PRIVACY POLICY

I The Controller's data

company name: registered sate: company registration number: tax number: e-mail: website: telephone number/fax:	**MOMART 2020 Marketing Korlátolt Felelősségű Társaság (abbreviated: MOMART 2020 Kft.)** 1117 Budapest, Budafoki út 187-189. 25182730-2-43, 01-09-204613 (Municipal Court as Registry Court) momartkft@momart.hu http://momart.hu +36 1 7816843

MOMART 2020 Marketing Kft. (hereinafter as: MOMART, Controller, and in Chapter V as: Processor) is a marketing agency involved in event hosting and conducting telemarketing campaigns. The present policy extends to the data processing related to the activities of MOMART as well as the website located at the http://momart.hu address (hereinafter as: website).

The Controller is committed to ensuring that the data processing procedures adhere to the general data protection regulation (hereinafter as: Regulation or GDPR)[1], the Info Act[2], as well as the provisions of other relevant acts.

Only the employees of the Controller are authorized to access personal data and perform processing for the extent and designated purpose of the individual processing. The individuals involved in the processing are bound by an obligation of confidentiality.

The Controller may be approached by the courts, investigative authorities, authorities dealing with administrative offences, administrative authorities, the Hungarian National Authority for Data Protection and Freedom of Information or other bodies empowered by legal instruments to provide information, state or deliver data and render documents. MOMART shall provide personal data to the authorities – when the precise purpose and range of said data is stated by the authorities – only to the extent that and for such period as is strictly necessary for the realisation of the purpose of the request in question.

Should you have questions and comments on the processing, you may contact the Controller at the contact information listed above.

II Basic definitions:[3]

For the sake of the interpretation of the terms used in the present policy, the following definitions shall be used pursuant to the Regulation:
"personal data": any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
'processing': any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"controller": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
'processor': a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council, also known as GDPR
2 Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter referred to as Info Act)
3 Further definitions are listed in Article 4 of the GDPR.

III Possible legal grounds for data processing

The Regulation recognises six separate legal bases:

- the data subject's consent [item a) paragraph (1) Article 6 of the GDPR],
- performance of a contract [item b) paragraph (1) Article 6 of the GDPR],
- compliance with a legal obligation [item c) paragraph (1) Article 6 of the GDPR],
- protection of vital interests [item d) paragraph (1) Article 6 of the GDPR],
- performance of a task carried out in the public interest [item e) paragraph (1) Article 6 of the GDPR],
- purposes of legitimate interests [item f) paragraph (1) Article 6 of the GDPR],

IV The data processing activities of MOMART (purpose, legal basis, duration, scope of processed data)

Controller shall only process personal data for specified purposes, for performing its main and auxiliary activities, practicing its rights and fulfilling its obligations while the processing shall adhere to the purpose of the processing throughout all stages of the process. The recording and handling of the processing shall take place in a fair and lawful manner. Controller strives to process no personal data that is not indispensible for the fulfilment of the purpose of the processing or which is not suitable for fulfilling said purpose. The processing of personal data shall only be carried out to the necessary extent and duration.

Processing of the data of points of contact

Brief description of the processing
In relation to its activities, when establishing contact with partner companies, principals, commissioners (hereinafter as: Clients), MOMART records various personal data. The contracts concluded with Clients also include the details of points of contact. In other cases, non-contractually, such contact information is provided directly by the data subject (e.g. in form of business cards). The data of individuals identified as points of contact (name, telephone number, e-mail address) only includes information that is necessary for establishing and maintaining contact.
The purpose of processing is to establish and maintain contact, particularly for the sake of the performance of contracts related to the activities of MOMART, as a legitimate purpose of processing.
Legal grounds for processing:
Pursuant to Recital 47 of the Regulation: "*legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.*"
The legal grounds of the processing can be identified as **the legitimate interests of the partner and the Controller pursuant to Article 6, paragraph (1), point f) of the Regulation**. In the case of processing based on legitimate interests, a balancing test is to be carried out, informing the data subjects on the results thereof. Controller has performed the relevant balancing test. The balancing test shows that the legitimate interests of the Controller poses no disproportionate restrictions to the data subject's right to the protection of personal data.
Scope of processed data
Name, e-mail address and telephone number of the point of contact.
Duration of the processing
Until the termination of contractual claims.

Recovery of claims and enforcement in the case of a breach of contract

Brief description of the processing
For the sake of legally enforcing arrears in bills and other claims for the Controller,
external businesses (e.g. attorney's offices) perform claim management tasks based on service contracts.
Legal grounds for processing:
The legal grounds of the processing can be identified as **the performance of contractual obligations pursuant to Article 6, paragraph (1), point b) of the Regulation, or in the case of non-contractual claims (e.g. damages), pursuant to Article 6, paragraph (1), point f) of the Regulation**.
Pursuant to Section 6:137 of the Civil Code, non-performance of a contractual obligation is any failure to perform said obligation. Pursuant to Section 6:138 of the Civil Code, in the event of non-performance, the aggrieved party shall be entitled to require performance of the obligation. In the case of processing based on legitimate interests,

a balancing test is to be carried out, informing the data subjects on the results thereof. Controller has performed the relevant balancing test. The balancing test shows that the legitimate interests of the Controller poses no disproportionate restrictions to the data subject's (debtor's) right to the protection of personal data. Upon request, the Controller shall provide information to the data subject on the contents of the present paragraph.
The purpose of the processing is **to legally enforce arrears in bills and other claims for the Controller**, which is a legitimate purpose of processing.
Based on the contents of the commission in question, it can be decided whether the commissioned claims management company constitutes a processor or an independent Controller.
Scope of processed data
Typically invoice data (name, address, time of purchase) and contact information (telephone number, e-mail address). Other data required for enforcement.
Duration of the processing
Until the recovery of the claims. Until the end of the limitation period as stipulated by law.

Recording images, videos or sound recordings

The recording and publishing of images, video and sound recordings related to the operation of the Controller is in each case tied to consent, with the exception of the appearance of public figures as well as mass recordings, the recording and use of which do not require the data subject's consent.

The use of the recordings is tied to a specific purpose, therefore the Controller shall inform the data subjects that the Controller, as well as their commissioned third parties may use said recordings in materials detailing the activities of the Controller and publish them through their own platforms or in the media in the form of quotes, articles, short film excerpts or images.

Consent can be considered a suitable legal basis of processing if it is based on information provided in a voluntary, specific, unambiguous and suitable manner. The data subject is entitled to withdraw their consent at any time. The withdrawal of consent shall have no bearing on the data processing carried out prior to said withdrawal. The withdrawal of consent must be made possible to be carried out as simply as providing consent.

Processing related to the visitors of the http://momart.hu website and the use of cookies

An electronic cookie is a small bundle of data that the browser saves to the device at the request of various websites (web servers). Websites use such cookies to store temporary, yet vital information that is to be retained, including your personal settings and these are used to identify the user, monitor browsing habits and track whether you have previously visited the website.
Most browsers accept cookies by default. However, the downloading of cookies can be turned off and there is an option to adjust these settings in the browser in order to be notified before such cookies are downloaded to your device. These settings are solely for the browser and device in question, therefore cookies settings must be adjusted or turned off separately per device and browser.

Our website does not use cookies that allow you to be identified; our only goal is to ensure the appropriate operation of the website and recording statistical data related to website usage. The independent measuring of the website's traffic and other web analytics data is performed by Google. More information on the processing of measurement data is available through the www.google.com/analytics/ website.

You can also delete cookies from your own device or adjust the settings of your browser at any time in order to block the use of cookies.
Through the website for turning off advertisements displayed by Google (https://policies.google.com/technologies/ads?hl=hu), Google allows users to block the cookies used by Google. However, blocking cookies can make using the website more inconvenient for you. By blocking cookies on the website, it's possible that you will be unable to access certain parts of the website and some functions of the website will not function as expected.

V Employment of processors on behalf of MOMART

During its activities as an independent controller, MOMART employs processors in certain cases. Processors record, handle and process the personal data transmitted to them or processed by the Controller pursuant to the Regulation.
The contractually employed external processors of MOMART only provide technological solutions for MOMART that are required for the processing of data. In relation to the personal data stored or handled through the information technology systems that they manage or monitor, they shall carry out no processing of data on their own. They shall not use personal data stored in the information technology systems for their own purposes or those of any third parties and shall not disclose such information.

The Controller's list of processors		
Name of processor	Tied to which of the Controller's processing activities	Processor's task, brief description of the processing
Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Ireland Tax number: IE8256796U	e-mail system, exchange server	IT service provider
EVOLUTIONET KFT. 7342 Mágocs, Széchenyi utca 75. Tax number: 14992511-2-02	website data	hosting provider
Adeco Számviteli és Adótanácsadó Kft. 1171 Budapest, Függőcinege u. 2. Fsz. 3. ajtó Tax number: 12208700-2-42	accounting documents, employer data	accountant
Dropbox International Unlimited Company One Park Place, Floor 6 Hatch Street Upper Dublin 2 Tax number: IE 9852817J	fileserver	cloud service operator

VI MOMART as Processor

In the course of the marketing-agency (mainly event hosting and telemarketing) tasks performed for its clients, MOMART shall act as a processor based on the data processing agreements concluded with clients as controllers.

The basic rules of MOMART's activities as processor include:

- the controller (the client) is responsible for the legality of data processing instructions issued to the processor,
- the processor is responsible for the processing, alteration, erasure, forwarding and publishing of personal data within its scope of activities as well as within the limits designated by the controller (the client),
- during its activities, the processor may not employ the services of additional processors without the advance written permission of the controller (the client),
- processor can make no substantial decisions related to the processing and may only process the obtained personal data according to the provisions of the controller (the client) and may carry out no processing for its own purposes; furthermore, it is required to store and keep the personal data according to the provisions of the controller (the client),
- processor shall report all privacy incidents without undue delay to the controller (the client) once it has become aware of said incident,
- the forwarding of data and the connection of databases processed by the controller (the client) with other clients can only take place with the data subject's consent or when authorised by a legislative instrument,
- the controller (the client) shall only forward personal data with an unambiguous legal basis and purpose, when the recipient of the forwarding has been specified
- subsequent to concluding the data processing service, at the discretion of the controller (the Client), the processor shall erase all personal data or return said data to the controller,
- in light of the nature of the processing, the processor shall employ adequate technical and organizational measures, as well as security measures.

VII Forwarding data to third countries

MOMART does not forward personal data to countries outside the European Union.
Personal data can only be forwarded to so-called third countries outside of the European Union by the Controller by ensuring the protection of the data required within the EU pursuant to the Regulation, while observing the Regulation's provisions on forwarding personal data.

VIII Data subjects' rights

Pursuant to the wording of the Regulation, a **"data subject"** is a natural person who can be identified, directly or indirectly, in particular by reference to the information or personal data related to them.
Data subjects are entitled to the rights listed below.
Prior to the request of enforcement actions, the Controller is obliged to identify the person submitting the request.
Insofar as the Controller has reasonable doubts about the identity of the natural person, they may request further information for the sake of identification.

IX Data subjects' processing-related rights

Right of information and access
The data subject shall have the right to obtain information from the controller on the processing of their personal data and the validation of their rights. Should you have such requests, we kindly ask you to contact the Controller in writing (e-mail).
Pursuant to the present Privacy Policy, the Controller shall provide the requested information in writing. The Controller may refuse requests by proving that it is unable to identify the data subject.
At the data subject's request, the Controller shall provide them with a copy of the personal data in question. Insofar as the data subject submitted their request electronically or if the processing of the personal data takes place electronically.

Controller shall respond to the data subject's request without undue delay yet no later than within 30 days and must justify any failures to fulfil said requests.
Requests for copies of the personal data are basically fulfilled free of charge. Controller may charge a reasonable fee for administrative costs in the case of requests for more than one copy or if there would be a cheaper, faster, more cost-effective way to fulfil the requests for data than the manner specified in the request for data.
Insofar as the Controller is engaged in the processing of the data of the data subject, the data subject is entitled to access to the personal data as well as the following information: the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed; the envisaged period for which the personal data will be stored, or if not possible, the criteria used to determine that period; where the personal data are not collected from the data subject, any available information as to their source; the existence of automated decision-making, including profiling.[4] Furthermore, the data subject is entitled to receive information on the right to lodge a complaint with a supervisory authority and that they may request the rectification, erasure or restricted processing of their personal data and may object against the processing of such personal data.[5]

Right to rectification

The data subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning them. Such requests require verifying the accurate data via official documents.
Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed. This includes completion by means of providing a supplementary statement.

Right to erasure ("right to be forgotten")

Pursuant to the Regulation, the data subject shall have the right to obtain from the Controller the erasure of personal data concerning them without undue 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; b) the data subject withdraws consent on which the processing was based and where there is no other legal ground for the processing; c) the data subject objects to the processing pursuant to the relevant provision of the Regulation and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing as this took place through direct marketing (including profiling);
d) the personal data has been unlawfully processed;
e) the personal data must be erased for compliance with a legal obligation in European Union or Member State law;
f) the personal data has been collected in relation to offering information society services directly to minors.

Controller may deny the erasure of data insofar as the processing is necessary for one of the following reasons:
a) when exercising basic rights (to exercise the right of freedom of expression and information);
b) in the case of obligatory processing (the personal data must be processed for compliance with a legal obligation in European Union or Member State);
d) in public interest (e.g. for the sake of public archiving, scientific research, historical research, or statistical purposes and where erasure of the data would likely to impair or halt progress towards the achievement that was the goal of the processing); or
e) for the establishment of a legal defence or in the exercise of other legal claims.

The right to erasure cannot lead to the erasure of personal data that was provided by the data subject for the performance of employment-related agreements insofar as to the extent that said personal data is required for the performance of the agreement in question.
Furthermore, the right to erasure cannot be applied when the duration of processing is determined by law.

Insofar as the Controller has forwarded the personal data in question to other recipients and is obliged to erase the personal data, in due consideration of the available technology and the costs of implementation, the Controller shall take reasonable steps, including technical measures to inform Controllers which are processing the personal data to erase said personal data. In such cases, the same rules on exceptions shall be applied.

4 During its activities, the Controller does not make use of automated decision-making or profiling pursuant to the Regulation.
5 Pursuant to Article 15 of the Regulation

Right to restriction of processing

Pursuant to the Regulation, the data subject shall have the right to obtain from the Controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject (in such cases, the restriction is for a period enabling the Controller to verify the accuracy of the personal data);

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

c) the Controller no longer requires 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

d) pursuant to the relevant provisions of the Regulation, the data subject has objected to processing; in such cases, the restriction is for a period 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.

Controller shall inform the data subject (who has obtained restriction of processing) before the restriction of processing is lifted.

Right to data portability

Pursuant to the Regulation, the data subject shall have the right to receive the personal data concerning them, which they have provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit said data to another controller without hindrance from the Controller to which the personal data have been provided, where:

a) the processing is based on consent or on a contractual legal basis; and

b) the processing is carried out by automated means.

In exercising their right to data portability, the data subject shall have the right – where technically feasible – to have the personal data transmitted directly from one controller to another.

We hereby inform data subjects that the right to data portability can be exercised when both the above-listed conditions exist (e.g. when the processing is based on consent or a contract AND the processing is carried out by automated means).

Pursuant to the stipulations of Article 29 Data Protection Working Party (WP29), as the right to data portability can only be applied when the processing is carried out by automated means, this shall not apply to paper-based processing of data.

Right to object

The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them when the processing is necessary for the purposes of the legitimate interests of the Controller (Article 6, paragraph (1), point f).

In such cases, the Controller shall no longer process the personal data unless the 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.

Means of exercising rights

Data subjects shall be informed by the Controller without undue delay, yet in all cases within 30 days of their requests, on the measures introduced in relation to the request. Where necessary and in due consideration of the complexity and number of requests, this deadline can be extended by two further months. Controller shall inform the data subject on the extension of the deadline, indicating the reasons for the delay, within one month from the receipt of the request. Insofar as the data subject files the request electronically, the information – when possible – shall be provided electronically as well, unless the data subject requests otherwise. Insofar as the Controller fails to take measures in relation to the data subject's request, it shall inform the data subject without undue delay, yet in all cases within one month of the receipt of the request, on the justification for no action as well as the data subject's right to lodge a complaint with a supervisory authority or to exercise their right to judicial remedy.

Pursuant to the right to information, the Controller shall provide the data subject with the requested information and the measures taken in relation to the exercise of rights free of charge by default. If the data subject's request is manifestly unsubstantiated or – in particular due to its repeated occurrence – excessive, Controller, in respect of the administrative costs arising from the provision of the requested information:
a) may charge a reasonable fee, or
b) may refuse to take the requested measure.
The burden of proof regarding the unsubstantiated or excessive nature of the request lies with the Controller.

X Options for legal remedy

The data subject is entitled to file a complaint with a supervisory authority – in particular in the Member State of their habitual residence, place of work or place of the alleged infringement – if they consider that their personal data has processed in non-compliance with the Regulation.
Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the competent supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where they consider that their rights under the Regulation have been infringed as a result of the processing of their personal data in non-compliance with the Regulation. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has their habitual residence.

Data subjects may forward their complaints on the data processing practices of MOMART to the Hungarian National Authority for Data Protection and Freedom of Information (abbreviation: NAIH, address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c., mail address: 1530 Budapest, Pf.: 5., telephone: +36 (1) 391-1400, fax: +36 (1) 391-1410, e-mail: ugyfelszolgalat@naih.hu, website: https://www.naih.hu), or turn to the competent tribunal. The adjudication of the proceedings falls under the competence of the regional court of justice. At the data subject's discretion, proceedings may be filed as per the data subject's habitual place of residence or abode.

XI Data security measures

The Controller shall ensure that reasonable security measures are implemented to protect personal data (particularly against unauthorised access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique).

In the course of their everyday work, the Controller's employees must pay special attention to comply with the Controller's data protection provisions and accordingly provide for the safety and integrity of the personal data they process and prevent any data breaches.

Safety requirements of the processing of **paper-based personal data**:
- personal data may only be disclosed to authorised persons and may not be accessed or disclosed to unauthorised parties,
- documents shall be kept in dry, locked premises equipped with fire safety and security devices,
- the person performing the processing may only leave the office or premises where the processing is carried out by securing the documents or locking the premises.
- once the work has been completed, the documents are to be stored in a secure place.

Safety requirements of the processing of **data stored on computers**:
- personal data stored on a computer can only be accessed with valid, individually issued identifiable authorisation,
- the access of information is to be restricted (e.g. the data can only be accessed by employees whose tasks require said access) while using available information technology devices to prevent the network access of unauthorised parties,

- said information technology systems are to be protected by firewall and antivirus software,
- during the processing of personal data, continuous backups are prepared on the computers along with regular backups of the network systems.

MOMART's information technology systems and data storage sites are located at the company's premises.

Controller employs the following of the technical and organisational measures listed under Article 32 of the GDPR: Ensuring confidentiality:

By controlling physical access (ensuring that unauthorised parties do not access the processing system):
- reception / reception service / security staff
- attendance sheets
- corporate regulation ensuring that visitors do not remain unsupervised in company premises
- keys and key administration
- 24/7 video surveillance (CCTV)

Controlling access to the system (ensuring that unauthorised parties do not access the systems)
- principle of authorisation
- logging (attempted evasion),
- firewall
- password protection according to IT security regulations (minimum length, special characters, expiry, password recovery, password antecedents)
- locking accounts after multiple unsuccessful password entry attempts
- PC monitor locking in case of inactivity

Data access control (unauthorised access of data in the system, preventing unauthorised copying, altering or deletion of data in the system)
- differentiated roles and principle of authorisation
- access to the extent that is necessary
- blocking access when the position of the employee is changed or their employment is terminated
- encryption

By controlling separation (ensuring that the data collected for various purposes are processed separately)
- The processing of various clients is performed by various employees

Integrity

Controlling transfer (measures to prevent unauthorised parties from accessing data and the unauthorised copy, alteration or deletion during electronic transfer or conveyance)
- encryption of all data storage devices
- encryption of internal e-mails
- storing data storage devices in a safe location

Input control (measures to ensure whether the personal data stored in the data processing system has been entered, altered or deleted and who carried out these operations), document management

Data availability and resilience

Resilience control (measures to prevent the accidental or intentional destruction or loss of data)
- regular safety backups
- disaster-proof storing of data storage devices
- the latest virus and malware protection, firewall and intrusion control
- uninterruptible power supply

Rapid recovery (measures to restore timely access to personal data and the availability of data in the case of a physical or technical breach)
- security backup data centre (hot swap)
- emergency contingency plan

Other control procedures

Regular testing, assessment and evaluation (data protection management, breach control)

Contractual control (regular inspection of compliance with data protection regulations, data protection-related measures amongst employees, appropriate processor contracts)

XII Management of privacy incidents

Privacy incident: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; Privacy incidents include the loss of laptops or mobiles, the unsecured forwarding of personal data, the unauthorised copying and forwarding of client or customer lists or those which include personal data, server attacks, website hacking.

Privacy incidents can be reported through the momartkft@momart.hu e-mail address or via the +36 1 7816843 telephone number.

Controller shall log and analyse instances of access and attempted access through its information technology systems.
Controller is obliged to keep records of possible privacy incidents, including the facts related to the privacy incidents, their impact and the measures taken to remedy said incidents. The data related to privacy incidents is to be stored for a period of 5 years.

Controller shall report possible privacy incidents without undue delay and if possible, no later than 72 hours after becoming aware of the privacy incident, to the Hungarian National Authority for Data Protection and Freedom of Information (https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html) unless said privacy incident will most probably pose no risk to the rights and freedoms of natural persons. Insofar as the report is not filed within 72 hours, a justification for the delay must be included with the report.
Insofar as the privacy incident will most probably pose great risks to the rights and freedoms of natural persons, the Controller shall inform the data subject of the privacy incident without undue delay.

There is no need to inform the data subject pursuant to paragraph (1) insofar as any one of the following conditions apply:

- the Controller applied adequate technical and organizational measures, which have rendered the data incomprehensible for unauthorised parties;
- subsequent to the privacy incident, the Controller has taken measures that ensure that there will be no further great risks to the rights and freedoms of the data subject;
- providing information would entail disproportionate efforts. In such cases, the data subjects must be informed through publicly issued information or by taking measures that ensure providing data subjects with the same level of effectiveness.

When receiving a report of a privacy incident, the Controller shall examine the report without undue delay, with the involvement of information technology and legal experts. Primarily, it shall be established whether it is a real incident or just a false alarm. The following must be examined and established:

- the time and place of the incident,
- the description of the incident, its circumstances and impact,
- the range and multiplicity of the compromised data,
- the range of concerned individuals,
- a description of the measures taken to remedy the incident and its consequences.

In the event of a privacy incident, the concerned systems, persons and data are be identified and measures must be taken to collect and store the evidence that support that a privacy incident has taken place. Subsequent to this, the reparation of the damages and the restoration of legal operation may commence.

XIII Entry into force and subsequent amendment of the privacy policy

The present privacy policy shall enter into force on: 1 July 2019
Controller reserves the right to unilaterally amend or update the present policy without notice – which shall enter into force upon the publishing of the amendment. The policy which is in force shall be published on the Controller's website. When necessary, upon request, the Controller shall dispatch the Privacy Policy in force via e-mail.

_____
Imre Berkovits CEO MOMART 2020 Marketing Kft.