Privacy Notice of Virpay Payment Service Provider Ltd.

1. Purpose and scope of the Privacy Notice, Governing Law

The purpose of this Privacy Notice is to define the data protection and management principles applied by VirPAY Payment Service Provider Ltd. (hereinafter referred to as "the Company"), the Company's data protection and processing policy which the Company as data controller to be bound by the agreement.

When creating the provisions of the Notice, the Company has taken into account the current legislation on data protection, with particular reference to:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR)
- Act CXII of 2011 on information self-determination and freedom of information (hereinafter referred to as „Information Act")
- Act V of 2013 on the Civil Code (hereinafter referred to as „Civil Code")
- Act C of 2000 on accounting (hereinafter referred to as „Accounting Act.")
- Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter referred to as „Anti-Money Laundering Act")
- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprise (hereinafter referred to as „Bank Act")
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Adverising Activities (hereinafter referred to as „Advertising Act")

The scope of this Privacy Notice extends to all personal data processed by the Company.

Unless otherwise stated, the scope of this Policy does not extend to the services and data processing associated with the personal promotions, services and contents placed online by third parties publishing on the Company's websites or appearing there in any other way.

The Company reserves the right to change this Notice at any time unilaterally and to inform the Users about the change on its website.

The Company is committed to protect the privacy of Users and Customers, considers exceptional importance to respect the right of its Customers to informational self-determination, keeps confidential their personal data and it takes all security, technical and organizational measures to guarantee the security of the data.

The Company's activity meets the requirements of the ISO27001 standard, defining information security management systems.

2. Terms and definitions

Data Processing: whatever method is used, any operation or set of operations performed upon Personal Data; in particular collection, recording, organization, structuring, storage, transformation, alteration, use, query, consultation, communication, disclosure by transmittion, dissemination or otherwise making available, publication, alignment or combination (including profiling), restriction, erasure, destruction.

Data Controller: a person defined in point 3 who determines the purposes and means of Data Processing alone or jointly.

Personal Data or Data: any data or information that allows a natural person User to be identified - directly or indirectly.

Data Processor: a service provider which processes personal data on behalf of the Data Controller.

User: a natural person who registers or requests information on all of the Company's websites as a customer, or visits any of these websites, or concludes a contract with the Company to provide services, and provides the information listed in points 8 and 9 below.

Customer: a natural person who has entered into contractual relationship with the Company, or calls for an offer in this matter.

External Service Provider: third party Service Providers, used by the Data Controller or Website Service Provider for the provision of certain services directly or indirectly, to which the Personal data are disclosed or may be disclosed by transmission, or they may transfer Personal data to the Data Controller.

Furthermore, those service providers are also considered as External Service Providers which are not in cooperation neither with Data Controller nor with operators of services, but by having access to the Website, they collect data from the Users which may be capable of identifying the User either in their own or in combination with other data.

In addition, when providing a hosting service, the Data Controller also considers the User to be an External Service Provider for the purposes of data processing activity carried out in the storage space used by him/her.

Notice: This Privacy Notice of the Data Controller

3. Data, contacts and activity of the Data Controller

Name: Virpay Payment Service Provider Ltd.

Company registration number: 08-09-026652

Tax number: 14767728-2-08

Headquarters: 9200 Mosonmagyaróvár, Szent István király utca 49.

Phone number: +36-70-5151511

E-mail: info@virpay.eu

Data protection officer: Tamás Vizi

Position of the data protection officer: executive director

The Data Controller is a registered incorporation, operates as one of the first bank-independent account management institutions of Hungary and, furthermore deals with the sale of vignettes for Hungarian motorways, service and installation of POS terminals, and building collateral managament.

4. Principles and methods of data processing, applicable law

4.1. The Data Controller acts in the data processing in accordance with the requirements of good faith, fair dealing, and transparency, in cooperation with the Users. The Data Controller processes only the data defined by the law or provided by the Users, for the purposes specified below. The scope of the processed Personal Data is proportionate to the purpose of data processing and can not be expanded.

4.2. Data processing of the Company's activity is based on the following legal basis:

a) **voluntary consents** (Article 6 paragraph 1, point a. of the GDPR):

In case of data processing based on a voluntary consent, the data subjects may withdraw their consent at any stage in the processing of data. In some cases, the processing, storage, disclosure by transmission of a particular set of data is mandatory by law, from which the Users and the Customers are specifically informed by the Company.

b) **performance of a contract** (Article 6 paragraph 1, point b. of the GDPR):

In that case if the data processing is necessary for the performance of a contract to which the data subject is party.

c) **fulfillment of legal obligations** (Article 6 paragraph 1, point c. of the GDPR)

If data processing is necessary for compliance with a legal obligation to which the data controller is subject, it falls within the scope of fulfillment of legal obligations (eg. fulfillment of accounting obligations, etc.)

d) **legitimate interest** (Article 6 paragraph 1, point d. of the GDPR)

Data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

e) in accordance with the Data processing permission provided by Act CVIII of 2001 on certain issues of electronic commerce activities and information society services [13./A §], Users' personal identification data ((name, birth name, mother's birth name, place and date of birth) and address for the purpose of establishment of a contract for providing information society service, definition of its content, modification, monitoring progress in establishment, invoicing the fees as per the contract and recovery of claims related to the contract can be processed without the consent of the User, furthermore, Users' personal identification data, address and data related to the date, time and place of a service as per the contract on information society service can be processed without the consent of the User for the purpose of invoicing fees as per the the contract on information society service.

4.3. In all cases where the Personal Data is intended to be used by the Data Controller for purposes other than those for which they have been entered, User shall be informed and his/her prior express consent shall be obtained, and he/she shall be provided by the opportunity to prohibit the usage.

4.4. The Data Controller does not control the Personal Data entered on its Web pages. Only the person who entered the Personal Data will be responsible for the compliance of the provided Personal Data.

4.5. The personal data of an individual below age of 16 can only be processed with the contribution of an adult having parental care over him/her. The Data Controller is not in a position to control the rights of the contributing person or the content of his / her declaration on its website, thus the User or the person having parental care over him/her guarantees that the consent is in accordance with the law. In the absence of declaration of consent, the Data Controller shall not collect personal data related to an individual below the age of 16.

4.6. The Data Controller shall not disclose the Personal Data processed by it to third parties except for the Data Processors specified in this Notice and in certain cases for External Service Providers referred to in this Notice.

The use of the data in a statistically aggregated form is an exception to the provision stated in this point which shall not include any personal data capable of identifying the User, thereby it is not counted as a processing or transfer of data.

In certain cases, the Data Controller shall make the personal data of the User accessible to third parties due to official court or police inquiries, legal proceedings, copyright, property or other infringement, or their suspect fraud, violation of interest to the data controller, prejudice of providing service, etc.

The Data Processors listed in this Privacy Notice and the External Service Providers shall record, maintain and process personal data transmitted by the Data Controller and maintained or processed by them in accordance with the provisions of the GDPR and they shall make a declaration on this to the Data Controller following the date of 25th of May, 2018.

4.7. The Data Controller informs the concerned User about the rectification, restriction and erasure of Personal Data, furthermore it informs all those individuals which the personal data were transferred to previously for the purpose of data processing. The notification may be omitted if it does not prejudice the legitimate interest of the User with the objective pursued by Data Processing.

4.8. Having regard to the provisions of the GDPR, the Data Controller is not obliged to designate a Data Protection Officer, as the Data Controller is not considered to be a public authority or a public law body service entity. Furthermore the data processing activities do not include any operations that require regular, systematic and high level of observation of Users, furthermore the Data Controller does not process specific data, or personal data related to decisions on criminal liability and to crime.

4.9. The Data Controller processes the personal data in accordance with the applicable law. Legislations governing data processing is especifically defined at point 1.

5. Data Processing

5.1. Payment service provider activity

The payment service provider business of the Company offers online account management service through VIRPAY Netbank service, after the personal conclusion of the contract.

5.1.1. websites www.virpay.eu, netbank.virpay.eu, www.virpaygroup.com

The purpose of the data processing: notification about conclusion of a contract in order to provide payment service, making an appointment, differentiation between customers, performance of the contract for payment service activity between the Data Controller and the Customer, provision of a contracted service, enforcement and recovery of possible claims in relation to the contract, statistical analysis, construction of analytical models, profiling, tracking of the services used

The legal basis of the data processing: voluntary consent of the data subject, performance of the contract

The scope of data processed: name, phone number, e-mail address. In the case of an application for netbank service, the customer's name, username, password, order codes, User's name, identifier, phone number, e-mail address, date, signature, IP address.

The deadline for deletion of the data: 3 months from the date of deletion of the data by the User on the websites www.virpay.eu, www.virpaygroup.com, 8 years from the date of closure of the contract including all data in accordance with the Accounting Act 169.§ (2)

Data Transfers: personal and contractual information to the Data Processors listed in 161-164. §§ of the Bank Act

The legal basis for the transfer of data: 161-164.§§ of the Bank Act

Data Processor: T-Systems Hungary Zrt. (1117 Budapest, Budafoki út 56.)

Possible consequences of failure to provide data: failure to contact and to provide information, furthermore the failure to provide payment services

5.1.2. Due diligence of a customer

The Company identifies the Customer appearing at its headquarters in order to sign a contract and to mandate for account operation based on his / her personal documents in accordance with Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing. makes a copy of his / her documents and keeps them for records until the mandatory deadline as stated in the law. The Anti-Money Laundering Policy of the Company is available at www.virpay.eu.

The purpose of data processing: identification of the Customer for conclusion of a contract in order to provide payment service, to fulfill the tasks in order to prevent and to combat money laundering and terrorist financing

The legal basis for data processing: performance of legal obligation in accordance with Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter referred to as "**Anti-Money Laundering Act**"). and Act LII of 2017 on the

implementation of financial and property restrictive measures (hereinafter as 'Kit.') ordered by the European Union and the UN Security Council.

The scope of processed data: family and first name, birth name (family and first name), nationality, place of birth, date of birth, permanent address, or temporary address in the absence,

The deadline for deletion of the data: 8 years after the date of data recording, notification or suspension

Data tranfers: based on requests from MNB, FIU, prosecutor's office, or court in order to initiate administrative proceedings

The legal basis for the transfer of data: Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing

Possible consequences of failure to provide data: failure of contracting

5.1.3. Recording of phone conversations

The Company shall record both incoming and outgoing telephone conversations on the telephone number **+36 70 51 51 511** from the date of 1 July 2018, on which phone number queries about payment service provider activity and installation of POS terminals can be administered. The administration concerning the Company's business on the sale of vignettes for Hungarian motorways is possible on the phone number **+36 30 30 36 608** and the conversations made here are also recorded.

The purpose of the data processing: fulfilment of customers' and Data Controller's rights, provision of evidence for possible disputes, provision of ex-post evidence and provision of possible non-recovery of the claim, and the ex-post proof of the agreements, quality assurance, compliance with legal obligations, complaint handling.

The legal basis for data processing: the voluntary consent of the data subject, in case of complaint in accordance with Bank Act 288.§ (2)

The scope of data processed: identification number, dialing number, dialed number, date and time of the call, phonogram of the telephone conversation, and other personal data provided during the conversation

The deadline for deletion of data: 5 years in case of complaint related to the payment services activity in accordance with Bank Act 288.§ (2), 60 days in case of administration related to the payment services activity in accordance with Act CXXXIII of 2005, 31 § (4), 30 days in case of queries about vignettes for Hungarian motorways in accordance with Act CXXXIII of 2005, 31 § (3)

Possible consequences of failure to provide data: failure of administration through the phone, the need for personal administration

Data Processor: Vodafone Magyarország Zrt., headquarters: 1096 Budapest, Lechner Ödön fasor 6.

5.1.4. Cookie handling on websites www.virpay.eu, www.virpaygroup.com, www.virpay.hu, palya-matrica.hu, vignetteungarn.eu, vignettehungary.com, vignetaungaria.ro, kartyas-fizetes.hu, epitoipari-fedezetkezeles.hu

In order to serve the Users fully, the Company applies the so -called anonymous User IDs located on the computers of the Users which are in contact with the Company.

Anonymous User ID (cookie) is a sequence of characters which can be used for unique identification or storage of profile information and located on the User's computer by the service providers.

It is important to know that such a sequence of characters is not capable of identifying the User in its own, it only recognizes the User's computer. Person related information and customized service in the world of the Internet can only be provided if the service providers can uniquely identify their customers' habits and needs. Service providers turn to the anonym identification on one hand to learn more about habits of customer, related to information usage in order to improve the quality of their services, further, and on the other hand, to offer options for customization to their customers.

As an example, the User’s preferences and settings can be stored with the help of cookies; these will help the User to sign in; to display personalized ads and to analize the operation of the web site. In order to do this, the Company uses services to collect and track data such as relevance, sponsor, search results, openings, and the most important and most commonly used features.

Flash cookies are used to tell us, for instance, whether the user has ever visited our website or they help to identify the features / services that may be of interest to the User.

Search and Flash cookies increase the online experience by retaining the information preferred by the User while visiting a particular site.

Neither the search engine nor the Flash cookies can personally identify the User, and he/she can disable browser cookies through browser settings, but he shall not be able to take an advantage of all the features of the website without such cookies.

If the User does not want this type of ID to be located on his/her computer, he/she can configure his/her browser to not allow the location of the unique identifier. But in this case, the User may not have access to the Services, or he/she shall not access to them in a way as if he/she has have allowed to locate the IDs.

The Services are used by a large number of Users in a variety of software and hardware environments for different purposes and areas. The development of Services can be tailored to the needs and opportunities of Users in the best way if we get an overall picture of the habits and needs of their use. However, due to the large number of Users, along with the personal request and feedback, it is an effective complementary method to collect and analyze their habits and the data related to the running environment of the Services through automated methods.

The Company's web pages use the web analytical service of Google Analytics (hereinafter referred as Google Analytics) provided by Google, Inc. (headquarters: 1600 Amphitheater Parkway Mountain View CA 94043) (hereinafter referred as "Google"). Google Analytics also uses text files located on User's computer (cookies) in order to help to analyze the use of the Site.

The Data Controller informs the User and the User explicitly agrees upon acceptence of the contract that Google transfers the data generated by cookies, and related to the usage of web pages (including the User's IP address) to its servers located in the USA, and stores them there.

By using the Websites, the User agrees to transfer his/her data in a manner and for the purposes specified above.

Google uses this information to evaluate and analyze the use of the Websites by the User, to compile reports about the activities on the Website and to provide other services associated with the activities on the website and the usage of the Internet.

Google is responsible for the legality, damages and claims related to the data transfer and processing described above. If the User has any questions or concerns regarding the above, he/she can contact us via e-mail as specified in point 3 of this Privacy Notice.

The Data Controller may also use tracking IDs in its newsletters or for other services, for the purpose of developing and tracking the User's habits:

Google Adsense,

Google Co-op (search),

Adverticum,

Gemius,

Median Webaudit,

OpenX,

Facebook (likebox, share),

Addthis.com (share),

Apple Inc. (meta tag).

The purpose of data processing: to identify Users, to differentiate between Users, to identify the current session of Users, to store data provided in the course of this session, to prevent data loss, to identify and track Users, web analytical measurements.

The legal basis for data processing: consent of the data subject.

The scope of processed data: identification number (IP address), date, time, and the website visited previously.

The duration of data processing: 30 minutes

The cookies can be deleted from the User's computer by the User, or they can be disabled in his/her browser. Cookies can usually be managed at browser menu Tools/Preferences, under Privacy / History / Custom Settings, with name cookie or tracking.

Possible consequences of failure to provide data: limited access to the services of the website, inaccuracy of analytical measurements.

5.1.5. Electronic monitoring system

The Company operates a monitoring and recording system at its headquarters, in the VirPAY Financial Point area, including infrared color-captured cameras, capable of zooming, providing images recognizable in the dark. Cameras are aimed at Customers, employees and entrants in the Financial Point and in the ATM Room

The controller of personal data: The Company has agreed on outsourcing with PATENT Remote Assurance Ltd. (headquarters: 9200 Mosonmagyaróvár, Szent István király út 49).

The purpose of the data processing: to operate an electronic monitoring and recording system for the purpose of safeguarding property, preventing and detecting possible criminal offenses

The legal basis for data processing: In case of customers, the consent of the data subject by entering into the territory of the Company, in case of employees in accordance with Act I of 2012, 11.§ (Labor Code)

The scope of processed data: The facial image appearing on the picture record of the person entering into the Company's area and his/her other personal data recorded by the monitoring system.

The duration of the data processing: up to sixty days in the absence of use in accordance with Personal and Property Protection Act 31.§ (4) point a.

Information on storing data: records are stored on the servers located at the headquarters of. PATENT Távfelügyelet Kft., with enhanced data security measures, ensuring that unauthorized persons are not allowed to view and copy the records.

Access to Images: Only the designated employee of PATENT Távfelügyelet Kft.has a right to view the current image of the cameras in order to accomplish the data processing objectives specified in this notice.

Only the designated employee of PATENT Távfelügyelet Kft. has a right to view the camera records and to store them on a backup system, in order to accomplish the data processing objectives specified in this notice.

Loggings: PATENT Távfelügyelet Kft. records in the minutes the accesses to the records, the savings on the backup system, the name of the person carrying out them, the reason, date and time of access to the data.

Possible consequences of failure to provide data: Failure of personal administration at the Financial Point.

Data subject whose right or legitimate interest is affected by the recording, may request the Data Controller with a proof of his/her right and legitimate interest not to destroy or delete the record until the request is received from the court or authority, but up to 30 days.

Furthermore, the person appearing on the record may also request the Data controller to inform him/her in written about what is visible on the record. The person in subject may get a copy only of that record on which there is no other person or, if there is, then he/she is unrecognizable. If the above requirements are not met, the Data controller will provide the data subject with the opportunity to see the record of him/her.

5.1.6. Customer correspondence of VirPAY Kft.

If you would like to contact our Company, you can contact the Data controller using the contact details provided in this notice or on the website.

The Company shall delete all emails received with the sender's name, e-mail address, date, time and other personal data provided in the message, up to five years after the date of providing the data.

The legal basis of data processing: voluntary consent or performance of the contract.

5.2 Sale of vignettes for Hungarian motorways

The Company publishes information about itself and vignettes for Hungarian motorways, and sends out newsletters on web sites palya-matrica.hu, vignetteungarn.eu, vignettehungary.com and vignetaungaria.eu, furthermore it sells electronic vignettes for Hungarian motorways at www.virpay.hu on which the customer can on-line purchase the vignettes for Hungarian motorways.

The purpose of the data processing: to contact and inform the prospective buyers, furtermore to sell and to record a purchase, and billing information

The legal basis for data processing: voluntary consent and performance of the contract, as well as the Accounting Act.

The scope of processed data: name, phone number and e-mail address in relation to web sites palya-matrica.hu, vignetteungarn.eu, vignettehungary.com and vignetaungaria.ro in case of registration on www.virpay.hu: e-mail address, password, registration type private / corporate, phone number, e-invoice request, name, country, postcode, town, name and type of public space, house number, door,

in case of purchase: type of vignette, flag of registration number / country, registration number, start date of validity, invoice e-mail, name, tax number, country, postcode, town, name and type of public space, house number, floor, door

The deadline for deletion of data: 5 years from the date of registration if there was no purchase within 5 years from the date of registration, and 8 years following the purchase, from the date of issuing the invoice in accordance with the Accounting Act 169.§ (2).

Possible consequences of failure to provide data: failure of contact and performance of the contract

5.3. Installation and operation of POS terminals

The Company provides information to those who are interested on its activities of POS terminal installation on its website www.kartyas-fizetes.hu In order to contact personally, a proposal form can be filled out through the web site. The Company processes personal data on the proposal form in order to contact the person requesting for a proposal.

The purpose of the data processing: to contact and inform the prospective buyers

Legal basis for data processing: voluntary consent

The scope of processed data: family name, first name, company name, phone number, e-mail address, website, message

The deadline for deletion of the data: 1 year from the request for proposal

Possible consequences of failure to provide data: failure of contact and performance of a contract

5.4. Building Collateral Management

The Company provides information to those who are interested on its activities of Building Collateral Management on its website www.epitoipari-fedezetkezeles.hu. In order to contact personally, a proposal form can be filled out through the web site. The Company processes personal data on the proposal form in order to contact the person requesting for a proposal.

The purpose of the data processing: to contact and inform the prospective customer.

Legal basis for data processing: voluntary consent

The scope of processed data: name, e-mail

The deadline for deletion of the data: 1 year from the request for proposal

Possible consequences of failure to provide data: failure of contact and performance of the contract

5.5 Other

The Company provides information on the data processing which is not listed in this Notice when the data is provided.

The Company informs its Users and Customers that the court, the public prosecutor, the investigating authority, the infringement authority, the administrative authority, the Hungarian National Authority for Data Protection and Freedom of Information

the Central Bank of Hungary, and other bodies based on a legal basis (hereinafter referred to as authorities) may contact the Data Controller for information, disclosure and transfer of data and submission of documents.

Furthermore, the Company informs the Users and Customers that the data processed by it may be transferred to the competent persons dealing with data processing, billing, accounting, handling of claims, delivery, customer service mandated by the Company, and to other competent bodies for the settlement of disputes based on a legal basis. The above listed recipients of personal data provide services to the Company and locally operate mainly in Hungary or in the European Economic Area. These persons act according to the instructions of the Company, they are not allowed to use the data for any other purpose, and they are bound by the obligations of confidentiality and data protection.

The Company provides the Authority with personal data only in a measure which is crucial to achieve the objectives of the request and only if the Authority indicated the proper aim and the scope of necessary data.

The Company informs Users that the so called cloud computing applications are also part of the services. Cloud applications are typically international or trans-border in nature and, for

instance are used for data storage when the User's computer / corporate computing center is not a data storage medium, but a server center that can be located anywhere in the world. The main advantage of cloud applications is that they provide highly secure and flexible storage and processing capacity which is essentially irrespective of geographic location.

The Company selects its cloud computing partners with the greatest possible care, makes every effort to perform a contract with respect to the data security interests of the Users, their data processing principles shall be transparent and they shall check the data security on a regular basis.

6. Method of storage of personal data and security of data processing

The computing systems and other data retention centers of the Company are located at its headquarters and at the premises of its data processors.

The Company selects and manages the IT tools used to process personal data in a way so that the data processed:

a) shall be accessible to the authorized persons (availability);

b) their authenticity and authentication shall be provided (authenticity of data processing);

c) their unchangingness is verifyable (data integrity);

d) shall be protected against unauthorized access (confidentiality of data).

The Company protects the data through appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or annulment, as well as unavailability due to accidental annulment, damage, and change of the technique used.

In order to protect files managed in its various records electronically, the Company ensures with a help of an appropriate technical solution that the data stored - unless permitted by law - can not be directly linked and assigned to the data subject.

Given the current state of the art technology, the Company protects the security of data processing with technical, and organizational measures ensuring an adequate level of protection against the risks associated with data processing.

In the course of data processing, the Company retains:

a) confidentiality: it protects the information so that it can only be accessable to the person who is authorized to it;

b) integrity: it protects the accuracy and completeness of the information and the method of processing;

c) availability: ensures that when the eligible user needs it, he / she can really access to the requested information, and the tools associated with it are available.

The IT system and network of the Company and its partners are protected against computer-aided fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer hackings, and denial of service attacks. The operator ensures the security with systemic and application-level security procedures.

The Company informs the Users and Customers that electronic messages forwarded via internet, irrespectively of protocols (email, web, ftp, etc.) are vulnerable to network threats that lead to fraudulent activity, disputation of contract, disclosure or modificiation of information.

In order to protect from such threats, the Data Controller shall take all the necessary precautions which can be expected from it. Systems are monitored by the Data Controller in order to record all security derogations and to provide evidence of any security incident. System monitoring also allows to check the effectiveness of the safeguards applied.

7. Rights of the data subjects

The data subject shall request information about processing of his/her personal data, and he/she shall ask to rectify his/her personal data. Except for mandatory data processing, he/she shall ask to cancel or withdraw his/her personal data, he/she shall utilise his/her right to discretion and right to object as indicated in the data entry, or using the above mentioned contact details of the Data Controller.

7.1. Right to information

The Company shall take appropriate measures to ensure that all the information relating to the processing of personal data as referred in Article 13 and 14, Articles 15-22 and 34 of the GDPR is provided to the data subjects in a concise, transparent, comprehensible and easily accessible form, and in a clear and unambiguous manner.

The right to information can be exercised in writing through the contact details indicated in point 3. At the request of the data subject, information may be given verbally, after his/her identity has been established.

7.2. Right to access by the data subject

The data subject shall have the right to obtain from the data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

the purposes of the data processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; the envisaged period for which the personal data will be stored, the right to rectification, erasure or restriction of data processing and the right to object; the right to lodge a complaint with a supervisory authority; information on data sources;

the existence of automated decision-making, including profiling, and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

The Company shall provide the data subject with a copy of the personal data subject to data processing. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on the administrative cost. At the request of the data subject, the information is provided by the Company in electronic form.

The Data Controller shall provide the information within 30 days following the submission of the application.

7.3. Right to rectification

The data subject shall have the right to obtain from the Data Controller the rectification of inaccurate personal data and the completion of incomplete personal data concerning him/her.

7.4. Right to erasure

The Data Controller shall have the obligation to erase personal data of data subject as per his/her request without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed

- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;

- 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;

- the personal data have been collected in relation to the offer of information society services.

Erasure of data can not be initiated if data processing is required: for exercising the right to freedom of expression and information; for compliance with a legal obligation which requires processing by Union or Member State law to which the data controller is subject or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the data controller; for reasons of public interest in the area of public health, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,or for the establishment, exercise or defence of legal claims.

7.5. Right to Restriction of Data Processing

The data subject shall have the right to obtain from the data controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the personal data;

- the data processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

- the data subject has objected to data processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent 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.

A data subject who has obtained restriction of processing shall be informed by the data controller before the restriction of processing is lifted.

7.6. Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the data controller, in a structured, commonly used and machine-readable format and to transmit those data to another data controller.

7.7. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, including profiling based on those provisions. The data controller shall no longer process the personal data unless the data controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

7.8. Automated individual decision-making, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The above right shall not apply if the decision:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;

- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

- is based on the data subject's explicit consent.

7.9. Right to revocation

The person subject has the right to revoke his consent at any time. Revocation of the contribution does not affect the lawfulness of the consent based on consent, prior to the revocation.

8. Legal remedies

8.1. Procedural rules

The data controller shall inform the data subject without undue delay, but in any case within one month from the receipt of the request, based on the request in accordance with GDPR Articles 15-22.

If necessary, taking into account the complexity and number of requests, this deadline may be extended by two additional months.

The data controller shall inform the data subject about the extension of the deadline by defining the reasons for the delay within one month of the receipt of the request. If the data subject provided the request electronically, the information shall also be provided electronically, unless otherwise requested by the data subject.

If the data controller fails to take measures following the request of data subject, it shall inform the data subject without delay and within one month of the receipt of the request about the reasons of non-action and whether the data subject may file a complaint with a supervisory authority and exercise his/her right to judicial remedy.

The Company provides the requested information free of charge. If the request of data subject is clearly unjustified or - in particular due to its repeated nature excessive, the data controller may charge a reasonable fee for administrative cost regarding the provision of the requested information, or the adoption of necessary measures, or may refuse the measure based on the request.

The data controller shall communicate any rectification, 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 controller shall inform the data subject about those recipients if the data subject requests it.

The data controller shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

8.2 Compensation for damages suffered

Any person who has suffered material or non-material damage as a result of an infringement of the data protection regulation shall have the right to receive compensation from the data controller or data processor for the damage suffered.

A data processor shall be liable for the damage caused by data processing only where it has not complied with obligations of data protection regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the data controller.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each data controller or data processor shall be held liable for the entire damage.

A data controller or data processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

8.3 Complaint

If you have a problem with the data processing of the Company, please contact the Data Protection Officer of the Company whose contact information can be found in point 3.

The data subject has a right to lodge a complaint about the conduct, activity or omission of the Company:

a) Verbally

- personally, **during opening hours**. The place of complaint handling is the headquarters of the Company, namely 9200 Mosonmagyaróvár, Szent István király út 49. lph 1, **opening hours on working days Monday 8:00 - 18:00, Tuesday, Wednesday and Thursday: 8:00 - 16:00, Friday 8:00 - 15:00.**

or

- by phone at **+36 70 51 51 511** and during the following opening hours: **Monday 8:00 - 18:00, Tuesday, Wednesday and Thursday: 8:00 - 16:00, Friday 8:00 - 15:00,**

b) In written

- personally or via delivery of the documenty by another person at the headquarters of the Company;
- By post using the postal address 9200 Mosonmagyaróvár, Szent István király út 49. A lph 1.
- via fax at +36-96-950-928;
- by e-mail (providing continous electronic access and an alternative availability for the case of malfunctions) at e-mail address: **panaszkezeles@virpay.eu**

In order to handle verbal compaints at its premises open to customers or, in the absence thereof, at it headquarters, the Company is obliged to ensure that customers have the possibility to make an appointment for personal administration electronically and via telephone.

The Company is obliged to make an appointment for personal administration with the customer within 5 business days of the date of the personal request of the customer.

The Company shall ensure the receipt and administration in case of complaint handling on the telephone, within a reasonable timeframe.
A proxy may act on behalf of the customer. If a proxy acts on behalf of the customer, the authorization shall be entered in a public document or in a private document of complete probative value.

The Company shall request the following personal information from the customer during the complaint handling

a) name;
b) contract number, customer number, payment account number (cashier identification nuber)
c) permanent address, headquarter, mailing address;
d) phone number;
e) the manner of notification
which is based on the legal obligation.

The records of complaints and the measures taken for their resolution shall be retained for five years and shall be presented only at the request of MNB acting solely as the supervisor of the financial intermediaries (unless otherwise provided in the law).

The operative Complaint Handling Policy of the Company is available at www.virpay.eu

8.4. Right of access to Court

In the event of violation of his/her rights, the data subject shall go to the law against the Data Controller in accordance with Information Act 22.§ (1). The trial is governed by the jurisdiction of the courthouse. The court proceeds out of turn. The case shall be run before the courthouse of domicile or temporary address of the data subject, at the choice of him/her.

8.5. Privacy Policy Procedures

A complaint can be lodged with the Hungarian National Authority for Data Protection and Freedom of Information:

Nemzeti Adatvédelmi és Információszabadság Hatóság

1125 Budapest, Szilágyi Erzsébet fasor 22/C

Tel: 06-1-391-1400

E-mail: ugyfelszolgalat@naih.hu