DATA MANAGEMENT POLICY

Boxelence Innovation Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság (registered office: 4200 Hajdúszoboszló, Rákóczi utca 188., company registration number: Cg.09-09-036512, tax number: 32690765-2-09, statistical number: 32690765-4755-113-09, represented by: László Dános, managing director), as Data Controller, hereby establishes the following Data Processing Policy (hereinafter: Policy) in accordance with 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 (EU Regulation):

I. Introduction

1. Purpose of the Policy

By creating, complying with, and enforcing the provisions of this Policy, the Data Controller implements organizational and technical measures in its business to process the personal data of natural persons who come into contact with it in accordance with the relevant EU regulation. The Data Controller undertakes to comply with the provisions of these Rules unilaterally and requests that its customers and partners also accept and comply with them.

In the course of its activities, the Data Controller pays particular attention to the lawful collection, secure storage, processing and protection of personal data, as well as to compliance with the relevant legislation in force and to secure and fair data processing.

The Data Controller implements appropriate technical and organizational measures to ensure and demonstrate that personal data is processed in accordance with the EU Regulation, taking into account the nature, scope, context, and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons. These measures shall be reviewed and, where necessary, amended by the Data Controller on an ongoing basis in accordance with this Policy.

The Data Controller reserves the right to unilaterally amend the Privacy Policy.

2. Interpretative provisions

The terms used in this Policy are interpreted and used by the Data Controller as follows:

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.

Data Subject: a natural person who provides personal data or whose personal data is made available to the Company.

Data processing**:** any operation or set of operations performed on personal data or data files, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data controller: a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union or Member State law, Union or Member State law may also lay down specific criteria for the controller or for the designation of the controller.

Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

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.

Data disclosure: making data available to a specific third party.

Disclosure: making data available to anyone.

Data erasure: rendering data unrecognizable in such a way that it can no longer be restored.

Data destruction: the complete physical destruction of the data carrier containing the data.

Recording system: a structured set of personal data organised in any manner, whether centralised, decentralised, functional or geographical, which is accessible on the basis of specific criteria.

Consent of the data subject**:** a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Recipient: a natural or legal person, public authority, agency or any other body to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party: a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and persons who, under the direct authority of the controller or the processor, are authorized to process personal data.

Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Scope of the Policy

a) Temporal scope

These Regulations shall be effective from 202 6.01 .10. until further notice or revocation.

b) Personal scope

The personal scope of these Regulations extends to

- the Data Controller,
- persons whose data are contained in data processing operations covered by these Rules, and persons whose rights or legitimate interests are affected by data processing. The Data Controller therefore primarily processes the data of natural persons who have contacted the Data Controller for the purpose of establishing a relationship, either through the means available to them, such as by sending their data to any of the Data Controller's e-mail addresses at , via social media, by telephone, or in person, have used or requested the Data

Controller's services; or have contacted the Data Controller for reasons or purposes other than establishing contact;
- to the Data Controller's employees;
- the Data Controller's natural person partners, representatives of non-natural person partners, contact persons, or other employees.

c) Material scope

The scope of this Policy covers all data processing involving personal data carried out in all organizational units of the Data Controller, regardless of whether it is done electronically and/or on paper.

In the case of paper-based data processing, the Data Controller shall also introduce and operate a document management and disposal policy that is formally separate from this Policy, which supplements the general provisions of this Policy and is covered by the scope of this Policy, and therefore shall be considered an annex to this Policy.

II. Principles of data processing

The Data Controller may only process personal data for the purposes specified in this Policy, in order to exercise its rights and fulfill its obligations. Only personal data that is essential for the achievement of the data processing purpose specified by the Data Controller and suitable for achieving the specified purpose may be processed. Personal data may only be used to the extent and for the duration necessary to achieve the purpose. Data processing must comply with this principle and the following basic requirements at all stages:

1. **Lawfulness, fairness and transparency**: Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. **Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with those purposes.

3. **Data minimization:** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy:** Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. **Storage limitation:** Personal data must be stored 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 only insofar as the personal data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6. **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. **Protection of data of persons under the age of 16:** The personal data of persons under the age of 16 may only be processed with the consent of their legal representative.

III. Purpose and legal basis of data processing

1. The purpose of data processing is to process the data of natural persons who enter into a legal relationship (civil law, labor law, administrative law, etc.) with the Data Controller in the course of its activities specified in its articles of association, to the extent necessary for the exercise of its rights and the fulfillment of its obligations. The Data Controller endeavors to process only personal data that is essential for the purpose of data processing and suitable for achieving that purpose. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose. The purpose of data processing is primarily to provide the Data Controller's services and to establish and fulfill its commercial and contractual relationships.

2. The Data Controller may only process the data subject's data in the following cases (legal grounds):
   a) the Data Subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
   b) the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   d) processing is necessary in order to protect the vital interests of the Data Subject or another natural person;
   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;
   f) 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 Data Controller processes only personal data provided by the Data Subjects or legal entities using the Data Controller's services for the purpose of performing the ordered service and does not collect data from other sources.

3. **The Data Controller processes data in the following cases:**
   a) Recording employee data in connection with the establishment, performance, modification, and termination of the employment relationship, as well as the enforcement of the employer's claims against the employee – GDPR Article 6(1)(b), (c)
   b) Recording employee data for the purpose of claiming family tax allowances – GDPR Article 6(1)(a)
   c) Recording employee data for the purpose of cafeteria benefits – GDPR Article 6(1)(a)
   d) Recording employee data for occupational health examinations – GDPR Article 6(1)(c)
   e) Processing of employee data for the purpose of investigating accidents at work – GDPR Article 6(1)(c)
   f) Recording employee data for training and further education purposes – GDPR Article 6(1)(a)
   g) Recording employee data for the purpose of accessing the data controller's IT system – GDPR Article 6(1)(a)
   h) Recording employee data for the purpose of providing work clothing – GDPR Article 6(1)(a)
   i) Recording employee data for the purpose of issuing workplace access cards – GDPR Article 6(1)(a)
   j) Recording of employee images by electronic surveillance system for the purpose of physical security, property protection and facility security – GDPR Article 6(1)(a), (c) and (f)
   k) Recording of employee GPS data for the purpose of property and personal protection – GDPR Article 6(1)(f)

l) Recording customer data for the purposes of placing, processing and fulfilling orders, invoicing, warranty and guarantee claims, assessing customer complaints and enforcing claims against customers – GDPR Article 6(1)(a)
m) Processing of contact details of persons employed by partner companies for the purpose of conducting business with partner companies – Article 6(1)(a) of the GDPR

4. Scope of data processed by the data controller:

a) Employees (name, birth name, place and date of birth, mother's name, address, personal identification number, tax identification number, social security number, driver's license number, telephone number, email address, bank account number, data relating to educational qualifications, health record, clothing size, photograph)
b) Contact persons employed by partner companies (name, address, telephone number, email address, position)
c) Natural person customers (name, place and date of birth, mother's name, tax identification number/tax number, billing address, email address, telephone number)

5. Categories of recipients:

a) In the case of employees, the Data Controller's accountant, auditor, lawyer, IT specialist, company doctor, National Tax and Customs Administration, National Health Insurance Fund, Hungarian State Treasury, labor inspector.
b) The personal data of customers may only be accessed by the Data Controller and its employees to the extent necessary for their activities. Personal data will be transferred to authorities upon request or in accordance with legal requirements.
c) Customer data is transferred to service providers performing payroll accounting and bookkeeping.
d) In addition to the named data processor, other third parties may also have access to customer data in order to comply with legal obligations (in particular accountants, auditors, lawyers, IT specialists, etc.).
e) An external service provider has been commissioned to maintain the IT systems and applications used.
f) The Data Controller collects the contact details of partners' representatives for internal use only.

The Data Controller shall not transfer the personal data it processes to third parties other than the recipients specified in this section. In certain cases – official court or police requests, legal proceedings, copyright, property or other infringements or reasonable suspicion thereof, damage to the Company's interests, jeopardizing the provision of services, etc. – the Data Controller may make the personal data of the Data Subject available to third parties.

6. Deadlines for the deletion of different categories of data:

a) The Data Controller shall store the data of employees for the period specified in the relevant legislation and delete them upon request.
b) The Data Controller shall delete the data of contact persons employed by partner companies upon request, or, in the absence of such a request, shall store them until the termination of the contractual relationship at the latest.
c) The Data Controller shall delete customer data upon request, or store it for a maximum of 5 years if no request is made.

IV. The Data Controller

The Data Controller is **BOXELENCE INNOVATION Kft.**

The Data Controller has not appointed a data protection officer, given that it does not carry out any data processing activities that would make this necessary.

The Data Controller does not engage in automated decision-making or data processing involving profiling.

V. Data processing

1. **Data transfer**: The Data Controller shall only transfer personal data to third parties if the Data Subject has given their explicit consent or if the data transfer is authorised by law. The Data Controller is entitled and obliged to transfer all Personal Data at its disposal and stored by it in accordance with the law to the competent authorities if it is obliged to do so by law or by a final official order. The Data Controller cannot be held liable for such Data Transfer and the consequences thereof. The Data Controller shall document all data transfers and keep records of them.

2. **Data processing**: The Data Controller is entitled to use data processors to perform its activities. Data processors do not make independent decisions; they are only entitled to act in accordance with the contract concluded with the Data Controller and the instructions received. The Data Controller supervises the work of data processors. Data processors are only entitled to use additional data processors with the consent of the Data Controller. The Data Controller may only use data processors who provide adequate guarantees for the implementation of appropriate technical and organizational measures to ensure compliance with data processing and the protection of the rights of data subjects. The data processor may not engage any further data processors without the prior written authorization of the Data Controller, either on a case-by-case basis or in general. In the case of general written authorization, the data processor shall inform the Data Controller of any planned changes affecting the use or replacement of additional data processors, thereby giving the Data Controller the opportunity to object to such changes.

3. **External service providers**: The Data Controller uses external service providers with whom the Data Controller cooperates. With regard to personal data processed in the systems of external service providers, the provisions of the external service providers' own data protection policies shall apply. The Data Controller shall do everything in its power to ensure that the external service provider processes the personal data transferred to it in accordance with the law and uses it exclusively for the purposes specified by the Data Subject or set out in the Policy below.

VI. Rights of the Data Subject

1. **Right of access/right to information:** The Data Subject has the right to receive feedback from the Data Controller as to whether their personal data is being processed, and if such processing is underway, they have the right to access their personal data and the following information.

2. **Right to rectification:** The Data Subject has the right to request that the Data Controller rectify inaccurate personal data concerning him or her without undue delay. Taking into account the purpose of the processing, the Data Subject has the right to request that incomplete personal data be completed, including by means of providing a supplementary statement.

3. **Right to erasure:** The Data Subject shall have the right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay and the Data Controller shall have the obligation to erase personal data concerning the Data Subject without undue delay in the cases specified by law.

4. **Right to restriction of processing:** The Data Subject shall have the right to obtain from the Data Controller restriction of processing where one of the following applies:
   a) the data subject disputes the accuracy of the personal data, in which case the restriction shall apply for a period enabling the data controller to verify the accuracy of the personal data;

b) the processing is unlawful and the Data Subject opposes the erasure of the data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or
d) the data subject has objected to the processing; in this case, the restriction applies for a period until it is determined whether the legitimate grounds of the controller override those of the data subject.

5. **Right to object:** The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. In this case, the Data Controller may no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.

6. The Data Subject provides the data independently, and the Data Controller does not give any mandatory guidelines or set any content requirements in this regard. The Data Subject expressly consents to the processing of the data provided by him/her. The Data Subject is entitled to provide data other than those requested by the Data Controller, in which case the legal basis for the processing of the data is also the voluntary consent of the Data Subject. The Data Controller records the IP address of the Data Subject when they access individual websites in connection with the provision of the service, in view of the legitimate interests of the Data Controller and for the purpose of ensuring the lawful provision of the service (e.g. to filter out unlawful use or unlawful content), without the separate consent of the Data Subject.

VII. Obligations of the Data Controller

In order to facilitate the exercise of the rights of the Data Subject specified in Section VI, the Data Controller shall be subject to the following obligations:

1. The Data Controller shall provide the Data Subject with any notification and information to be provided in the cases specified in this Act in an easily accessible and readable form, with content that is concise, clear, and easy to understand.

2. The Data Controller shall assess any request submitted by the Data Subject to exercise his or her rights within the shortest possible time from the date of submission, but no later than twenty-five days, and shall notify the Data Subject of its decision in writing or, if the Data Subject submitted the request electronically, by electronic means. The Data Controller shall perform its duties specified in this Act in connection with the exercise of these rights free of charge.

3. In order to enforce the right to prior information, the Data Controller shall, prior to the commencement of data processing operations carried out by it or by a data processor acting on its behalf or on its instructions, or at the latest immediately after the commencement of the first data processing operation, make available to the data subject
   a) the name and contact details of the data controller and the data processor;
   b) the contact details of the data protection officer;
   c) the purpose of the planned data processing;
   d) the rights of the data subject under this Act and the manner of exercising those rights
   .

4. The data controller shall also provide the data subject with information on
   a) the legal basis for data processing;
   b) the period for which the personal data will be stored, and the criteria used to determine that period;

c) in the event of the transfer or planned transfer of the personal data processed, the recipients of the data transfer;
d) the source of the personal data processed;
e) any other relevant facts relating to the circumstances of the data processing.

5. In order to enforce the right of access, the data controller shall, at the request of the data subject, inform him or her whether his or her personal data are processed by the data controller itself or by a data processor acting on its behalf or on its instructions.

6. In order to exercise the right to rectification, if the personal data processed by the data controller or by a data processor acting on its behalf or on its instructions is inaccurate, incorrect, or incomplete, the data controller shall, in particular at the request of the data subject, immediately rectify or correct them, or, if compatible with the purpose of the processing, supplement them with additional personal data provided by the data subject or with a statement by the data subject attached to the personal data processed.

7. The Data Controller shall protect the data in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction and damage. The Data Controller, together with the server operators, shall take technical, organizational, and organizational measures to ensure the security of the data, providing a level of protection appropriate to the risks associated with data processing.

8. The Data Controller and the data processor shall take into account the state of the art and the costs of implementation, and the nature, scope, context, and purposes of the data processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons, in order to ensure a level of data security appropriate to the risk. In other words, the Data Controller shall ensure the security of the data, take the technical and organizational measures and establish the procedural rules necessary to enforce the applicable laws and data and confidentiality protection rules. The Data Controller shall protect the data by appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction and damage, and against inaccessibility resulting from changes in the technology used.

9. Organizational measures include controlling physical access to buildings, training employees, and locking paper-based files in appropriate rooms. Technical measures include encryption, password protection, and the use of antivirus software for access to systems.

10. The Data Controller is not required to appoint a data protection officer, as the Data Controller is not a public authority or a body performing a public task, and the Data Controller's activities do not involve operations that require regular and systematic monitoring of Data Subjects on a large scale. and the Data Controller does not process special data or personal data relating to decisions on criminal liability and criminal offenses.

VIII. Data security breach (data protection incident)

1. A **data** security breach results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data that has been transmitted, stored or otherwise processed.

2. In the absence of appropriate and timely measures, a data breach **may cause** physical, financial or non-financial **damage to natural persons**, including loss of control over their personal data or restriction of their rights, discrimination, identity theft or misuse of identity , financial loss, unauthorized disclosure of pseudonyms, damage to reputation, breach of confidentiality of personal data protected by professional secrecy, or other significant economic or social disadvantage affecting the natural persons concerned.

3. In view of the above**,** the Data Controller shall notify the competent supervisory authority of any data protection incident that comes to its attention **without undue delay, no later than 72 hours after becoming aware of the data protection incident** unless it can demonstrate, in accordance with the principle of accountability, that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

4. If the notification cannot be made within 72 hours, the Data Controller shall indicate the reason for the delay and may provide the required information in phases without further undue delay.

5. **In the notification** of the data breach, the Data Controller shall:
   - describe **the nature of** the data breach, including the categories and approximate number of data subjects concerned and the categories and approximate number of data concerned by the breach;
   - provide the name and contact details of the **data protection officer** or other contact person providing further information;
   - describes **the** likely **consequences** of the data breach;
   - describe **the measures taken or planned** by the data controller to remedy the data breach, including, where appropriate, measures to mitigate any adverse consequences resulting from the data breach.

IX. Remedies available to the data subject

1. Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every Data Subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement – if they consider that the processing of personal data relating to them infringes the EU Regulation.

2. Right to effective judicial remedy against the supervisory authority

Without prejudice to any other administrative or non-judicial remedy, every natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

3. Right to effective judicial remedy against the controller or processor

Without prejudice to any other administrative or non-judicial remedy, every data subject shall have the right to an effective judicial remedy if the competent supervisory authority does not deal with the complaint or does not inform the data subject within three months of the progress or outcome of the complaint. Every data subject shall have the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

4. Right to compensation and liability

Any person who has suffered material or non-material damage as a result of an infringement of the EU Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. All controllers involved in the processing of data shall be liable for any damage caused by processing that infringes the EU Regulation.

The data processor shall only be liable for damage caused by data processing if it has not complied with the obligations laid down in this Regulation, specifically those incumbent on data processors , or if it has disregarded or acted contrary to the lawful instructions of the data controller.

5. Information on legal remedies

- In Hungary, the data protection supervisory authority is:

National Authority for Data Protection and Freedom of Information
Registered office: 1055 Budapest, Falk Miksa utca 9-11.
Contact details: ugyfelszolgalat@naih.hu

- Proceedings against the supervisory authority shall be brought before the courts of the Member State where the supervisory authority has its registered office.

- Proceedings against the data controller or data processor shall be brought before the courts of the Member State where the data controller or data processor has its place of business. Such proceedings may also be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

X. Specific areas of personal data processing

1. Processing of employees' personal data

In the processing of employment data, you must act in accordance with the principle of data minimization: you may only keep data required by the labor code as part of the employment contract, as well as data that enables communication with the employee, the conditions necessary for the employee's fitness for work and performance of their job, other data required by law, and data that enables the employee to exercise their rights.

In accordance with its obligations under the GDPR, the Infotv. and the Mt., the Employer shall provide its employees with a written employee data processing notice, written in simple, understandable language, which describes the data stored about them, how it is processed, and their rights in this regard. This information may be supplemented by the parts of the employer's data processing policy that apply to employees or impose obligations on them.

The employer may require the employee to make a statement or disclose personal data that is relevant to the establishment, performance, termination (cancellation) of the employment relationship or the enforcement of a claim arising from this Act.

The employer, the works council, and the trade union may require a statement or the disclosure of data for the purpose of exercising their rights or fulfilling their obligations as specified in Part III of the Labor Code.

An aptitude test may be applied to the Employee if it is required by the rules governing the employment relationship or if it is necessary for the exercise of a right or the fulfillment of an obligation specified in the rules governing the employment relationship.

The Employer shall inform employees in writing about its data processing activities.

2. Handling of CVs and job applications

CVs submitted to the Data Controller by job applicants shall be processed by the Data Controller for a specific purpose, i.e. to fill vacant positions, to recruit employees, and until the purpose is achieved, i.e. until a suitable candidate is selected or the candidate is hired.

The data processed in this way is provided by the applicants themselves and typically includes their name, contact details (telephone, e-mail, postal address), information on their education, professional qualifications, other licenses and skills, professional experience, professional competencies, and areas of interest.

CVs are generally retained by the Data Controller until the selection process is complete, i.e. until a stable, permanent employee is hired for the position.

The Data Controller will retain the CVs of employees selected in the selection process until the conclusion of the employment contract. At the end of the selection process, the Data Controller shall destroy the CVs of unsuccessful candidates at its discretion without separate notification, or retain them for six months from the evaluation and completion of the selection process (in the case of unsuccessful probationary applicants or early termination), unless the data subject objects to this. The Data Subject must be notified of this immediately, and in the event of an objection, the Data Controller shall immediately cease data processing and the CV shall be destroyed.

CVs submitted/received without an advertised job opportunity shall be destroyed by the Data Controller at its discretion without separate notification, returned to the Data Subject, or, in the absence of any other statement by the Data Subject, retained for six months from the date of submission in case of a vacancy.

The legal basis for data processing in relation to CVs is the consent given by the applicant through the voluntary submission of their CV, and in the case of extended storage of the CV, the legitimate interest of the applicant and the Data Controller, until the Data Subject objects to the data processing, that the applicant's material may be taken into consideration for a position that may become available at a later date.

3. Processing of customers' personal data

a) Contact

The Data Subject may contact the Data Controller by email (info@boxelence.hu), , by phone (+36 70 802 7736) or in person (1191 Budapest, Üllői út 200.) in order to discuss the details of the order to be placed.

The data processed are those provided by the Data Subject during the contact.

The Data Controller will only process the data until the contact is completed.

The legal basis for data processing is the voluntary consent of the Data Subject, which is given to the Data Controller upon contact [data processing pursuant to Article 6(1)(a) of the Regulation].

b) Ordering and processing of products

The Data Subject personally orders the manufacture of the Products from the Data Controller by filling out the order form on the Data Controller's website at www.boxelence.hu .

Data processing activities are necessary for the performance of the contract during the processing of orders. During data processing, the Data Controller processes the Data Subject's name, place and date of birth, mother's name, tax identification number, tax number, billing address, e-mail address, telephone number, the characteristics of the ordered product, and the date of the order.

The Data Controller processes the data for five (5) years in accordance with the limitation period specified in the Civil Code.

The legal basis for data processing is the performance of the contract (data processing pursuant to Article 6(1)(b) of the Regulation).

c) Issuing invoices

The data processing is carried out for the purpose of issuing invoices in accordance with the law and fulfilling the obligation to retain accounting documents. Pursuant to Section 169 (1)-(2) of the Accounting Act, business associations must retain accounting documents that directly and indirectly support their bookkeeping.

The Data Controller processes the Data Subject's name, address, tax identification number, billing address, and the e-mail address provided by the Data Subject for receiving electronic invoices in connection with the invoice.

The Data Controller shall retain the data for eight (8) years in accordance with Section 169 (2) of Act C of 2000 on Accounting [data processing pursuant to Article 6 (1) (c) of the Regulation].

The legal basis for data processing is Act CXXVII of 2007 on Value Added Tax and Act C of 2000 on Accounting.

The Data Controller issues e-invoices to its business partners and customers who have consented to receive e-invoices. The purpose of data processing related to e-invoices is the issuance and storage of electronic invoices, and the legal basis for this is, on the one hand, the Data Subject's consent to receive e-invoices and, on the other hand, the applicable laws in force (Act CXXVII of 2007 on Value Added Tax; Decree 23/2014 (VI.30.) NGM, other legislation relating to electronic invoices). The data related to e-invoices originate from the Data Subject, and without this data, the Data Controller cannot issue electronic invoices.

The Data Controller shall store electronically issued invoices for the same period as paper-based invoices, i.e. it shall process and retain them for 8 years from the date of submission of the financial statements, in accordance with the provisions of the Accounting Act.

If the Data Subject withdraws their consent to receive electronic invoices, the Data Controller will not process their data for this purpose in the future.

By ordering the Product or accepting the invoice or the Product, the Data Subject accepts the Data Controller's Data Management Policy and General Terms and Conditions and acknowledges that they are binding on him/her.

d) Exercising warranty and guarantee rights

The data processing is carried out in order to enforce the Data Subject's warranty and guarantee rights.

During data processing, the Data Controller processes the Data Subject's name, e-mail address, telephone number, and the content of the complaint.

The Data Controller shall retain data related to the enforcement of warranty and guarantee rights for five (5) years in accordance with the Consumer Protection Act.

The legal basis for data processing is Act CLV of 1997 on Consumer Protection [data processing pursuant to Article 6(1)(c) of the Regulation].

e) Handling of other consumer protection complaints

The data processing is carried out for the purpose of handling consumer protection complaints.
During data processing, the Data Controller processes the name, email address, telephone number, and content of the complaint of the Data Subject.

The Data Controller shall retain data relating to consumer complaints for five (5) years in accordance with the Consumer Protection Act.

The legal basis for data processing is Act CLV of 1997 on Consumer Protection [data processing pursuant to Article 6(1)(c) of the Regulation].

4. Processing of business partners' personal data

The Data Controller processes the following data in relation to business partners:

- The names and signatures of representatives of customer and supplier partner companies; the contact details of their contact persons and administrators, i.e. their names, telephone numbers and, where applicable, fax numbers; where necessary, their positions and signatures;

- Data required for contracts/invoicing with individual business partners, i.e. their names, addresses/registered offices, tax numbers, registration numbers, bank account numbers, telephone numbers, e-mail addresses, and signatures. With regard to these partners, it processes data relating to orders placed with the partners in question, as well as data on transactions and debts/non-payments.

The Data Controller processes this data for the purpose of facilitating the conclusion of sales contracts, fulfilling them, fulfilling its related contractual obligations, and enforcing its rights.

This includes maintaining contact with customers and suppliers in order to facilitate the establishment of business relationships, answering questions, requesting and submitting offers; contract-related administration, invoicing, shipping, handling complaints; and debt collection.

The Data Controller primarily processes data on the legal basis of the preparation and performance of the contract as set out in the GDPR.

The consent of the Data Subject also provides a legal basis for the Data Controller's data processing, typically in the case of voluntary provision of contact details.

Data processing is also required by law for the Data Controller, primarily in the case of contracts/orders that have already been executed, such as tax laws and accounting laws.

Finally, the legitimate interest of the Data Controller or even a third party may also constitute a legal basis for data processing, typically in the case of data processing for the purpose of enforcing legal rights.

The data processed by the Data Controller about the Data Subject originate from the Data Subject. In the absence of such data, the Data Controller cannot enter into a contract with the Data Subject, except for optional contact details (typically the name and email address of the administrator or contact person, and their telephone number).

Other data relevant to the enforcement of rights shall be processed by the Data Controller until the five-year limitation period for the enforcement of rights under the Civil Code expires. Data processed solely on the basis of the Data Subject's voluntary consent shall be processed by the Data Controller until the purpose ceases to exist or the Data Subject withdraws their consent.

The Data Controller is obliged to retain data entered into our data controller records on the basis of the Infotv. (e.g. data relating to requests for the exercise of the rights of the Data Subject or data relating to data protection incidents) for ten years after the deletion of the processed data.

5. Data processing related to camera recordings

The Data Controller's branch office is under camera surveillance, and a separate camera policy sets out further details of data processing, which you can find out about at the office of the monitored objects or request a copy of at our contact details above.

The Data Controller uses camera recordings to protect human life, physical integrity, property, business, payment, banking, and securities secrets, to track the movement of goods, to effectively investigate complaints, and to prevent and detect violations and accidents, catch perpetrators in the act, and prove violations. The recordings are stored for 3 business days.

The legal basis for our camera-based data processing is the voluntary consent of persons entering the area, which they give by entering the area marked with warning signs, as well as the legitimate interest of the Data Controller, supported by a balancing of interests test.

6. Data processing related to GPS tracking

The Data Controller installs GPS trackers in the vehicles it owns. The data recorded by the GPS tracker is processed for the purposes of efficient organization of work processes, property protection, and personal protection.

The legal basis for the Data Controller's processing of data recorded by GPS trackers is the Data Controller's legitimate interest, supported by a balancing test.

7. Further data processing

If the Data Controller wishes to carry out further data processing, it shall provide the Data Subject with prior information on the essential circumstances of the data processing (legal background and legal basis of the data processing, purpose of the data processing, scope of the data processed, duration of the data processing). The Data Controller shall comply with written requests for data from the authorities based on statutory authorization. The Data Controller shall keep records of data transfers in accordance with Sections 15. The Company records that its products (e.g., mobile applications) and business partners are subject to detailed, separate data processing notices.

The Company notes that detailed, separate data processing information applies to the products it has developed (e.g., mobile applications) and its business partners.

XI. Data processing.

The Data Controller has a contractual obligation with all data processors in accordance with legal requirements, which ensures that personal data is processed exclusively on the basis of the Data Controller's written instructions. Data subjects consent to the transfer of data to all data processors referred to in this section, provided that the conditions detailed above are met.

a) Data processing related to the storage of personal data

Name: **Boxelence Innovation Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság**
Abbreviated name: **Boxelence Innovation Kft.**
Registered office: **4200 Hajdúszoboszló, Rákóczi utca 188.**
Mailing address: **4200 Hajdúszoboszló, Rákóczi utca 188.**
Registering court: **Debrecen Court of Justice, Company Registry**
Company registration number: **Cg.09-09-036512**
Tax number: **32690765-2-09**

Represented by: **László Dános, managing director with independent signing authority**

Ádám Szabó, managing director with independent signing authority

Telephone number:+3670/6354921

Email address: info@boxelence.hu

The data processor stores personal data.

b) Data processing related to accounting

Name of the data processor: **Boxelence Innovation Kft.**
Registered office of the data processor: **4200 Hajdúszoboszló, Rákóczi utca 188.**
Company registration number of the data processor: **Cg.09-09-036512**
Tax number of the data processor: **32690765-2-09**

Boxelence Innovation Kft. performs its own accounting documentation, given that its managing director, Ádám Szabó, has the appropriate training and qualifications. In doing so, it processes the name and address of the data subject to the extent necessary for accounting records, for the period specified in Section 169(2) of the Accounting Act, and then deletes it immediately.

c) Data processing related to online payments

Name of data processor: **OTP Mobil Szolgáltató Korlátolt Felelősségű Társaság**
Registered office of the data processor: **138 Budapest, Váci út 135-139. B. ép. 5. em.**
Data controller's telephone number: **+36(70)366-6611 +36(1)366-6611 +36(20)366-6611**
Data controller's email address: **ugyfelszolgalat@simple.hu; sales@otpmobil.com**
Data controller's website: https://simplepay.hu/

Online credit card and other payment methods are implemented through the system of **OTP Mobil Szolgáltató Korlátolt Felelősségű Társaság** (OTP Mobil Limited Liability Company). Credit card and other payment-related data are not disclosed to the merchant. The service provider, **OTP Mobil Szolgáltató Korlátolt Felelősségű Társaság**, is an institution supervised by the Hungarian National Bank, license number: H-EN-I-1064/ 2013 .

The payment service provider cooperates with the Data Controller in the execution of online payments on the basis of a contract concluded with the Data Controller, for which purpose data is transferred to the online payment service provider during the purchase process. In doing so, the online payment service provider processes the billing name and address of the data subject, as well as the order number and date, in accordance with its own data processing rules. The purpose of the data transfer is to provide the online payment service provider with the transaction data necessary for the payment transaction initiated by the data subject in connection with the purchase. Legal basis for data transfer: pursuant to Article 6(1)(b) of the Regulation, the performance of the contract concluded between you and the Data Controller, which includes payment by the buyer, and in the case of online payment, the data transfer referred to in this section is necessary for the payment.

d) data processing related to the use of the website

Name of the data processor: Sybell Informatikai Korlátolt Felelősségű társaság
Registered office of the data processor: 1138 Budapest, Tomori utca 34. 2nd floor
Company registration number of the data processor: 01 09 293034
Tax number of the data processor: 25859502-2-41

Based on the contract concluded with the Data Controller, the Data Processor shall receive all data sent and received on the backend interface of the www.boxelence.hu website in the form

of server logs, which it shall store on its own server for operation/maintenance purposes. The logs contain personal data received via the contact form (name, email address, telephone number).
Purpose of data processing: To make the Web Store available and to operate it properly. The purpose of recording order data is to process and fulfill the order. Duration of data processing , deadline for data deletion: Data processing lasts until the termination of the agreement between the Data Controller and the hosting provider, or until the data subject's request for deletion addressed to the hosting provider has been processed.

e) Data processing for marketing purposes

Name of the data processor: **Facebook Inc.**
Registered office of the data processor: **1 Hacker Way, Menlo Park, CA 94025**

Based on the contract concluded with the Data Controller, the Data Processor shall receive, in electronic form, the personal data provided by customers for the purpose of conducting prize games in addition to their Facebook registration (postal address, telephone number) for maintenance purposes.

f) Data processing related to newsletter distribution

Name of the data processor: **Google Inc.**
Data processor's registered office: **1600 Amphitheatre Parkway, Mountain View, CA 94043**

Based on a contract concluded with the Data Controller, personal data related to advertisements (name, address, telephone number, email address, credit card number) are transmitted electronically to the Data Processor in the form of logs for administrative purposes (invoicing, advertising cost settlement).

XII. General description of technical and organizational measures related to data security

In order to ensure the secure processing of personal data, the electronic surveillance system is a completely closed system, inaccessible from the outside, inaccessible from the internet, with a strong password-protected user interface, and the video data stream is also encrypted. The cameras communicate with the recording unit via a separate subnetwork within the building, with a direct physical cable connection. Recording only takes place when motion is detected.

This is achieved by means of pictograms placed in the vicinity of the cameras, at the entrance to the monitored premises, brief information notices, and camera regulations available to those concerned (Information on the use of electronic surveillance systems).

Electronic data is stored on password-protected computers. Access to the database is regulated by the Data Controller.

Paper-based documents are stored in a branch office monitored by cameras, in an alarm-protected room, in locked cabinets.

XIII. Applicable legislation

- 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)
- Act CXII of 2011 on the right to self-determination in information and freedom of information (Infotv.);
- Act V of 2013 on the Civil Code (Ptk.);

- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Eker. tv.);
- Act C of 2003 on Electronic Communications (Eht.);
- Act CLV of 1997 on Consumer Protection (Fgytv.);
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers.
- Act CXIX of 1995 on the processing of name and address data for research and direct marketing purposes (Katv.);
- Act XLVIII of 2008 on the basic conditions and certain restrictions of economic advertising activities (Grt.);
- Act CXXXIII of 2005 on the rules governing personal and property protection and private investigation activities (SzVMt.);
- Act CXVII of 1995 on personal income tax (Szja tv.).

B u d a p e s t , 2025.01 .10.

……

Boxelence Innovation Kft.

represented by: László Dános, managing director

Data controller