GENERAL DATA PROCESSING AGREEMENT

between the following parties:

Bisnode D&B Magyarország Kft., reg. no. 01-09-167465 (”Processor”), with address 30-32. Közraktár street, 1093 Budapest; and

Customer ("Controller"), as defined in Section I of the General Terms and Conditions of Bisnode D&B Magyarország Kft. which is available on https://www.bisnode.hu/aszf webpage.

The parties above are hereinafter also jointly called the “**Parties**” or individually a “**Party**.

1. Background

1.1. The Parties have previously, or in conjunction with this data processing agreement (the “**Agreement**”), entered into a service agreement in accordance with the provision of the General Terms and Conditions of the data processor (the "**Service Agreement**").

1.2. According to the terms and conditions of the Service Agreement, the Processor may process personal data on behalf of the Controller.

1.3. Under this Agreement, the terms and conditions for the Processor’s processing of and access to personal data, which the Controller is responsible for, are set out. The Agreement shall apply to all agreements entered into between the Parties and shall apply for the time period during which the Processor processes personal data on behalf of the Controller under the Service Agreement.

2. Definitions and interpretation

2.1. Unless the circumstances clearly set out otherwise, the definitions used in the Agreement, which are not defined herein, shall have the same meaning as defined under Article 4 of 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**”).

2.2. When interpreting this Agreement, the GDPR and other from time to time applicable laws, regulations, guidelines and codes of conduct regarding data protection shall be taken into consideration by the Parties.

2.3. Article 85 of the GDPR sets out that constitutionally protected databases fall out of the scope of the provsions of the GDPR. The Controller is aware of that the Processor's processing of personal data can be carried out in such constitutionally protected data bases and that – as a consequence thereof – the provisons of the GDPR are not applicable to such processing of personal data.

3. Processing of personal data

3.1. The Controller is, in the capacity of the data controller, responsible for the personal data processed within the scope of the Service Agreement.

3.2. The Processor shall process personal data on behalf of the Controller in accordance with the Agreement, including documented instructions to the Processor and in accordance with the documented, specific, instructions provided by the Controller from time to time. Such specific instructions, including inter alia relevant categories of personal data and data subjects and the purposes for which the personal data is processed, are set out in Appendix 1.

4. Use of sub-processors

4.1. By signing this Agreement, the Controller approves that the Processor is entitled to engage sub-processors for processing personal data on behalf of the Controller under the Agreement. The Processor shall notify the Controller of any intended changes concerning the addition or replacement of sub-processors. The Controller is, when applicable, entitled to object to such change provided that such objection is based on a reasonable ground such as lack of data protection or security. In such case, the Controller is entitled to terminate the Agreement and the Service Agreement as per the effective date of the relevant change of sub-processor. The Controller shall, however, not be entitled to such premature termination if the Processor chooses to instead replace the intended new sub-processor with another sub-processor that reasonably should be accepted by the Controller based on that the sub-processor fulfils applicable data protection and security requirements.

4.2. The Processor shall keep an updated list of the sub-processors engaged by the Processor from time to time (the "**Current List**") and shall, upon the Controller's request, provide a copy of the Current List to the Controller.

4.3. Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the Processor shall secure that the sub-processor, by way of a contract, undertakes to comply with the same data protection obligations, or obligations meeting the same level of data protection, as set out in the Agreement and the instructions provided by the Controller under the Agreement or the Service Agreement. The Processor shall be liable for all processing of personal data carried out by a sub-processor engaged by the Processor in relation to the Controller.

5. Transfer of personal data outside of EU/EEA

5.1. The Processor is entitled to transfer personal data to a country outside of the EU/EEA, including UK as from the effective date of Brexit, (a so called "**third country**") provided that at least one of the legal grounds (adequacy decision or appropriate safeguards) below shall apply;

a) the European Commission has decided that the security level in the relevant third country, to which personal data shall be transferred, is adequate. These countries are listed on the European Commisson's homepage;

b) the Processor has, on behalf of the Controller, entered into a binding agreement incorporating the European Commission's from time to time applicable standard data protection clauses for the transfer of personal data to third countries, with the subprocessor in the third country;

c) the transfer is based on binding corporate rules in accordance with article 47 of the GDPR; or

d) the recipient in the third country has adhered to the US Privacy Shield framework.

5.2. The legal grounds described in section 5.1 above shall not be required if transfer of personal data to a third country is required by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

6. Processor's obligations

General and data subjects' rights

6.1. The Processor undertakes to process the personal data in accordance with the provisions of this Agreement. The Processor shall thereby process the personal data in accordance with the documented instructions of the Controller and exclusively for the purposes described in the Service Agreement and this Agreement.

6.2. If a data subject exercises any of its rights regarding processing of its personal data under Chapter III of the GDPR, the Processor shall, taking into account the natue of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fullfillment of the Controller's obligation to respond to such requests from data subjects.

6.3. Should a data subject contact the Processor directly regarding a complaint relating to the processing of its personal data, or a request relating to the exercise of its rights, the Processor shall transmit such request to the Controller without undue delay including clear information on the subject of the request. The Processor shall not handle such request without prior instruction from the Controller.

Notification obligations of the Processor

6.4. If the Processor deems that an instruction from the Controller regarding the proccesing of personal data is in breach of the GDPR or other applicable data protection regulations, the Processor shall immediately inform the Controller thereof. In such case, the Processor is entitled to await acting on the relevant instruction until it has been confirmed or modified by the Controller.

6.5. If the Processor becomes aware of a personal data breach relating to the personal data under this Agreement, the Processor shall notify the Controller thereof without undue delay after becoming aware of the personal data breach.

6.6. Further, the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 33-34 of the GDPR, taking into account the nature of processing and the information available to the Processor.

Audits

6.7. The Controller is entitled to verify that the personal data processed by the Processor on behalf of the Controller under this Agreement are processed in accordance with this Agreement and the instructions provided by the Controller. Thereby, the Processor shall make available to the Controller all information necessary to demonstrate such compliance. The Processor shall also take measures for allowing, and contributing to, the audits, including inspections, conducted by the Controller or a third party appointed by the Controller. Such third party shall not be a direct competitor to the Processor and shall have undertaken to comply with confidentiality obligations not less restrictive than those set out under the Service Agreement.

6.8. The Controller shall no later than ten (10) business days prior to an intended inspection notify the Processor thereof. For any other audits, the Processor shall have at least 14 business days of time to compile and provide to the Controller the relevant information set out in section 6.7 above.

Technical and organizational measures

6.9. The Processor shall take sufficient technical and organisational measures in order to protect the personal data processed under the Agreement in accordance with Article 32 of the GDPR, see Appendix 2.

6.10. The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 and 35-36 taking into account the nature of processing and the information available to the Processor.

7. Compensation

7.1. The Processor is entitled to reasonable compensation for such assistance provided by the Processor in accordance with sections 6.2, 6.6 and 6.10 above if such assistance results into that the Processor on a frequent basis must allocate resources to a non-insignnificant extent. The Processor shall also be entitled to reasonable compensation for assistance in

audits, including inspections, conducted by the Controller (or any third party mandated by the Controller) in accordance with section 6.7 above if conducted more frequent than on an annual basis. However, if the result of the audit shows that the Processor has not fulfilled its obligations under the Agreement, the Processor shall not be entitled to such extra compensation.

7.2. In addition to what is set out in section 7.1 above, the Processor is entitled to reasonable compensation upon changed instructions which results into an increased cost or extra work for the Processor and which goes beyond the requirements under applicable data protection legislation.

7.3. If the Processor is entitled to extra compensation under sections 7.1-7.2 above, the Processor's from time to time applicable price list for time and material work shall apply.

8. Liability

8.1. If a data subject, a supervisory authority or other third party directs any claim or action against the Controller resulting in that the Controller incurrs any damages (including both damages to data subjects and administrative fines to a supervisory authority) due to the Processor's (or its subprocessor's) processing of personal data outside or in violation of the Controller's instructions, this Agreement or applicable data protection legislation, the Processor shall compensate and hold the Controller harmless for such damages.

8.2. If the event a data subject, a supervisory authority or other third party directs any claim or action against the Processor resulting in that the Processor incurrs any damages (including both damages to data subjects and administrative fines to a supervisory authority) due to the Controller's inadequate or unlawful instructions or breach of this Agreement or applicable data protection legislation, the Controller shall compensate and hold the Processor harmless for any such damage.

8.3. Each Party's liability according to section 8.1 and section 8.2, respectively, shall per contract year be limited to direct damages up to a maximum amount of 100% of the annual contract value of the Service Agreement.

8.4. For the avoidance of doubt, the Parties shall never be held liable for indirect damages, such as but no limited to loss of profit and/or income, unless such damages have been caused by intent or gross negligence.

9. Termination and expiry of the Agreement

9.1. In case the Service Agreement is terminated, this Agreement shall be deemed automatically terminated in accordance with the terms of the Service Agreement.

9.2. Upon the the termination of the Service Agreement, the Processor shall return all personal data to the Controller or, where so notified by the Controller in writing, delete all personal data processed by the Processor under this Agreement.

10. Confidentiality

10.1. The Processor undertakes to not discolse or otherwise in any way provide information relating to personal data or processing of such under this Agreement to any third party. The Processor shall also secure that persons being authorised to process, or otherwise having access to, personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. These confidentiality undertakings do not apply if the Processor is required to disclose the information by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

11. Governing law

11.1. This Agreement shall be governed by and construed in accordance with the provisions set out in the Service Agreement.

Adoption of this Agreement is concluded by the acceptance of the Controller together with the Service Agreement. The statement is concluded in one of the following ways:

- in case of filling in a printed order form with signing the order form,

- in case of electronic (online) contracting with ticking in a separate checkbox,

- in case of a phone contract with the acceptance of the agreement via phone.

******

APPENDIX 1

SPECIFIC PROVISIONS

Categories of treated personal data:

Identification and Contact Information (Name, Address, Phone, Email Address, Tax ID, etc.)
Financial characteristics (income, financial transactions, credit information, tax information, etc.)
Occupation and job position
Personal characteristics (age, gender, marital status, etc.)
Legal information (judgments, court and official decisions, etc.)

Special data

Special data will not be processed.

Categories of data processing purposes

See the Data Processing General Terms and Conditions

Categories affected

Workers, consultants and their representatives
Clients
Potential Customers
Suppliers

Categories of data processing

See the Data Processing General Terms and Conditions

******

APPENDIX 2

TECHNICAL AND ORGANISATIONAL MEASURES

Contents

1. Scope of application

Under the Data Protection Regulation (GDPR) any entity which, either itself or on behalf of another, collects, processes or uses personal data is obliged to take such technical and organisational measures as are necessary to ensure the implementation of statutory data protection rules. This document sets out the safeguards which have been put in place pursuant to Article 28 in GDPR.

2. Entry Control

Entry control serves to bar unauthorised parties from gaining access to technical equipment by which personal data is processed or used.

2.1. Entry control at Processor operating premises

Entry to Processor's buildings is regulated by admission controls. For Processor staff, these primarily consist of electronic keys which permit entry to operating premises according to the rights of access stipulated for each key. Rights of access are aligned with the powers granted to staff both timewise (according to permitted usage on certain weekdays and certain times of day) and location-wise (according to specific parts of the operating premises). For outsiders, entry control is ensured by a central reception lobby or doorman service which records visitors' data and issues visitors with visitors' passes valid for the duration of their respective visits.

2.2. Control of entry to Processor computer centre

Processor's IT systems are operated on behalf of Processor by different data centre. The data centres are designed as closed security spaces. There is both structural and technical admission control. The data centres are secured electronically and visitors are only permitted access when accompanied and

are not left unsupervised. The entry cards required are only issued after prior notification and on strict terms and conditions. Usage is logged. The data centres are monitored by video and the site as well as critical internal areas of the building are also overseen around the clock by a security company.

3. Admission Control

Admission control encompasses measures by which the use of data processing systems by unauthorised parties is prevented (logical security).

3.1. Control of admission to Processor operating premises

Administrative work done by Processor or the data centre operator is only carried out by certain members of staff who have signed a special confidentiality agreement and been checked before being hired. The confidentiality agreement contains a commitment to data secrecy. Where administrative work is done through external access those so-called VPN connections are encrypted using the latest technology and additional authentication is required. Identification with user names and secure passwords is obligatory. The Processor IT system is also shielded from outside attacks by firewall technology.

3.2. Control of admission at data centre operator

In order to secure the systems run for Processor the data centre operator has installed additional high-end firewall functions within the network layer and admission products.

4. Access Control

Access control encompasses measures to ensure that parties authorised to use a data processing system can only gain access to data which they are authorised to access and that personal data cannot be read, copied, changed or deleted without permission during the course of processing or use and after being saved.

4.1. Access control at Processor operating premises

Processor has defined and documented internal standards for the handling of permissions. These govern the rights that administrators have over systems run for clients. These set out, for example, the requirements concerning secure passwords.

4.2. Access control at data centre operator

Where the data centre operator is contracted by Processor to take over the setting up of users and authorisations at application layer it will in principle be bound by the same security standards as those applicable to Processor operating premises themselves. Deviations are only permitted if directed by Processor in writing. The definition of guidelines as to how application-specific authorisation concepts are to be designed by the data centre operator is determined by Processor.

5. Transmission Control

Transmission control encompasses measures to ensure that personal data cannot be read, copied, changed or deleted without permission during electronic transfer, whilst in transit or when saved on data media and that it is possible to verify and establish where personal data is to be transmitted using data communication equipment.

5.1. Transmission control at Processor operating premises

With regard to the general processing of data at Processor (staff data, supplier data, customer base data) transmission control (transfer control, transportation control, communication control) is ensured by way of appropriate technical measures. These include firewall, virus protection, VPN tunnel, data encryption (especially by https/SSL transmission or VPN tunnel) and password protection for individual documents. The only storage media used for the electronic transmission of confidential data are those which enable data to be encrypted. Only suitable service providers are employed in the logistical transportation of data.

With regard to the commercial processing of data at Processor, especially the receipt and provision of its clients' data in the course of Processor's information business, transmission control is ensured by logging all data processing stages. Where agreed with the client, data classified as particularly confidential is further encrypted for the purposes of transmission via public networks.

5.2. Transmission control at data centre operator

The data centre operator is bound by the same obligations regarding transmission control as Processor itself. For operationally essential copies (backup), especially in the context of essential data security, only standardised and documented procedures are used. The production of all backups is logged.

6. Input Control

Input control encompasses measures to ensure that it is possible to subsequently verify and establish whether and by whom personal data in data processing systems has been entered, changed or deleted.

Inputting may only be undertaken by staff who have access to the data (see stipulations on access control in section 3).

Logs of "certain process actions" on systems are also automatically created. The logging of "certain process actions" relates to processes which serve to ensure business continuity, which serve accounting purposes and the fulfilment of statutory retention requirements.

7. Contract Control

Contract control encompasses measures to ensure that personal data processed under a contract can only be processed according to the client's instructions.

Where Processor processes personal data on a contract basis a written agreement on contract data processing is always concluded with the statutory content required under GDPR. Processor also has its own specimen form contracts available for such an eventuality which the client may use for that purpose. Contractual commitments ensure that Processor only processes client data according to their instructions, that the confidentiality of data is guaranteed and in particular that, in the absence of the client's express instructions to the contrary, client data does not become incorporated in Processor's general database of information.

Furthermore, the details of technical and organisational security measures in place at Processor form part of every contract data processing agreement with Processor as a result of this document being an agreed annex to such contract data processing agreement.

8. Availability Control

Availability control encompasses measures to ensure that personal data is safeguarded from accidental loss or destruction.

The foundation of availability control is the outsourcing of the operation of IT equipment to the data centre operator's high-security data centre. The latter has, in particular, redundant supply systems with an uninterruptible power supply and emergency generating unit (using redundant diesel generators, for example). The data centre is linked to Processor's operating premises by means of a direct connection to the medium-voltage level via its own transformer station or an equivalent connection. There are also early fire detection systems installed in the data centres which automatically trigger an extinguishing process.

Data availability, especially protection from data loss due to technical malfunction or accidental deletion, is also ensured through regular data safeguards and backups of all relevant databases and systems, so that in the event of a breakdown they can be restored on at least a monthly basis.

9. Separation Rule

The separation rule encompasses measures to ensure that data gathered for different purposes can be processed separately.

9.1. Separation rule at Processor operating premises

With regard to the general processing of data at Processor (staff data, supplier data, customer base data) the separation rule is implemented, for example, by a physical separation and storage on separate systems or data media, the separation of productive, testing and development environments for our applications and IT systems, appropriate authorisation concepts, as well as database rights. Furthermore, on the software side, a logistical client separation system is implemented.

With regard to the commercial processing of data at Processor, especially the receipt and provision of its clients' data in the course of Processor's information business, separation in the data protection sense is principally achieved on an application basis. All data packs supplied are processed quite separately from each other so that any possibility of client data overlapping is ruled out. The appropriate precautions have been taken here (hardware and software).

9.2. Separation rule at data centre operator

The data centre operator separates all data both physically and logically at client level at least. Where a Processor layer is outsourced to the data centre operator there are generally further separate interfaces available based on a system or database.

******