PRIVACY AND CONFIDENTIALITY POLICY

Effective from: 25 November 2019

I. GENERAL PROVISIONS

1. Purpose and scope of the policy

This policy ("**Policy**") lays down rules related to the protection of natural persons with regard to processing personal data and rules related to the free movement of personal data. This Policy shall apply for specific data processing activities as well as for issuing directives and notices regulating data processing. In order to comply with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter: Info Act) as well as the **General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council**, **Bluck Kft.** ("**Controller**") has drawn up this Policy and regards it as authoritative and obligatory to apply at all times in the course of its activities.

This purpose of this Policy is to harmonize the provisions of the Controller's other internal regulations on data processing in order to protect the fundamental rights and freedoms of natural persons and to guarantee the proper processing of personal data. Another important purpose of this Policy is to ensure that the Controller's employees should be able to lawfully process the personal data of natural persons by getting acquainted with and observing this Policy.

The subjective scope of this Policy covers:

- All of the Controller's employees, workers, sub-contractors as well as persons maintaining a contractual or other relationship with the Controller and dealing with data processing and having access to the data processed by the Controller under a specific legal title;
- Data flow towards the employed data processors and – unless otherwise agreed – the activities of such data processors;
- Data flow towards the recipients of transferred data;
- Data transferred by the Controller to, or exchanged with other controllers or third parties affecting personal data, as well as the activities of controller partners.

The objective scope of this Policy covers all data processing, data transfer and information transfer regarding all personal data processed, controlled or influenced by the Controller as well as all other activities related to the protection of data processing constituting the subject matter of such data processing and information transfer as well as all data processing operations regardless of the place of emergence and processing as well as the form of appearance.

The objective scope of the Policy covers all personal data that are processed, stored or transferred by the Controller electronically or in another manner – e.g. on paper – or accessed by the Controller in some manner.

2. Applicable regulations and internal regulatory documents

Data processing is governed by the following, effective laws, which may be modified from time to time. Should any of the laws change, the change required by the effective law shall be considered in the given part of the Policy and the Controller shall take the required actions to modify the policy within the shortest time possible.

Key legislation:

- Regulation (EU) 2016/679 of the European Parliament and of the Council 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**),
- Act V of 2013 on the Civil Code (hereinafter: "Civil Code"),
- Act I of 2012 on the Labour Code (hereinafter: "LC"),
- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter: „Info Act"),
- Act C of 2000 on Accounting

3. **Definitions**

Should there be any deviation between the following terms and the legal definitions, the definition specified by law shall apply.

- **data processing**: means 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.
- **data processor**: means a natural or legal person who processes personal data on behalf of the Controller;
- **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;
- **consent by the data subject**: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which s/he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her.
- **restriction of processing**: the marking of stored personal data with the aim of restricting their processing in the future;
- **registration system**: means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **data protectionincident**: a violation of security that results in incidental or unlawful annihilation, loss, change, authorized publication of, and unauthorized access to transferred, stored data or data processed in another manner.

4. **Eventual differences between certain rules and directives**

The Company acts as a Controller with regard to certain services specified below and as a data processor with regard to some other services. The data processing activities shall be governed by the contracts – and their annexes – concluded with the Controller. In the event of any difference, the provisions of the laws shall be authoritative, except for cases where deviation is permitted by law. In such cases this Privacy and Confidentiality Policy and the contract signed with the Controller shall be decisive.

5. **The basic principles of data processing**

Personal data may only be processed for a specific purpose, in order for rights to be exercised and obligations to be fulfilled. Data processing shall at all stages comply with the purpose of data processing, the data shall be collected and processed in a fair and lawful manner. Only those personal data may be processed that are indispensable, and are suitable for fulfilling the objective of data processing. Personal data shall be processed only to the extent and for the period required for achieving the purpose, in compliance with this Policy.

Before starting data processing, the data subject shall be given unambiguous and detailed information on all the facts related to processing his/her data, in particular on the purpose and the legal basis of data processing, on the person authorised to carry out the data processing, on the duration of data processing, whether the Company as Controller processes the personal data of the data subject by virtue of article 6 (5) of the Info Act as well as on who is authorised to have access to the data. Information shall also be given on the rights and legal remedies of the data subjects in connection with data processing.

Accountability: The Controller shall be responsible for, and be able to demonstrate compliance with the following basic principles. Should the Company act as a data processor, it shall fully promote the fulfilment of the basic principles and their accountability.

(1) Legitimacy, fairness and transparency

The Company shall process personal data lawfully, fairly and in a manner transparent for the data subject.

2) Purpose limitation

Data may only be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes.

(3) Data minimization

The data processing shall be adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed.

(4) Accuracy

The data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate with regard to the purposes for which they are processed are erased or rectified without delay.

(5) Storage limitation

Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject.

(6) Integrity and confidentiality

Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. **Lawfulness of processing**

From 25 May 2018, personal data processing shall be lawful only if and to the extent that at least one of the following applies:

1. a) the data subject has given appropriate, informed and voluntary consent to the processing of his or her personal data for one or more specific purposes;
2. b) data processing is needed for contractual fulfilment where the data subject is one of the parties, or it is needed for taking actions upon request by the data subject prior to signing the contract;
3. c) data processing is necessary for compliance with a legal obligation to which the Controller is subject
4. d) data processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. e) 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;
6. f) data processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The legal basis of data processing by the Company is briefly summarised in the table below:

Processed personal data	**Data categories**	**Legal basis**
Website visitors	Information stored in cookies	Consent
Client data	Contact details	Interest weighing based on legitimate interest Legitimate interest: the Company's interest in continuous business
Subcontractor data	Contact details	Interest weighing based on legitimate interest Legitimate interest: the Company's interest in continuous business
Employee data	Data set forth in the taxation act and other taxation rules	Fulfilling statutory obligations

Data processing in specific cases is explained in details in paragraph II.7.

7. **Data processing**

The Company, as a Controller, employs data processors: employees, workers, sub-contractors who accepted this Policy and are obliged to confidentiality.

We inform our Clients that the following personal data stored in the user account of Bluck Kft, (2310 Szigetszentmiklós, ÁTI-Sziget Ipari Park 12.) in the user database of www.gomining.com website and will be handed over to OTP Mobil Ltd. (H-1093 Budapest, Közraktár u. -32.) and is trusted as data processor. The data transferred by the data controller are the following: client's name, client's ID number, client's bankcard number, the time of payment.

The nature and purpose of the data processing activity performed by the data processor in the SimplePay Privacy Policy can be found at the following link: http://simplepay.hu/vasarlo-aff

8. **Data transfers**

The Company transfers the client's data to its partners. Special notification may be requested about the transfers. The company reserves the right to transfer data in a third country (for example: Russia, Japan etc.)

9. **Right to legal remedy**

The managers of the Company shall continuously check the compliance with the privacy laws and the internal regulations.

The Company's managers may review the internal regulations, minutes and records related to document management and data processing to check that the statutory data processing order is duly observed.

Supervisory authority:

Nemzeti Adatvédelmi és Információszabadság Hatóság

(Hungarian National Authority for Data Protection and Freedom of Information)

1125 Budapest, Szilágyi Erzsébet fasor 22/C

In the case where legal remedy is needed at court: regional courts have power and competence with the proviso that the regional court with territorial competence at the residence of the data subject shall also be entitled to proceed.

II. **DETAILED RULES**

1. **Transferring personal data**

With regard to contracts to be concluded with persons or organizations dealing with data processing for and on behalf of the Company, the Company shall ensure that the privacy requirements and guarantees are integrated in the text of the contract.

The Company's Client may store the applicants' materials until the purpose is achieved, in compliance with the relevant and effective laws, thus specifically with the provisions of Act CXII of 2011 on Informational Self-Determination and Freedom of Information („Info Act") and Regulation (EU) 2016/679 of the European Parliament and of the Council 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 - GDPR), such materials shall be processed confidentially and lawfully and exclusively for the purpose of filling the job position in question, in connection with the specific vacancy already available upon the use, such materials shall not be disclosed or made accessible to third parties once the job has been filled.

The Company and the Company's Client are obliged, and they warrant to fully cooperate in order to fulfil the applicants' requests, to respond to requests as well as with regard to eventual authority and/or court proceedings.

2. **Reporting complaints / claims**

Reporting claims to the Company:

The Company may provide the opportunity to report service-related claims in several manners: in writing, via e-mail. If the Company provides the opportunity to submit claims via e-mail, claims sent from the e-mail address – and exclusively from that e-mail address – provided to the Company earlier in connection with the given Service shall be regarded as a claim received from the data subject.

If data processing by the Company is not based on the data subject's consent but it was initiated by a third party through abuse, the data subject may request erasure of the personal data relevant to him/her that was disclosed by another person and s/he may request information about the data processing whilst properly verifying his/her personal identity and his/her relationship with the personal data.

In the event of death of the data subject, any close relative of the data subject or the person who gained benefits by way of a last will and testament may request erasure of data on the applicant or the Client or the potential Client whilst verifying his/her relationship with the data subject and may request data transfer by presenting the death certificate or sending a copy of it to the customer service address of the Service.

The Controller has 30 days for complaint management, but the Controller does its best to respond to each complaint or claim within the shortest time possible.

3. **The data subject's rights and their enforcement**

RIGHT OF THE DATA SUBJECT TO RECEIVE NOTIFICATION

The Controller primarily receives personal data from the data subjects, the Controller shall – upon request - provide the data subjects with the following information:

- Person and contacts of the Controller and its representative;
- Contacts of the data protection officer of the Controller:
- The purpose of the planned data processing and the legal basis for data processing;
- The categories of personal data concerned;
- Recipients of the personal data and recipient categories; information, if any, specified in the GDPR about transferring personal data to third countries;
- The period for which the personal data will be stored, or if it is not possible, the criteria used to determine that period;
- The Controller's legitimate interest if interest weighing is the legal basis of data processing;
- The fact that the data subject may request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object processing as well as the right to data portability;
- In the case of data processing based on consent, the right to withdraw the consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- The right to lodge a complaint with NAIH as the supervisory authority;
- Source of the personal data and, in a given case, whether the data come from a publicly available source;
- The existence of automated decision-making, including profiling, and, at least 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.
- Exercising the right to provide information may only be refused in cases set forth in article 14 (5) of the GDPR.

RIGHT OF ACCESS BY THE DATA SUBJECT

In response to the request by the data subject the Controller shall notify the data subject whether his/her personal data are being processed. If such data processing is in progress, the following information can be given upon request:

- the purposes of data processing:
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- 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, and, at least 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.

If requested separately, the Controller shall provide a copy of the personal data undergoing processing. 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. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

RIGHT TO RECTIFICATION AND ERASURE

Upon request by the data subject, the Controller shall rectify the relevant incorrect personal data without unreasonable delay and - taking into account the purposes of the processing – supplements the deficient personal data upon request by the data subject, e.g. by means of providing a supplementary statement.

Upon request by the data subject, the Controller shall delete the relevant personal data without unreasonable delay if

- 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 there is no other legal ground for the processing;
- the data subject objects to data processing and there is no lawful, prioritized reason for data processing or the data subject objects to using his/her data for direct marketing;
- processing the data subject's personal data is unlawful;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject;
- the personal data have been collected in relation to the offer of information society services to children.

The Controller shall communicate any rectification or erasure of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate efforts. The Controller shall inform the data subject about those recipients if requested by the data subject.

RIGHT TO LIMIT DATA PROCESSING

Upon request by the data subject, data processing by the Controller shall be limited if

- the accuracy of the personal data is contested by the data subject, in this case the limitation covers a period enabling the Controller to verify the accuracy of the personal data;
- the 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 data processing but the data subject needs them to submit, enforce or protect legal claims;
- the data subject has objected to data processing for legitimate interest or for public purpose; in this case the limitation shall refer to the period until it is established whether the legitimate grounds of the Controller override those of the data subject.

The Controller shall communicate any limitation of data processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate efforts. The Controller shall inform the data subject about those recipients if requested by the data subject.

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 a Controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another Controller if

- data processing is based on the consent or contract under the GDPR as a legal basis, or
- processing is carried out by automated means,
- excluding and limiting the right to data portability shall be governed by the provisions of the GDPR.

RIGHT TO PROTEST

The data subject is entitled to protest at any time against processing his/her personal data for a public purpose or a legitimate interest, for reasons related to his/her own situation, also including profiling. 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.

At the latest at the time of the first communication with the data subject, this right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

4. **Incident management as a Controller**

The data processing incident shall be reported by the Controller to the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information) without unreasonable delay, if possible, within 72 hours at the latest. The report shall be made in the form and manner as may be specified by the authority (e.g. on the platform indicated by the authority or on a hot line). If the data protection authority provides no platform, the report shall be made with its obligatory elements.

- If the data processing incident probably involves no risk for the rights and freedoms of natural persons, the report does not have to be made. This decision shall be made by the managing director, in consideration of all circumstances of the case.
- The Controller registers the data protection incidents, indicating the facts related to the data processing incident, their impacts and the actions taken for remedy. If the supervisory authority prescribes obligatory content elements for registering incidents, the incident registration table shall be drawn up with that content.
- The Controller shall notify the data subject about the data processing incident without unreasonable delay if the data processing incident probably involves a high risk for the rights and freedoms of natural persons. This decision shall be made by the managing director in consideration of all circumstances of the case, and s/he shall prepare a memorandum thereof.
- The data subject does not have to be notified if
    - The Controller took appropriate technical and organizational actions and these actions were applied for the data affected by the data processing incident, especially actions – e.g. applying encryption – that make the data uninterpretable by persons not authorized to access the personal data; or
    - After the data processing incident the Controller took further actions to guarantee that the high risk affecting the data subject's rights and freedoms will presumably not take place in the future; or
    - The notification would require disproportionate efforts, and in such a case the data subjects shall be notified through publicly disclosed information, or similar actions shall be taken to ensure that the data subjects are informed in a similarly effective manner.

5. **Data security rules**

All data must be protected through appropriate measures, with special regard to unauthorized access, modifications, transfer, disclosure, deletion or destruction as well as accidental destruction and damage, furthermore against becoming inaccessible due to a change in the applied technology.

When specifying and taking actions aimed at serving data security, the Company shall take into consideration the current technical development level. From among the several possible data processing solutions, the Company has to select the one that provides a higher protection level of personal data, unless it would represent a disproportionate difficulty for the Company.

With a view to enforce the data security rules, the required actions shall be taken for the security of personal data both processed manually as well as stored and processed on a computer.

The following basic principles must be taken into account when working out the specific security actions:

- Awareness: All users shall get acquainted with the security methods and procedures at least at a basic level in order to raise confidence in the IT systems.
- Responsibility: The responsibility of the IT system owners, the supporting staff and the data subject with regard to security shall be clear and unambiguous.
- Proportionality: The security levels and actions shall be appropriate for, and proportionate with the value of the protected systems and reliability requirements, with the costs of enhancing security as well as with the weight and the probability of potential damage arising from violating the security.
- Risk-proportionate security actions
- Timeliness: Security must be frequently reconsidered and updated according to the changes in the potential risks and consequences arising from violating the security. (Risk analysis – risk management)
- Integration: Coherent and integrated security approach is required with regard to all elements of an information system.
- Reaction ability: All participants shall cooperate in order to prevent the violation and the injury of security and to provide fast response to violation.

6. **Managing physical danger sources**

The physical protection system must be prepared for avoiding unauthorized access and the operators of the “infocommunication” infrastructure must be prepared for detecting and averting them as well as for preventing the unauthorized use of the devices.

The current anti-virus client is installed at each work station, and the periodical updates are downloaded and installed (with special regard to virus definitions).

7. **Specific data processing actions**

Website visitors

With regard to article 155 (4) of Act C of 2003, which says that “data may only be stored on subscribers’ or users’ electronic communications terminal devices, and data stored on such only accessed on the basis of the concerned user or subscriber’s consent following clear and full scope - also extending to the purpose of data processing - information provision to them”, the Controller provides the following information about the analytic devices used by it, i.e. cookies.

The Controller uses the following cookies for the following purposes:

Indispensable cookies

Such cookies are indispensable for proper website operation. Without accepting these cookies the Controller cannot guarantee the proper operation of the website and that the users will access all information searched by them. These cookies do not collect personal data from the data subjects or data that can be used for marketing purposes.

Indispensable cookies are e.g. the performance cookies that collect information as to whether the website is operating properly and whether there are errors in its operation. By indicating eventual errors they help the Controller to improve the website and they also indicate the most popular parts of the website.

Functionality cookies

These cookies provide for website appearance consistent with the data subject's needs and they remember the settings selected by the data subject (e.g.: colour, font size, layout).

The cookie also helps to improve the ergonomic design of the website, to make the website user-friendly and to enhance the visitors' online experience.

Management of Client data

Managing Client data means data processing carried out in order to provide the services of the Controller. The purpose of data processing is that the services of the Controller are provided effectively and contractually, by keeping proper contacts. In this case, the Controller will mainly store the data (name, address, phone number, e-mail address) of the contact person laid down in the contract or the order between the Controller and the Client in question. The legal basis of data processing is the fulfilment of the contract between the Controller and the Client.

The processed data are the personal data laid down in the contract between the Controller and the data subject, mainly the name, phone number, e-mail address, address at work of the contact person.

The Client data are accessed exclusively by the Controller's managing director as well as the Controller's associates and sub-contractors.

The Client data shall be processed confidentially, and the Client's personal data may not be accessed by persons other than those mentioned above.

The data may be processed until the date of contractual fulfilment or for 8 years based on Article 169 (2) of Act C of 2000 on Accounting.

Processing sub-contractor data

The purpose of data processing is to process data indispensable for keeping contacts with contracted sub-contractors. Data processing is based on the contract concluded by the Controller and the sub-contractor.

Scope of the processed data: personal data laid down in the contract between the Controller and the sub-contractor involved, mainly the name, phone number, e-mail address, address of the contact person.

The personal data of the sub-contractors may be accessed by the Company's management, its associates and the accountant in charge.

The data may be processed until the date of contractual fulfilment or for 8 years based on Article 169 (2) of Act C of 2000 on Accounting.

Processing employee data

When establishing employment, the employee provides the Controller with his/her personal data required for establishing employment, for exercising the employment-related rights and fulfilling the employment-related obligations. Apart from these data, the Controller shall not collect and not process employee data. The legal basis of personal data processing is the employee's consent and the Labour Code.

The processed personal data are as follows:

- Personal data specified in the act on the order of taxation,
- Personal data specified in the act on social insurance provisions and on their coverage,
- Personal data specified in the act on obligatory health insurance provisions.

The data may be accessed by the Controller's managing director and the accountant in charge.

If deemed necessary, the Controller may send its employees for an obligatory medical check-up every year. The medical aptitude document issued based on the check-up shall be delivered to the Controller but – apart from the employee's personal data – it may only feature information as to whether the employee is suitable or unsuitable for taking the job. Accordingly, the Controller shall not process any sensitive data on the employees either for the medical aptitude test or for other purposes.

The data are stored until the last day of the 6th calendar year following the year of termination of the employment, except where the legal regulations specify a longer period.

8. **Closing provisions**

This Policy shall enter into effect on the day following its approval by the Controller's managing director, the former privacy policy shall simultaneously become ineffective and its forms and sample declarations may not be used any further.

Budapest, 25 November 2019

Bluck Kft.