I. Purpose of the Policy

1. The purpose of this Data Processing Policy (hereinafter: the "Policy") is to define in detail the framework of the data processing activities carried out by the Company, thereby ensuring that the processing of personal data complies in all respects with the applicable legal requirements, in particular the provisions of the GDPR and the Hungarian Information Act (Infotv.).

---

2. A further key purpose of the Policy is to ensure that during data processing the Company:

- respects the privacy of data subjects,
- minimizes risks associated with data processing,
- establishes transparent and controllable data processing practices, and
- documents its data processing procedures in accordance with the principle of accountability.

---

3. The Policy also serves as an internal compliance instrument providing guidance for the lawful processing of personal data.

II. Scope

1. The Policy applies to all data processing activities and processes carried out by the Company, regardless of whether they are performed electronically, on paper, or in any other form. Accordingly, the material scope of the Policy includes all operations during which the Company collects, records, organizes, stores, uses, transfers, makes accessible, modifies, deletes, or otherwise processes personal data.

---

2. The personal scope of the Policy extends to the data controller itself as a business entity, as well as to all persons who carry out data processing activities on behalf of or under the authorization of the data controller.

---

3. The temporal scope of the Policy begins upon its adoption and remains in force until amended or expressly revoked. The Company undertakes to comprehensively review the provisions of this Policy regularly, but at least every two years, in order to determine whether modernization, updating, or alignment with the applicable legal, technological, and organizational environment is necessary, with particular regard to changes in data protection legislation, case law, and the Company's operations.

III. Name and Contact Details of the Data Controller

1. For the purposes of this Policy, the data controller is yesBTL Hungary Korlátolt Felelősségű Társaság(hereinafter: the "Company" or the "Data Controller"), which processes personal data in the course of its economic activities.

---

2. The contact details of the Data Controller are as follows:

- Name: yesBTL Hungary Ltd.
- Registered office: 1044 Budapest, Váci út 83.
- Representative: Gábor András Száler, Managing Director
- Email: info.hu@yesbtl.com
- Phone: +36 1 444 9227

---

3. The Company ensures that Data Subjects may directly contact the Data Controller via the above contact details with any questions, comments, or requests concerning the Policy or the exercise of their rights.

IV. Principles

1. In the course of its operations, the Company processes personal data in accordance with the principles set out in Article 5 of the GDPR.
2. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes ("purpose limitation");

c) adequate, relevant and limited to what is necessary ("data minimization");

d) accurate and, where necessary, kept up to date ("accuracy");

e) kept in a form permitting identification of data subjects for no longer than necessary ("storage limitation");

f) processed in a manner ensuring appropriate security of personal data ("integrity and confidentiality").

3. In addition, the Data Controller is responsible for, and must be able to demonstrate compliance with, these principles ("accountability").

V. Records of Processing Activities

1. The Company maintains an internal data protection register concerning its personal data processing activities, which ensures the transparency, traceability, and enforcement of the principle of accountability under the GDPR.

---

2. The purpose of the register is to clearly document, for each processing operation carried out by the Company, the purpose of processing, legal basis, categories of data subjects, categories of personal data processed, recipients, retention periods, and the technical and organizational measures applied.

---

3. The register is maintained on an ongoing basis in practice, and the Company updates its contents without delay whenever a new data processing process is introduced or an existing process is modified.

---

4. Categories of Data Subjects:

1. B2B contact person data
2. Employees of the Data Controller
3. Image recordings made by the camera system of natural persons physically present in the Data Controller's office premises

---

5. B2B Contact Person Data

A. Categories of Personal Data:

- name
- email address
- telephone number
- job title / position

B. Persons Authorized to Access the Personal Data of Contact Persons:

- processors designated by the Company where strictly necessary for the performance of contracts; and
- employees of the Company where strictly necessary for the performance of their duties.

C. Purpose of Processing:

- for marketing purposes until an order is placed;
- where an order is placed, for the performance of the contract.

D. Legal Basis for Processing:

- for marketing purposes: the legitimate interest of the Data Controller pursuant to Article 6(1)(f) GDPR (supported by the legitimate interest assessment attached as Annex 1 to the Policy);
- after conclusion of a contract: performance of a contract pursuant to Article 6(1)(b) GDPR.

E. Planned Deletion Deadline:

If no order or contract is concluded following the marketing contact, the Company shall delete the personal data within 30 days from the date of the unsuccessful contact attempt. If a business relationship is established following the contact, the Data Controller shall process the data of the Data Subject only for as long as strictly necessary for the performance of the contract.

F. Data Transfers and Recipients:

In practice, outreach and business communications are conducted through the Gmail system, while records of business relationships, status management, and documentation of communication history are maintained in the Salesforce system.

G. Technical and Organizational Measures:

To protect B2B contact person data, the Company applies within both Gmail and Salesforce systems:

- two-factor authentication;
- username and password-based access control;
- role-based access authorization systems.

---

6. Employee Data

A. Categories of Personal Data:

The Data Controller may process the following employee data in personnel records (collectively: personnel file):

- identification data;
- tax and social security data;
- employment-related data;
- payroll data;
- performance evaluations;
- other data required by law.

B. Persons Authorized to Access Employee Personnel Files:

- persons responsible for HR administration and payroll processing, where strictly necessary for the performance of their duties;
- service providers acting as processors and providing payroll, accounting, auditing, legal, or tax advisory services to the Company, where necessary in scope and duration;
- executive officers of the Data Controller, where necessary in scope and duration;
- courts, prosecutors, investigative authorities, or other competent authorities upon official request, to the extent requested.

C. Purpose of Processing:

Establishment, maintenance, and termination of employment relationships.

D. Legal Basis for Processing:

Performance of a contract pursuant to Article 6(1)(b) GDPR.

E. Planned Deletion Deadline:

The Company processes employment-related data for the retention periods required by law, which may continue for certain documents even after termination of employment.

F. Data Transfers and Recipients:

Employee data may only be transferred to recipients specified by law, in particular accounting, payroll, and public authorities, to the necessary and proportionate extent.

G. Organizational and Technical Measures:

In practice, employee data is stored partly in paper form and partly on a local server not capable of external network communication. Paper documents are stored in locked cabinets accessible by key only.

---

7. Camera Recordings of Natural Persons Present in the Data Controller's Office Premises

(1 camera installed in the office premises)

A. Categories of Personal Data:

- video recordings of persons entering or present in the office premises;
- date and time of recording.

B. Persons Authorized to Access the Personal Data:

- the Managing Director of the Company;
- a person expressly authorized by the Managing Director, to the extent strictly necessary for asset protection purposes;
- authorities, courts, or police upon official request;
- external security or IT service providers, solely to the extent necessary for system operation, acting as processors.

C. Purpose of Processing:

Protection of the office premises rented by the Company, the assets located therein, IT devices, documents, and trade secrets, as well as prevention and subsequent investigation of unlawful acts, unauthorized entry, damage, and offences against property.

D. Legal Basis for Processing:

The legitimate interest of the Data Controller pursuant to Article 6(1)(f) GDPR, supported by the legitimate interest assessment attached as Annex 2 to the Policy.

E. Planned Deletion Deadline:

Recordings are retained by the Company for 30 days and then automatically deleted, unless the recording serves as evidence in relation to an incident, authority procedure, or legal dispute, in which case retention may be extended until the final conclusion of the relevant proceeding.

F. Data Transfers and Recipients:

Recordings may only be transferred to third parties where required by law, upon official request by an authority, or for the enforcement of legal claims, particularly to the police, courts, or other authorities.

G. Technical and Organizational Measures:

- access to the camera system is protected by password authentication, and recordings may only be accessed by authorized persons;
- access logs are maintained and traceable;
- the camera monitors only the office entrance and areas necessary for the protection of assets;
- the camera is not directed at areas where enhanced privacy protection is justified;
- the monitored area is marked with clearly visible information signage.

VI. Rights of Data Subjects

1. In accordance with the applicable legal requirements, the Company supports the exercise of the rights of persons affected by data processing. Accordingly, data subjects may contact the Company for the purpose of exercising the following rights:

A. Right to Information (Articles 13 and 14 GDPR)

The data subject has the right to know:

a. what personal data is processed about them;
b. for what purpose and on what legal basis such data is processed;
c. who receives the data.

B. Right of Access (Article 15 GDPR)

a. the data subject may request confirmation regarding whether their personal data is being processed; and
b. may request a copy of their personal data.

C. Right to Rectification (Article 16 GDPR)

a. the data subject may request the correction of inaccurate or incomplete data.

D. Right to Erasure – "Right to be Forgotten" (Article 17 GDPR)

a. the data subject may request deletion of personal data (for example, if the purpose has ceased or consent has been withdrawn).

E. Right to Restriction of Processing (Article 18 GDPR)

a. the data subject may request that the data be stored only and not otherwise used.

F. Right to Data Portability (Article 20 GDPR)

a. the data subject may receive the data in a structured, commonly used, machine-readable format;
b. may transmit such data to another service provider.

G. Right to Object (Article 21 GDPR)

a. the data subject may object to processing based on legitimate interest;
b. may object to direct marketing processing (in practice, this right generally always applies).

H. Rights Related to Automated Decision-Making (Article 22 GDPR)

a. the data subject may request human intervention;
b. shall not be subject solely to automated decision-making, subject to applicable exceptions.

VII. Enforcement of Data Subject Rights

1. The Company ensures that data subjects are able to effectively and genuinely exercise their rights in connection with the processing of their personal data. For this purpose, the Company applies a transparent, documented procedure compliant with applicable laws for handling incoming requests. Each request is assessed individually, taking into account the circumstances of the specific case, applicable legal provisions, and the principle of accountability.

---

2. Upon receipt of a data subject request, the Company shall begin processing it without undue delay and shall in all cases seek to inform the data subject of the outcome as soon as reasonably possible. Accordingly, the Company shall provide information on measures taken in response to the request no later than one month from receipt of the request. Where the request is submitted electronically, the response shall also, as a general rule, be provided electronically, unless the data subject requests another form of communication.

---

3. Where the Company does not take action in response to a request, it shall inform the data subject without delay, and no later than one month from receipt of the request, of the reasons for not taking action. In such notice, the Company shall also inform the data subject of their right to lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH) and of their right to seek a judicial remedy.

---

4. If a question of legal interpretation arises during the assessment of a request, or if the matter is not clear, the Company shall obtain an expert opinion from its appointed data protection lawyer in order to ensure that the decision fully complies with applicable legal requirements.

---

5. The Company shall in all cases ensure that the handling of data subject requests is properly documented, traceable, and auditable.

---

6. Responsibility for implementing this procedure and handling data subject requests rests with the Managing Director of the Company.

VIII. Security of Personal Data

1. The Company shall ensure the following:

A. Preventive Security

Within the scope of preventive security, the Company continuously strives to minimize potential risks already during the design of its data processing operations, taking into account the GDPR principle of "data protection by design and by default." For this purpose, the Company applies procedures and control mechanisms aimed at preventing personal data breaches.

B. Detection and Management of Incidents

With regard to the detection and handling of incidents, the Company establishes operational procedures that enable the timely identification, investigation, and proper management of potential personal data breaches. In this framework, the Company ensures that relevant persons are aware of how to identify and report incidents, as well as what steps must be taken in order to mitigate possible harm.

C. Restorative Security

Within the scope of restorative security, following each incident or security risk event, the Company analyzes the circumstances of the event and takes the necessary measures to prevent similar future occurrences and to further strengthen the security level of its data processing operations.

---

2. Technical Measures

The Company has implemented multi-layered technical measures to ensure the security of personal data:

1. device security (hard drive encryption);
2. access protection (username + password);
3. two-factor authentication (2FA);
4. role-based access control.

Accordingly, the Company provides multi-step protection for access to its IT systems, in particular:

- Gmail email system;
- Salesforce customer relationship management system;
- local server infrastructure.

3.The hard drives of the IT devices used by the Company operate in encrypted form, ensuring that in the event of physical loss or unauthorized acquisition of a device, the personal data stored on it cannot be directly accessed.

---

4. Access to the Company's IT systems is in all cases tied to unique username and password credentials. User identifiers are assigned individually to specific persons, thereby ensuring clear traceability of access and accountability for actions performed. The Company applies strong password requirements, particularly with regard to adequate length and complexity.

---

5. In addition, the Company applies two-factor authentication (2FA) when accessing systems processing personal data. Accordingly, login is not performed solely by entering a username and password, but also requires an additional authentication step, particularly approval sent to a mobile device, a code generated by an authentication application, or another secondary identification method. The purpose of this measure is to significantly reduce the risk of unauthorized access even where a password has been compromised.

---

6. The Company continuously monitors and regularly reviews access rights and ensures that personal data may only be accessed by persons for whom such access is strictly necessary for the performance of their job duties. Rights are modified or revoked without delay whenever authorization related to data processing ceases or changes.

---

7. Organizational Measures

Considering the Company's current organizational structure, decisions, supervisory responsibilities, and compliance measures relating to personal data processing fall centrally within the competence of the Managing Director.

Given that the Company currently employs only one employee (the Managing Director), the establishment of separate internal roles such as a dedicated data protection officer, separate compliance function, or internal privacy officer is currently feasible only to a limited extent. Accordingly, operational and strategic decisions relating to data processing are made by the Managing Director, with the involvement of an external privacy lawyer or expert where necessary.

The Company further undertakes that if its organizational structure expands, internal data protection tasks and responsibilities shall be reviewed again.

Beyond the above, the Company continuously seeks to improve its data security measures and align them with technological developments, thereby ensuring that its data processing practices remain compliant with applicable legal requirements and industry expectations at all times.

IX. Management of Personal Data Breaches

1. If the Company detects a personal data breach concerning personal data processed by it — meaning unlawful processing or handling of personal data, including in particular unauthorized access, alteration, transmission, disclosure, deletion, destruction, accidental loss, or damage — it shall immediately begin investigating the case.

During the investigation, the Company shall identify the circumstances, timing, cause, and course of the breach, and shall assess:

- the nature of the infringement;
- the categories and scope of personal data potentially or actually affected;
- the number and categories of affected individuals;
- risks and possible consequences for the rights and freedoms of data subjects.

The Company shall also document measures taken and planned, and shall implement all technical, organizational, and legal steps necessary to mitigate damage, prevent further infringements, and comply with legal obligations.

---

2. Once the Company becomes aware of a personal data breach, it shall notify the Hungarian supervisory authority, the National Authority for Data Protection and Freedom of Information (NAIH), without undue delay and, where feasible, no later than 72 hours thereafter, unless it can demonstrate in accordance with the principle of accountability that the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

---

3. Where notification cannot be made within 72 hours, the reasons for the delay shall be stated in the notification, and the required information may be provided in phases without further undue delay.

The notification shall include:

- the nature of the personal data breach, including where possible the categories and approximate number of affected data subjects, and categories and approximate number of personal data records concerned;
- the name and contact details of a contact point for further information;
- the likely consequences of the breach;
- measures taken or proposed to remedy the breach, including mitigation of possible adverse effects.

---

4. Informing the Data Subject About the Breach

Where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall inform the data subject without undue delay.

The communication shall include:

- the name and contact details of a contact point for further information;
- the likely consequences of the breach;
- measures taken or proposed to remedy the breach, including mitigation of possible adverse effects.

---

5. Remedial Measures and Mitigation

Following discovery of a breach, an immediate action plan shall be prepared for the implementation of appropriate technical and organizational protective measures, with the involvement of external experts where necessary.

The employee responsible for data protection shall maintain a register of breaches containing at least:

- categories of personal data concerned;
- categories and number of affected persons;
- date of the breach;
- circumstances and effects of the breach;
- measures taken to remedy the breach;
- any additional data required by applicable law.

X. Profiling

1. The Company does not carry out profiling activities during the processing of personal data.

Accordingly, the Company does not use personal data relating to data subjects for automated processing operations intended to analyze, evaluate, or predict personal characteristics, economic situation, professional interests, reliability, behavior, or preferences of data subjects.

---

2. The Company's data processing practices are limited exclusively to the fulfillment of specific, predefined business and administrative purposes, in particular:

- communication;
- marketing outreach;
- performance of contractual obligations.

The Company does not apply automated decision-making or segmentation procedures resulting in individual evaluation or categorization based on personal characteristics of data subjects.

---

3. Accordingly, the Company ensures that personal data is processed solely in accordance with the principles of purpose limitation and data minimization, and that the processing neither directly nor indirectly results in profiling within the meaning of Article 4(4) GDPR.

XI. Data Processors

1. During certain data processing activities, for the purposes of efficient operation and the performance of contractual obligations, the Company engages data processors that carry out specified processing operations on behalf of and under the instructions of the Company. The Company ensures in all cases that data processors are selected with due care and provide adequate guarantees regarding compliance with applicable legal requirements governing the processing of personal data, including compliance with the GDPR.

---

2. The Company enters into a written agreement with each data processor, which regulates in detail the subject matter, duration, nature, and purpose of the processing, the types of personal data processed, and the categories of data subjects, and also records the rights and obligations of the processor. Data processors are authorized to act solely on the basis of the documented instructions of the Company and are not entitled to use personal data for their own purposes.

---

3. Data Processors Engaged by the Company Include in Particular:

- Google Ireland Limited
Gordon House, Barrow Street, Dublin 4, Ireland
Services: Gmail email system, document storage, communication
- Salesforce, Inc.
415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA
Services: CRM system, business relationship records, status management, contact history
- DHL Supply Chain Magyarország Kft.
2225 Üllő, Zöldmező út 2.
Services: warehouse logistics services
- the current accounting service provider
Services: accounting services

4. The Company ensures that data processors may access personal data only to the extent strictly necessary for the performance of their duties and are required to implement appropriate technical and organizational measures to guarantee data security.

5.The Company regularly monitors the activities of data processors and verifies that they carry out processing in accordance with legal requirements and contractual obligations. If any risk arises in connection with the activities of a data processor, the Company is entitled and obliged to take the necessary measures, including amendment or termination of the contract.

6.The Company further ensures that where a data processor intends to engage a further processor (sub-processor), it may do so only with the prior written authorization of the Company, and the same data protection obligations shall apply to the sub-processor as to the original processor.

7.The Company takes all necessary measures to ensure that the engagement of data processors does not result in any reduction in the security of personal data, and that the protection of data subject rights and the lawful and secure processing of personal data are ensured at every stage of the processing operations.

XII. International Data Transfers

1. When using certain data processors engaged by the Company — in particular Google Ireland Limited, DHL Supply Chain Magyarország Kft., and Salesforce, Inc. — it may occur that personal data is processed or stored in a country outside the European Economic Area (EEA), in particular in the United States of America.

The Company ensures that all such transfers take place only with safeguards compliant with Chapter V of the GDPR.

A. Google Ireland Limited

When using Google services, the processing of personal data is governed by the Cloud Data Processing Addendum (CDPA) provided by Google, which forms part of Google's contractual framework or becomes applicable by separate acceptance.

The CDPA contains contractual safeguards regarding personal data processing, security, incident management, and international data transfers.

Where personal data is transferred outside the EEA, Google ensures the lawfulness of such transfers through the use of Standard Contractual Clauses (SCCs) adopted by the European Commission. The SCCs form part of Google's CDPA.

B. DHL Supply Chain Magyarország Kft.

The logistics and warehousing provider engaged by the Company, DHL Supply Chain Magyarország Kft., may use systems and infrastructure within the DHL group in the course of service performance.

Accordingly, personal data may be transferred to DHL group companies or sub-processors located outside the EEA.

The Company ensures that such transfers take place only with safeguards compliant with Chapter V of the GDPR, in particular on the basis of Binding Corporate Rules (BCRs) applied by the DHL group.

C. Salesforce Inc.

In the case of the Salesforce system, the Data Processing Addendum (DPA) sets out in detail the obligations of Salesforce as processor, security measures, incident management, and the conditions of data transfers.

For international transfers, Salesforce applies SCCs adopted by the European Commission and, for certain services, additional contractual and technical safeguards.

XIII. Remedies and Complaint Forum

1.The Company ensures that data subjects have access to effective remedies where their rights relating to the processing of personal data are infringed. Accordingly, a data subject is entitled to lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH) if, in their view, their personal data has been processed in breach of applicable legal requirements, in particular the provisions of the General Data Protection Regulation (GDPR).

---

2. Contact Details of NAIH:

- Registered office: 1055 Budapest, Falk Miksa utca 9–11.
- Postal address: 1363 Budapest, P.O. Box 9
- Phone: +36 (1) 391-1400
- Email: ugyfelszolgalat@naih.hu
- Website: www.naih.hu

3.The data subject may also bring proceedings before a competent court if, in their view, they have suffered a legal infringement in connection with the processing of their personal data.

4.In every response to a data subject request, the Company shall clearly inform the data subject of the remedies available to them, including the possibility of filing a supervisory complaint and seeking judicial enforcement.

XIV. Data Protection Officer

1. Pursuant to Article 37 GDPR, the Company has examined whether it is required to appoint a Data Protection Officer.

As a result of that assessment, the Company has determined that, based on its current processing activities, the appointment of a Data Protection Officer is not mandatory, since:

- the Company is not a public authority or body exercising official authority;
- its core activities do not consist of regular and systematic monitoring of data subjects on a large scale; and
- it does not process large quantities of special categories of personal data or criminal data.

---

2. The Company nevertheless ensures that data protection compliance remains under continuous supervision and, where necessary, secures compliance with applicable legal requirements through the involvement of an external privacy expert or privacy lawyer.

The Company further undertakes to reassess the necessity of appointing a Data Protection Officer if the scope or nature of its processing activities changes.

XV. Final Provisions and Change Log

1. The effective date of this Policy is **30 March 2026.**
2. Change Log:

Version	Effective date	Main changes
1.0	30 March 2026	first version

LEGITIMATE INTEREST ASSESSMENT

Legal Basis: Legitimate interest (Article 6(1)(f) GDPR)
Purpose of Processing: Business (B2B) marketing activities

---

1. Identification of the Legitimate Interest of the Controller

The Company has a legitimate interest in carrying out active business development and marketing activities for the purpose of maintaining, developing, and expanding its economic activities. Within this framework, the Company contacts potential business partners and strengthens and expands existing business relationships.

Such activities particularly include:

- sending targeted business offers;
- contacting potential B2B clients;
- presenting services;
- initiating and preparing business cooperation opportunities.

In the Company's view, marketing activity is a necessary and essential part of the operation of commercial undertakings, without which market presence and competitiveness cannot be maintained. Accordingly, the Company's legitimate economic interest is directly connected to its core business activity and constitutes a lawful and generally accepted business practice.

---

2. Assessment of Necessity and Proportionality

The Company has examined whether the processing of personal data is necessary and proportionate for achieving the above purpose and has reached the following conclusions:

Due to the specific nature of the B2B business environment, business communication is in all cases linked to specific natural person contact persons; therefore, processing necessarily involves certain personal data.

For the effective implementation of marketing activities, it is essential to process the following data:

- name;
- email address;
- telephone number;
- position/title.

The Company has determined that:

- the scope of data is the narrowest possible and complies with the principle of data minimization;
- the purpose cannot be achieved by a less data-intensive method;
- the processing does not involve special category data;

- the processing does not involve automated decision-making or profiling.

The Company further ensures that processing is limited in time: where the marketing approach does not lead to a business relationship, the data shall be deleted no later than 30 days after the unsuccessful contact attempt.

Based on the above, the Company concludes that the processing is necessary and proportionate for achieving the intended purpose.

---

3. Assessment of the Interests, Rights, and Reasonable Expectations of Data Subjects

The affected data subjects are contact persons of companies and sole traders acting in their professional capacity and not as private individuals.

In the Company's view, such data subjects may reasonably expect that:

- publicly available business contact details may be used for business-related approaches;
- other market participants may contact them for the purpose of offering services;
- their data is processed in connection with their professional role.

Based on the nature of the processing, it may be established that:

- the processing does not affect the private sphere of the data subjects;
- the processing is limited in scope and low in intensity;
- the processing does not entail significant risk to the rights and freedoms of data subjects.

---

4. Balancing Test

The Company has balanced:

- its own legitimate economic interests; and
- the rights and interests of data subjects regarding the protection of personal data.

The Company's legitimate interests are:

- maintaining and developing its business activity;
- acquiring new clients;
- strengthening its market presence.

The interests of data subjects are:

- protection of privacy;
- minimization of unwanted approaches.

During the balancing exercise, the Company gave particular weight to the fact that:

- the processing takes place exclusively in a B2B environment;

- data subjects are approached in their business capacity;
- the scope of data processed is narrowly limited;
- the processing is short in duration;
- appropriate safeguards are provided (right to object);
- according to Recital 47 GDPR, direct marketing may constitute a legitimate interest.

Based on the above, the Company concludes that any potential adverse impact arising from the processing does not override the weight of the Company's legitimate interest. Therefore, reliance on legitimate interest as the legal basis is justified.

---

5. Safeguards and Protective Measures

During direct marketing and business acquisition communications, the Company ensures that the data subject can exercise the right to object easily, directly, and free of charge.

The data subject is entitled to object at any time to the processing of personal data for direct marketing purposes without the need to provide justification. Objections may be submitted in particular:

- by email;
- by telephone;
- in writing;
- through any contact channel indicated in the communication.

Following receipt of the objection, the Company shall immediately delete the personal data used for direct marketing purposes and terminate such processing.

Data affected by the objection shall not be used in the future for marketing purposes, and no further business or advertising communications may be sent to the data subject.

In addition, the Company applies the following measures:

- informs the data subject of the right to object in every marketing communication;
- strictly limits the duration of processing;
- processes only relevant and necessary data;
- restricts access to data;
- uses secure IT systems, in particular Salesforce, Inc. and Google Ireland Limited systems;
- regularly reviews its processing practices.

These safeguards collectively ensure compliance with the requirements of necessity and proportionality.

---

6. Conclusion

Based on this legitimate interest assessment, the Company determines that marketing-related data processing complies with applicable legal requirements, particularly the conditions for relying on legitimate interest as a lawful basis.

The Company concludes that:

- the purpose of processing is legitimate and lawful;
- the processing is necessary and proportionate;
- the rights and freedoms of data subjects are not disproportionately affected;
- appropriate safeguards have been implemented.

Accordingly, the Company is entitled to process personal data for marketing purposes on the basis of legitimate interest.

LEGITIMATE INTEREST ASSESSMENT

Legal Basis: Legitimate interest (Article 6(1)(f) GDPR)
Purpose of Processing: Operation of 1 camera in the office premises rented by the Company for asset protection purposes

---

1. Identification of the Legitimate Interest of the Controller

The Company has a legitimate interest in ensuring appropriate protection of the assets located in the rented office premises, including IT equipment, business documents, contracts, and confidential business information.

This legitimate interest particularly extends to:

- physical protection of the office premises;
- protection of equipment and documents located therein;
- prevention of unauthorized entry;
- prevention of theft, vandalism, or other unlawful acts;
- retrospective investigation of incidents;
- securing evidence for possible authority or court proceedings.

Asset protection is recognized as a legitimate interest under GDPR principles and the practice of the National Authority for Data Protection and Freedom of Information (NAIH).

---

2. Assessment of Necessity and Proportionality

The Company examined whether CCTV monitoring is necessary and proportionate for achieving the intended purpose.

The Company established that the office contains assets whose loss, theft, or damage could result in significant economic harm.

Camera monitoring is necessary because:

- purely mechanical protection (locks, alarms) does not allow retrospective reconstruction of events;
- identification of perpetrators may be necessary in the event of an incident;
- recordings may serve as evidence;
- cameras have a preventive deterrent effect.

The Company also considered less intrusive means but concluded that access-control or alarm systems alone do not ensure the same level of asset protection.

The monitoring is proportionate because:

- only 1 camera is used;
- the camera monitors only the office entrance and the necessary internal area;

- no continuous employee performance monitoring takes place;
- the retention period is short;
- access is strictly restricted.

---

3. Assessment of the Interests, Rights, and Reasonable Expectations of Data Subjects

The affected persons include:

- employees of the Company;
- contractual partners;
- other visitors.

They may reasonably expect that cameras operate in a business office environment for asset protection purposes, especially near entrances.

The Company ensures that:

- the existence of monitoring is indicated in advance by clearly visible signage;
- a detailed privacy notice is available;
- the camera does not monitor changing rooms, washrooms, or rest areas;
- the camera is not directed at direct supervision of work performance.

---

4. Balancing Test

The Company balanced:

- its legitimate economic interests in asset protection and evidentiary capability; and
- the rights of affected persons to privacy and protection of personal data.

Particular account was taken of the fact that:

- monitoring takes place in a business environment;
- the number of cameras is minimal;
- the monitored area is narrow in scope;
- the retention period is short;
- access is restricted.

Accordingly, the limitation on data subject rights is not disproportionate and does not override the Company's legitimate interest.

---

5. Safeguards and Protective Measures

The Company applies the following safeguards:

- clearly visible CCTV warning signs;

- separate privacy notice;
- maximum retention period of 10 working days;
- password-protected access;
- documentation of access events;
- documented transfers in case of authority requests;
- separate incident register where necessary.

---

6. Conclusion

Based on this legitimate interest assessment, the Company determines that:

- the purpose of processing is legitimate and lawful;
- the processing is necessary;
- the processing is proportionate;
- the rights of data subjects are not disproportionately affected;
- appropriate safeguards are in place.

Accordingly, the Company is entitled to operate CCTV monitoring on the basis of legitimate interest pursuant to Article 6(1)(f) GDPR.