad.
<b>Protocall 2009 Ltd.</b> (2724 Újlengyel, Ady Endre utca 41., Reg. No.: 13-09-140629)	Performing Protocall customer service activities, contacting Merchants via e-mail and phone, acting on behalf of and on the instructions of the Data Controller.	There is no data transfer to abroad.

#### Individual recipients of data transfers

On the instructions and on behalf of the Merchant as the data controller, Simple transfers data to GIRO Plc. and Innopay Plc. in the case of a payment (instant transfer) solution based on the Uniform Data Entry Solutions (qvik Service), in the context of which the transaction data of the Merchants are transferred.

Furthermore, Simple transfers the following personal data to CMO24 Hungary Plc as data controller for the purpose of contacting the merchants: the name, e-mail address, phone number of the merchant's contact person, tax ID of the sole proprietor in case of merchants which indicated that they are interested in the services of the CMO24 Hungary Plc during the contractual onboarding with Simple and granted consent to the data transfer. The data subject can withdraw their consent any time by sending e-mail to Simple.

#### 13. Simple's data protection officer

##### Zsombor Sári

Contact:

- (a) Simple's seat (1138 Budapest, Váci út 135-139. B. ép. 5. em.)
- (b) e-mail address: [dpo@simplepay.com](mailto:dpo@simplepay.com)
- (c) Mailing address: 1138 Budapest, Váci út 135-139. B. ép. 5. em.

#### 14. 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 and data controller nominated under point 3. hereto.

## **15. Rights of Merchants' contact persons**

The detailed rights and remedies of the data subjects 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 month 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.

### **15.1 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.

## **15.2 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.

## **15.3 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.

#### **15.4 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.

#### **15.5 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.

#### **15.6 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.

#### **15.7 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.

If the individual objects to system messages (for example, notifications of shutdowns, planned maintenance, upgrades) and does not wish to receive such messages in the future, the Data controller will no longer send system messages to the individual. Due to the technical operation of the database containing the name and e-mail address of the individual used by the Data controller to send system messages, and in view of the system update time required for the technical implementation of the right to object, the individual may receive further system messages within 48 hours at the latest after the exercise of his/her right to object and unsubscribe.

#### **15.8 Right to lodge a complaint with a supervisory authority**

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

#### **15.9 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.

#### **15.10 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. In Hungary, such proceedings fall within the jurisdiction of the regional court. The individual may also bring proceedings – at his/her discretion – before the regional court competent by his/her domicile or habitual residence. You can find more information about the jurisdiction and contact details of the courts here: [www.birosag.hu](http://www.birosag.hu).

## **16. 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.

### **16.1 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 the data processed by us.

Office workstations are password protected, third-party storage devices are restricted and may only be used under secure circumstances, following inspection.

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

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

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

### **16.2 Data security in communications**

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

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

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

### **16.3 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. 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.

### **16.4 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.

### **16.5 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. Security and protection of the office premises is ensured on a 24/7 basis.

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.

**17. 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.

**18. 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](http://www.simplepay.hu) website. Please pay attention to the amendments of this notice, as they contain important information regarding the management of your personal data.

(end of document)