CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Table of Contents

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

INTRODUCTION

This Privacy Policy ("Policy") applies to the data processing and data handling activities of the following company:

The purpose of this Policy is to outline the fundamental rules regarding the handling and protection of personal data, as well as the rules on the free flow of personal data with respect to cases arising during the company's operations. Additionally, this Policy summarizes the company's internal data protection procedures.

The company commits to implementing technical and organizational measures when determining the method of data processing and throughout the data processing, aimed at adhering to data protection principles and protecting the rights of data subjects. Furthermore, the company undertakes only to process personal data that is essential for achieving the specific purpose of the data processing.

Company Name: CLAIR & CURTIS COMMUNICATION
Consultancy Limited Liability Company ("Company")

Company Registered Office: Budapest, Bécsi út 68-84, 1034
Company Registration Number: 01-09-882705
Company Tax Number: 13974787-2-41
Managing Director of the Company: Éva Magdolna Simon-Tábori, CEO

Company Personnel Responsible for Data Management:
Éva Magdolna Simon-Tábori

Company Activities:
The main activity of the company, as registered in the company registry, is advertising agency services. The company primarily engages in event organization, the organization and execution of sweepstakes, lotteries, promotions, the design, editing, and production of publications, public relations activities (PR), corporate social responsibility (CSR) activities, and their execution.

The company ensures that its representatives, employees, and any other persons acting on behalf of and/or in the name of the company are aware of and comply with the provisions of this Policy.

The company commits, where necessary, to inform its business partners about the contents of this Policy, and prior to transferring any personal data, will ensure that its business partners maintain a data protection standard equivalent to the one outlined in this Policy and guarantee the same level of data security as the company.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The company will comply with the provisions of this Policy and the relevant laws in all of its data handling and processing activities, with particular regard to the following laws:

- (I) The Fundamental Law of Hungary ("Fundamental Law");
- (II) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR");
- (III) Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("Infotv.");
- (IV) Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation Activities ("Szvtv.").

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

GLOSSARY OF TERMS

Data Processor: A natural or legal person, public authority, agency, or any other body that processes Personal Data on behalf of the Data Controller.

Data Processing: Any operation or set of operations performed on Personal Data or sets of Personal Data, whether by automated or non-automated means, 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.

Restriction of Data Processing: The marking of stored Personal Data with the aim of limiting their processing in the future.

Data Controller: A natural or legal person, public authority, agency, or any other body that, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for its designation may be provided for by Union or Member State law.

Data Protection Incident: 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.

Pseudonymization: The processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Data Subject's Consent: A freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of Personal Data relating to them.

Identifiable Natural Person: A natural person 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.

Recipient: A natural or legal person, public authority, agency, or any other body to which Personal Data are disclosed, whether a third party or not. However, 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.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Data Subject: Any identified or identifiable natural person who can be identified based on any information.

Third Party: A natural or legal person, public authority, agency, or any body other than the Data Subject, the Data Controller, the Data Processor, and persons who, under the direct authority of the Data Controller or Data Processor, are authorized to process Personal Data.

Special Data: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

- (a) **Genetic Data**: Personal Data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and that result, in particular, from an analysis of a biological sample from the natural person in question.
- (b) **Biometric Data**: Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data (fingerprints).
- (c) **Health Data**: Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status.

Profiling: Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

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.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

POLICY

1. Handling of Personal Data

1.1 Personal Data

Personal Data refers to any information relating to an identified or identifiable natural person.

An identifiable natural person is one who can be identified, directly or indirectly, especially by reference to an identifier such as a name, identification number, location data, online identifier, or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal Data includes, but is not limited to, a person's name, address, place, and date of birth, as well as their image or any sound recording of their voice.

1.2 Data Processing

Data Processing refers to any operation or set of operations performed on Personal Data, either by automated or non-automated means. Data Processing includes the collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction of Personal Data.

Data Processing includes, but is not limited to, the recording and storage of employee data, the collection of contact details of contractual partners in a database, and the storing of names and email addresses in a database for the purpose of sending newsletters.

1.3 Detailed records of Personal Data processing are contained in Appendix 2 of this Policy.

2. Handling of Special Data

2.1 Special Data

Special Data represents a special category of Personal Data. Special Data includes the following types of Personal Data:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.
- Genetic and biometric data used to uniquely identify a natural person.
- Health data.
- Data related to a natural person's sex life or sexual orientation.

Special Data includes, but is not limited to, information on an employee's pregnancy, medical certificates regarding sick leave, or fingerprint data stored in an access control system.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

2.2 Processing of Special Data
Processing of Special Data is prohibited!

However, the prohibition on processing Special Data does not apply in the following cases:

- If the Data Subject has given explicit consent for the processing of their Special Data (even with explicit consent, Special Data may not be processed if Union or Member State law prohibits it).
- If processing is necessary for the performance of obligations and the exercise of specific rights of the Data Controller or the Data Subject in the field of employment, social security, or social protection law.
- If processing is necessary to protect the vital interests of the Data Subject or another natural person, and the Data Subject is physically or legally incapable of giving consent.
- If processing is carried out within the legitimate activities of a foundation, association, or any other non-profit body with political, philosophical, religious, or trade union purposes, provided that:
    - (i) the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes, and
    - (ii) the Personal Data is not disclosed outside the body without the consent of the Data Subjects.
- If the Data Subject has made their Special Data public.
- If processing is necessary for the establishment, exercise, or defense of legal claims, or when courts are acting in their judicial capacity.
- If processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law, which is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject.
- If processing is necessary for preventive or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care, or treatment, or for the management of health or social care systems and services, on the basis of Union or Member State law, or pursuant to a contract with a health professional.
- If processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border health threats or ensuring high standards of quality and safety of healthcare, medicinal products, or medical devices.
- If processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, which are proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the rights and freedoms of the Data Subject.

2.3 The Company processes Special Data necessary for the employment of its employees.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

2.4 Information regarding the processing of Special Data is contained in Appendix 2 of this Policy.

3. Data Processing Activities

3.1 A Data Processor is a natural or legal person, public authority, agency, or any other body that processes Personal Data on behalf of the Data Controller.

Examples of Data Processors include external contractors performing payroll activities for the Company's employees, the Company's IT system administrator, or the web hosting provider for the Company's website, as well as third parties sending newsletters on behalf of the Company.

3.2 The contract for data processing must be in writing. A data processor cannot be entrusted with processing personal data if it has any interest in using the personal data in its own business activities.

The data processing contract must include, at a minimum, the following provisions:

- (a) The Data Processor will process Personal Data only on documented instructions from the Data Controller, including with regard to the transfer of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law.
- (b) The Data Processor ensures that persons authorized to process Personal Data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) The Data Processor takes appropriate measures to ensure the security of data processing.
- (d) The Data Processor respects the conditions referred to regarding engaging another processor.
- (e) The Data Processor assists the Data Controller, where possible, by appropriate technical and organizational measures, in fulfilling the Data Controller's obligation to respond to requests for exercising the Data Subject's rights.
- (f) The Data Processor assists the Data Controller in ensuring compliance with data security obligations, data protection incident notifications, data protection impact assessments, and prior consultations, considering the nature of processing and the information available to the processor.
- (g) Upon completion of the data processing services, the Data Processor will, at the choice of the Data Controller, delete or return all Personal Data and delete existing copies unless Union or Member State law requires the storage of such data.
- (h) The Data Processor will make available to the Data Controller all information necessary to demonstrate compliance with the obligations and will allow for audits and inspections by the Data Controller or another auditor.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

4. Principles of Personal Data Handling

4.1 Lawfulness, Fairness, and Transparency

Personal Data must be processed lawfully, fairly, and in a transparent manner for the Data Subject.

The Company processes Personal Data lawfully if the processing is based on an appropriate legal basis. For instance, if the Company processes Personal Data necessary for the performance of a contract, the processing is lawful when the legal basis is the performance of the contract. However, the processing would not be lawful in such a case if it were based on the consent of the Data Subject instead of the contract.

The Company processes Personal Data fairly if it adheres to the rules of moral fairness and respects human dignity during the processing. The principle of fairness sets limits on data processing activities, taking into account that the Data Subject is not merely an object but a subject of the data processing. Therefore, the Company must not mislead the Data Subject during data processing, nor can it issue misleading information materials.

The Company processes Personal Data transparently if it fully informs the Data Subject about the data processing before it begins and at regular intervals during the processing. The Company must inform the Data Subject of their rights and the risks, rules, and guarantees associated with the processing and ensure that the Data Subject has control over their Personal Data within the bounds of the law. The transparency of data processing is ensured when the Company informs the Data Subject about any changes to the processing—considering the potential impact of these changes on the Data Subject—in a timely manner.

The principle of transparency also requires that the Company properly documents all data processing-related measures. The Company provides repeated information to Data Subjects at appropriate intervals to ensure that they are aware of the processing of their Personal Data.

The Company meets the requirements of transparency if, during communication with Data Subjects (including communication related to the exercise of rights and Data Protection Incidents), it considers the following aspects:

- Conciseness, transparency, comprehensibility, and accessibility;
- Clear and plain language;
- Written communication, or where appropriate, communication in another suitable form, and, upon request, oral communication.

The form of communication is not specified by the GDPR; to meet the transparency requirements, information may be provided in various ways depending on the circumstances, including:

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- Multi-level electronic information (for example, providing brief information via a pop-up window when requesting certain personal data, and more detailed information in the privacy notice);
- Pop-up windows providing information electronically;
- Offering an interface allowing the Data Subject to manage Personal Data processing;
- Paper-based information;
- Information via pre-recorded phone messages;
- Face-to-face communication;
- Standardized icons for information purposes.

4.2 Purpose Limitation

The Company may only process Personal Data for specified, explicit, and legitimate purposes. The Company may not process Personal Data for any purpose incompatible with the original purpose for which the data was collected. Furthermore, the Company may not process Personal Data without a defined purpose or for future undefined uses.

The Company clearly defines the purpose of data processing in compliance with the law before starting the processing and ensures that the purpose is neither too narrow nor too broad. The Company informs the Data Subjects of the purpose of the data processing to enable them to make informed decisions.

To comply with the purpose limitation principle, the Company considers, documents, and takes the necessary steps to ensure proper data handling.

If the Company processes the same Personal Data for multiple unrelated purposes, each data processing purpose must comply with this principle. For example, unrelated purposes could include registering for a sweepstake and subsequently sending a newsletter to the Data Subject.

4.3 Data Minimization

The Company processes only the Personal Data that is adequate, relevant, and limited to what is necessary for the specific purpose of the data processing.

For every data processing activity, the Company evaluates whether the goal could be achieved in another way that is less invasive of privacy. From the planning phase of data processing, the Company considers whether the Personal Data to be processed is necessary and proportional to the specific purpose and whether there are any other means to achieve the goal.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

4.4 Accuracy
The Company ensures that Personal Data is accurate, complete, and—where necessary—kept up to date. The Company takes reasonable steps to ensure that inaccurate Personal Data, in relation to the purpose for which it is processed, is erased or rectified without delay.

The Company takes all reasonable measures to ensure that databases containing personal or contact information are accurate. This includes regularly reviewing and updating data as needed.

4.5 Storage Limitation
Personal Data must be kept in a form that allows identification of the Data Subject only for as long as is necessary for the purposes for which the data is processed.

The Company maintains a list specifying the storage period for each category of Personal Data, monitoring the deletion timelines. The list is regularly reviewed, and once the purpose for processing is fulfilled or the set storage period expires, the Personal Data is deleted. The deletion is documented in writing.

4.6 Integrity and Confidentiality
The Company implements technical and organizational measures to ensure the security of Personal Data and protect it against unauthorized or unlawful processing, accidental loss, destruction, or damage.

The Company ensures that only authorized personnel within the organization have access to Personal Data, and that third parties cannot access the data without proper authorization.

To guarantee the confidentiality of Personal Data, the Company assesses the risks arising from the nature of the processing and implements measures to mitigate these risks. Data protection safeguards are integrated into the systems used for processing from the earliest design stages, considering the state of technology, the risks associated with the data, and the costs of implementing such protections. In case of a data protection incident, the Company ensures that Personal Data can be restored in a timely manner.

4.7 Accountability
The Company is responsible for ensuring compliance with all of the above principles. Additionally, the Company is accountable for demonstrating compliance with these principles. The Company is liable for the implementation of data protection principles.

To demonstrate compliance, the Company undertakes the following actions, among others:

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- Preparing a written privacy policy;
- Creating privacy notices;
- Drafting documentation related to data protection matters;
- Reviewing, securing, and improving the security of computer networks as necessary;
- Providing training to employees, etc.

5. Legality of Personal Data Handling

5.1
The processing of Personal Data is lawful only when, and to the extent that, at least one of the following conditions is met:

- (I) The Data Subject has given their consent to the processing of their Personal Data for one or more specific purposes.
- (II) The processing is necessary for the performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into a contract.
- (III) The processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- (IV) The processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- (V) The 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 Data Controller.
- (VI) The processing is necessary for the purposes of the legitimate interests pursued by the Data 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, especially where the Data Subject is a child.

The Company determines the purpose of the processing with reference to one of the above legal bases.

5.2
If the Company collects Personal Data for a specific purpose and intends to use the data for another purpose, the Company must assess the lawfulness of the secondary use of the data, unless the new purpose is based on the Data Subject's consent or is mandated by Union or Member State law as a necessary and proportionate measure in a democratic society.

The Company will consider the following factors in determining the lawfulness of the secondary processing:

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- (I) The connection between the purposes for which the Personal Data was collected and the purposes of the intended further processing.
- (II) The context in which the Personal Data was collected, particularly regarding the relationship between the Data Subjects and the Data Controller.
- (III) The nature of the Personal Data (whether it includes Special Data or data related to criminal convictions and offenses).
- (IV) The possible consequences of further processing for the Data Subjects.
- (V) The existence of appropriate safeguards (e.g., encryption or pseudonymization).

5.3 Conditions for Consent

When the processing is based on consent, the Company must be able to demonstrate that the Data Subject has consented to the processing of their Personal Data. The Company records all electronically collected consents and retains all paper-based consents.

Consent is only valid under the GDPR if it meets the following conditions:

- **Voluntary**
  Consent is voluntary if the Data Subject has a real choice to either provide or withhold consent without facing negative consequences. Consent is not voluntary, for example, if the Data Subject would face adverse consequences if they refuse or withdraw their consent, or if the consent is bundled with acceptance of general terms and conditions that are non-negotiable.

  Consent is also not voluntary when there is an imbalance of power between the Data Subject and the entity requesting consent, such as in an employment relationship where the employee (Data Subject) does not have a real choice due to the hierarchical nature of the relationship.

- **Specific**
  Consent must be specific to the processing activity in question. The Company must clearly define the purpose of the data processing and request consent specifically for that purpose, separating the request for consent to process Personal Data from other information.

  If the same Personal Data is to be used for different purposes, the Company will request separate consents for each purpose.

- **Informed**
  Consent can only be valid if it is based on adequate information. Before obtaining consent, the Company provides the Data Subject with the information outlined in sections 6.1(III) or 6.1(IV) of this Policy.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The Company ensures that the language and form of the information provided are appropriate for the audience and context.

- **Unambiguous**
  The Data Subject must clearly indicate their agreement to the processing of their Personal Data, either by making a statement or by taking a clear affirmative action that signifies consent.

Any consent that does not meet these criteria will not be considered valid under the GDPR.

If the Data Subject gives consent within a statement that also pertains to other matters, the request for consent regarding the processing of Personal Data must be clearly distinguishable from the other matters and presented in a comprehensible and accessible form, using plain and clear language. If any part of the statement does not comply with the GDPR, it will not be binding.

The Data Subject has the right to withdraw their consent at any time. However, the withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

6. Rights of the Data Subject

The Company ensures that the following rights of Data Subjects are upheld in accordance with the applicable laws and regulations, particularly with the provisions of the General Data Protection Regulation (GDPR). The Company acknowledges that the exercise of these rights is fundamental to ensuring the protection of personal data.

6.1 Right to Information and Access

The Data Subject has the right to receive clear and comprehensible information about the handling of their Personal Data. Upon request, the Company provides the Data Subject with the following information:

- (I) The identity and contact details of the Company (the Data Controller) and, if applicable, those of the Data Protection Officer.
- (II) The purposes for which the Personal Data is processed, and the legal basis for the processing.
- (III) The categories of Personal Data concerned.
- (IV) The recipients or categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in third countries or international organizations.
- (V) Where applicable, the period for which the Personal Data will be stored or, if this is not possible, the criteria used to determine that period.
- (VI) The Data Subject's right to request from the Company the rectification or erasure of Personal Data, or the restriction of processing concerning the Data Subject, or to object to such processing.
- (VII) The right to lodge a complaint with a supervisory authority.
- (VIII) If the Personal Data was not collected from the Data Subject, any available information as to its source.
- (IX) The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

The Company must provide this information at the time the Personal Data is obtained or, if the data is collected indirectly, within a reasonable period after the data is obtained.

6.2 Right of Access

The Data Subject has the right to request confirmation as to whether the Company is processing their Personal Data. If such processing is taking place, the Data Subject has the right to access the following information:

- (I) The purposes of the processing.
- (II) The categories of Personal Data concerned.
- (III) The recipients or categories of recipients to whom the Personal Data has been or will be disclosed.
- (IV) The envisaged period for which the Personal Data will be stored or the criteria used to determine that period.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- (V) The existence of the right to request rectification or erasure of Personal Data, restriction of processing, or to object to the processing.
- (VI) The right to lodge a complaint with a supervisory authority.
- (VII) Where the Personal Data is not collected from the Data Subject, any available information regarding its source.
- (VIII) The existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the Data Subject.

The Company provides the Data Subject with a copy of the Personal Data undergoing processing, free of charge. For any further copies requested, the Company may charge a reasonable fee based on administrative costs.

6.3 Right to Rectification
The Data Subject has the right to request the rectification of inaccurate Personal Data concerning them without undue delay. Considering the purposes of the processing, the Data Subject also has the right to request the completion of incomplete Personal Data, including by means of providing a supplementary statement.

6.4 Right to Erasure ("Right to be Forgotten")
The Data Subject has the right to request the erasure of Personal Data concerning them without undue delay, and the Company is obligated to erase such data in the following cases:

- (I) The Personal Data is no longer necessary for the purposes for which it was collected or otherwise processed.
- (II) The Data Subject withdraws their consent on which the processing is based, and there is no other legal ground for the processing.
- (III) The Data Subject objects to the processing, and there are no overriding legitimate grounds for the processing.
- (IV) The Personal Data has been unlawfully processed.
- (V) The Personal Data must be erased to comply with a legal obligation under Union or Member State law to which the Company is subject.
- (VI) The Personal Data has been collected in relation to the offer of information society services to a child.

However, the right to erasure does not apply to the extent that processing is necessary for:

- (I) Exercising the right of freedom of expression and information.
- (II) Compliance with a legal obligation requiring processing under Union or Member State law.
- (III) Reasons of public interest in the area of public health.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- (IV) Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing.
- (V) The establishment, exercise, or defense of legal claims.

6.5 Right to Restriction of Processing

The Data Subject has the right to request the restriction of processing of their Personal Data where one of the following applies:

- (I) The accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Company to verify the accuracy of the data.
- (II) The processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead.
- (III) The Company no longer needs the Personal Data for the purposes of processing, but the Data Subject requires it for the establishment, exercise, or defense of legal claims.
- (IV) The Data Subject has objected to the processing pending the verification of whether the legitimate grounds of the Company override those of the Data Subject.

Where processing has been restricted, such Personal Data will only be processed (with the exception of storage) with the Data Subject's consent, or for the establishment, exercise, or defense of legal claims, or for protecting the rights of another natural or legal person, or for reasons of important public interest.

The Data Subject must be informed before any restriction is lifted.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

6.6 Right to Data Portability
The Data Subject has the right to receive the Personal Data concerning them, which they have provided to the Company, in a structured, commonly used, and machine-readable format. The Data Subject also has the right to transmit that data to another Data Controller without hindrance from the Company, where:

- (I) The processing is based on consent or on a contract; and
- (II) The processing is carried out by automated means.

In exercising their right to data portability, the Data Subject also has the right to have the Personal Data transmitted directly from one Data Controller to another, where technically feasible.

The exercise of the right to data portability does not affect the right to erasure ("right to be forgotten"). This right must not adversely affect the rights and freedoms of others.

6.7 Right to Object
The Data Subject has the right to object, on grounds relating to their particular situation, at any time to the processing of their Personal Data, which is based on the following legal grounds:

- (I) The 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 Data Controller; or
- (II) The processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party.

In such cases, the Company must stop processing the Personal Data unless the Company can demonstrate 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.

If Personal Data is processed for direct marketing purposes, the Data Subject has the right to object at any time to the processing of their Personal Data for such marketing, including profiling related to direct marketing. If the Data Subject objects to processing for direct marketing purposes, the Personal Data will no longer be processed for such purposes.

Where Personal Data is processed for scientific or historical research purposes or statistical purposes, the Data Subject has the right to object, on grounds relating to their particular situation, to the processing of their Personal Data, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

6.8 Rights Related to Automated Decision-Making, Including Profiling
The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This does not apply if the decision:

- (I) Is necessary for entering into, or performance of, a contract between the Data Subject and the Data Controller.
- (II) Is authorized by Union or Member State law, which lays down suitable measures to safeguard the Data Subject's rights, freedoms, and legitimate interests.
- (III) Is based on the Data Subject's explicit consent.

In cases where automated decision-making (including profiling) is allowed, the Company ensures that appropriate measures are in place to protect the Data Subject's rights, freedoms, and legitimate interests, including the right to obtain human intervention, express their point of view, and contest the decision.

6.9 Right to Lodge a Complaint
The Data Subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement, if they consider that the processing of their Personal Data infringes the GDPR.

6.10 Right to an Effective Judicial Remedy
The Data Subject has the right to an effective judicial remedy if they consider that their rights under the GDPR have been infringed as a result of the processing of their Personal Data that is not in compliance with the GDPR.

Proceedings against the Company, as Data Controller, must be brought before the courts of the Member State where the Company has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the Data Subject has their habitual residence, unless the Data Controller is a public authority of a Member State acting in the exercise of its public powers.

6.11 Right to Compensation and Liability
The Data Subject has the right to receive compensation from the Company for any damage suffered as a result of an infringement of the GDPR. The Company, as the Data Controller, is liable for the damage caused by the unlawful processing of Personal Data unless the Company can prove that it is not in any way responsible for the event giving rise to the damage.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

7. Data Transfers

7.1 Transfers Within the European Economic Area (EEA)

The Company may transfer Personal Data to other Data Controllers or Data Processors within the European Economic Area (EEA), as long as the processing complies with the requirements of this Policy and the applicable legal regulations, including the GDPR.

7.2 Transfers to Third Countries or International Organizations

The Company may transfer Personal Data to a third country or an international organization under the following conditions:

- (I) **Adequacy Decision**: Personal Data may be transferred to a country or international organization outside the EEA if the European Commission has decided that the country or organization ensures an adequate level of protection for Personal Data. In this case, the transfer can take place without the need for further authorization.
- (II) **Appropriate Safeguards**: If no adequacy decision exists, the Company may transfer Personal Data to a third country or international organization only if it provides appropriate safeguards, such as:
    - A legally binding and enforceable instrument between public authorities or bodies;
    - Binding corporate rules (BCRs);
    - Standard contractual clauses (SCCs) adopted by the European Commission;
    - An approved code of conduct or certification mechanism.

In these cases, Data Subjects must be provided with enforceable rights and effective legal remedies in the destination country.

7.3 Derogations for Specific Situations

In the absence of an adequacy decision or appropriate safeguards, the Company may transfer Personal Data to a third country or international organization only if one of the following conditions is met:

- (I) The Data Subject has explicitly consented to the proposed transfer, after being informed of the potential risks due to the absence of an adequacy decision and appropriate safeguards.
- (II) The transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or for the implementation of pre-contractual measures taken at the Data Subject’s request.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- (III) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person.
- (IV) The transfer is necessary for important reasons of public interest.
- (V) The transfer is necessary for the establishment, exercise, or defense of legal claims.
- (VI) The transfer is necessary to protect the vital interests of the Data Subject or other persons, where the Data Subject is physically or legally incapable of giving consent.
- (VII) The transfer is made from a register that, according to Union or Member State law, is intended to provide information to the public and is open to consultation by the public or anyone able to demonstrate a legitimate interest.

Where none of these conditions apply, and no adequacy decision or appropriate safeguards are in place, the transfer of Personal Data may still take place if it is necessary for the purposes of compelling legitimate interests pursued by the Data Controller, provided that such interests are not overridden by the interests or rights and freedoms of the Data Subject. In such cases, the Company will inform the Data Protection Authority of the transfer.

7.4 Transparency of Data Transfers

In all cases, the Company must inform the Data Subject about any intended transfers of their Personal Data to third countries or international organizations. This includes information about the existence or absence of an adequacy decision by the European Commission, the appropriate safeguards applied, and how the Data Subject can obtain a copy of those safeguards or where they have been made available.

7.5 Records of Transfers

The Company maintains records of all Personal Data transfers to third countries or international organizations, documenting:

- The countries or international organizations involved in the transfer.
- The categories of Personal Data transferred.
- The date and purpose of each transfer.
- The legal basis for each transfer.

This documentation will be made available to the relevant Data Protection Authorities upon request.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

8. Records of Data Handling Activities

8.1 Obligation to Maintain Records

The Company is required to maintain records of all data processing activities under its responsibility, except where the processing involves occasional activities or processing of data that does not include Special Data or data related to criminal convictions and offenses. These records must be available to the supervisory authorities upon request.

8.2 Contents of the Records

The records of data handling activities must contain the following information:

- (I) The name and contact details of the Company (Data Controller), as well as any joint controllers, representatives, and the Data Protection Officer (if applicable).
- (II) The purposes of the data processing.
- (III) A description of the categories of Data Subjects and the categories of Personal Data.
- (IV) The categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in third countries or international organizations.
- (V) Information about any transfers of Personal Data to a third country or an international organization, including the identification of that country or organization, and the documentation of appropriate safeguards applied to the transfer.
- (VI) Where possible, the envisaged time limits for erasure of the different categories of Personal Data.
- (VII) Where possible, a general description of the technical and organizational security measures implemented by the Company to ensure the protection of Personal Data.

8.3 Records of Processing by Data Processors

Where the Company acts as a Data Processor on behalf of another Data Controller, the Company must also maintain records of the processing activities it carries out, including:

- (I) The name and contact details of the Data Controller or controllers on behalf of whom the Company is processing data, and any representatives or Data Protection Officers involved.
- (II) The categories of processing carried out on behalf of the Data Controller.
- (III) Information about transfers of Personal Data to a third country or international organization, including identification of that country or organization and the documentation of the appropriate safeguards applied to the transfer.
- (IV) A general description of the technical and organizational security measures implemented.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

8.4 Inspection of Records

The Company ensures that records of all data processing activities are readily available for inspection by the relevant Data Protection Authorities. The Company is committed to maintaining accurate and up-to-date records to demonstrate compliance with data protection regulations.

- event of a technical failure or data loss incident. These backups are stored securely, and access is restricted to authorized personnel.

9. Data Security

The Company is committed to ensuring the confidentiality, integrity, and availability of Personal Data. It takes appropriate technical and organizational measures to protect Personal Data from unauthorized access, alteration, disclosure, accidental or unlawful destruction, loss, or damage.

9.1 Security Measures

The Company implements the following security measures to protect Personal Data:

- **Physical Security**:
  The Company ensures that Personal Data stored in physical form (e.g., paper documents) is protected by physical security measures, such as controlled access to facilities, locked storage, and the use of security staff or surveillance systems to monitor access.
- **Technical Security**:
  The Company applies state-of-the-art technology to protect electronically stored Personal Data. This includes the use of encryption, firewalls, secure data transmission methods (e.g., SSL), and regular software updates and patches to minimize security vulnerabilities.
- **Access Control**:
  Only authorized personnel are permitted to access Personal Data. The Company uses password protection, role-based access controls, and other authentication measures to restrict access to systems and data. Each user is assigned a unique user ID, and their activities are monitored and logged.
- **Data Minimization**:
  The Company processes only the amount of Personal Data necessary for the intended purpose, minimizing the amount of data collected, stored, and processed.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Data Backup**:
  Regular backups of Personal Data are conducted to ensure that data can be restored in the event of a technical failure or data loss incident. These backups are stored securely, and access is restricted to authorized personnel.

9.2 Data Security Policies

The Company maintains written data security policies that outline the measures in place to safeguard Personal Data. These policies are reviewed and updated regularly to reflect changes in technology, business practices, and legal requirements.

9.3 Security of Third-Party Service Providers

When the Company engages third-party service providers (e.g., cloud service providers, IT support), it ensures that the provider complies with the Company's data security standards. Contracts with third-party service providers must include provisions for safeguarding Personal Data and ensuring compliance with the Company's security policies and applicable data protection regulations.

9.4 Security Incident Response Plan

In the event of a data security breach or other data protection incident, the Company has established a security incident response plan that includes the following steps:

1. **Identification and Containment**:
   The incident is immediately identified, and measures are taken to contain the breach to prevent further damage.
2. **Assessment and Notification**:
   The Company assesses the nature and scope of the breach and determines whether the breach poses a risk to the rights and freedoms of Data Subjects. If there is a significant risk, the Data Subjects and the relevant supervisory authority are notified without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
3. **Mitigation**:
   The Company takes appropriate steps to mitigate the effects of the breach and prevent similar incidents in the future. This may include additional security measures, staff training, or changes in data handling procedures.
4. **Documentation and Reporting**:
   All security incidents are documented, and a report is generated, detailing the nature of the breach, the actions taken to mitigate the impact, and any measures implemented to prevent recurrence.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

9.5 Regular Security Audits

The Company conducts regular internal and external audits of its data security practices to ensure compliance with its data protection obligations. These audits evaluate the effectiveness of the Company's security measures and identify areas for improvement.

9.6 Staff Training

The Company ensures that all employees who handle Personal Data receive training on data security practices, data protection regulations, and the Company's internal policies. Employees are regularly updated on changes to these policies and are trained to recognize and respond to potential security incidents.

10. Data Protection Incident

A data protection incident refers to any security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. This includes incidents that affect the confidentiality, integrity, or availability of the data.

10.1 Reporting a Data Protection Incident

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The Company has established a procedure for detecting, reporting, and responding to data protection incidents. All employees are required to immediately report any suspected data protection incidents to the designated officer responsible for data protection.

Upon becoming aware of a data protection incident, the Company will take immediate action to:

- (I) Investigate the incident.
- (II) Assess the potential impact on the rights and freedoms of Data Subjects.
- (III) Mitigate any harm caused by the incident.
- (IV) Take steps to prevent the recurrence of similar incidents.

10.2 Notification to the Supervisory Authority

If the data protection incident is likely to result in a risk to the rights and freedoms of individuals, the Company will notify the relevant supervisory authority without undue delay and, where feasible, within **72 hours** of becoming aware of the incident.

The notification to the supervisory authority must include the following information:

- (I) A description of the nature of the data protection incident, including the categories and approximate number of Data Subjects affected, and the categories and approximate number of Personal Data records concerned.
- (II) The name and contact details of the data protection officer or another contact point for more information.
- (III) A description of the likely consequences of the data protection incident.
- (IV) A description of the measures taken or proposed by the Company to address the data protection incident, including measures to mitigate its possible adverse effects.

If the Company is unable to provide all of this information at the same time, it will provide the information in phases, without undue further delay.

10.3 Notification to the Data Subject

If the data protection incident is likely to result in a high risk to the rights and freedoms of the Data Subject, the Company will inform the affected Data Subjects without undue delay. The notification to the Data Subject will describe:

- (I) The nature of the incident.
- (II) The contact details of the data protection officer or another point of contact.
- (III) The likely consequences of the incident.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- (IV) The measures taken or proposed by the Company to mitigate the effects of the incident.

The Company may not be required to notify the Data Subjects in the following cases:

- (I) The Company has implemented appropriate technical and organizational protection measures (such as encryption) that render the Personal Data unintelligible to any unauthorized person.
- (II) The Company has taken subsequent measures to ensure that the high risk to Data Subjects' rights and freedoms is no longer likely to materialize.
- (III) Individual notification would involve disproportionate effort. In such cases, a public communication or similar measure would be made to inform Data Subjects in an equally effective manner.

10.4 Documentation of Data Protection Incidents

The Company keeps records of all data protection incidents, including the facts related to the incident, its effects, and the remedial actions taken. This documentation helps the Company demonstrate compliance with data protection regulations and allows for thorough audits and reviews of security incidents.

11. Data Protection Impact Assessment and Prior Consultation

11.1 Data Protection Impact Assessment (DPIA)

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

A Data Protection Impact Assessment (DPIA) is required when the processing of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The Company performs a DPIA to assess the origin, nature, particularity, and severity of this risk.

The DPIA is conducted before the processing begins and must be completed in the following situations, among others:

- (I) Systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling, which produces legal effects concerning the person or significantly affects them.
- (II) Large-scale processing of Special Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning health, sex life, or criminal convictions and offenses.
- (III) Systematic monitoring of publicly accessible areas on a large scale.

11.2 DPIA Process

The DPIA includes:

- (I) A description of the intended data processing operations and the purposes of the processing.
- (II) An assessment of the necessity and proportionality of the processing in relation to the purposes.
- (III) An assessment of the risks to the rights and freedoms of Data Subjects.
- (IV) The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with legal requirements.

If the DPIA identifies high risks that the Company cannot mitigate, the Company will consult the relevant supervisory authority before proceeding with the processing.

11.3 Prior Consultation

If a DPIA reveals that the processing would result in high risks to Data Subjects' rights and freedoms, and the Company is unable to mitigate those risks through appropriate measures, it must seek prior consultation from the supervisory authority before processing.

The consultation request to the supervisory authority must include:

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- (I) The roles and responsibilities of the Company and any Data Processors involved.
- (II) The purposes and means of the intended processing.
- (III) The measures and safeguards proposed to protect Data Subjects' rights and freedoms.
- (IV) The results of the DPIA.
- (V) Any other information requested by the supervisory authority.

The supervisory authority will provide guidance on the proposed processing and advise on any additional safeguards or adjustments necessary.

11.4 Updating and Reviewing DPIAs

The Company regularly reviews and, if necessary, updates DPIAs, especially when there are significant changes to the nature, scope, or context of the processing. Regular reviews help ensure ongoing compliance with data protection regulations and assess whether the initial safeguards continue to be effective in mitigating risks.

12. Data Protection Officer

12.1 Appointment of a Data Protection Officer (DPO)

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The Company is required to appoint a Data Protection Officer (DPO) if one of the following conditions applies:

- (I) The processing is carried out by a public authority or body (except for courts acting in their judicial capacity).
- (II) The core activities of the Company consist of processing operations that require regular and systematic monitoring of Data Subjects on a large scale.
- (III) The core activities of the Company consist of large-scale processing of Special Data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, or criminal convictions and offenses).

If the Company does not meet these criteria, it may still choose to appoint a DPO voluntarily to ensure compliance with data protection regulations.

12.2 Role and Responsibilities of the DPO

The DPO is responsible for overseeing the Company's data protection strategy and ensuring compliance with GDPR and other applicable data protection laws. The DPO's duties include:

- (I) Informing and advising the Company, as well as its employees, on their data protection obligations.
- (II) Monitoring compliance with GDPR, other relevant laws, and the Company's internal data protection policies, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations.
- (III) Advising on data protection impact assessments (DPIAs) and monitoring their performance.
- (IV) Cooperating with the supervisory authority and acting as the Company's contact point for the supervisory authority on issues related to data processing, including prior consultations.
- (V) Serving as the point of contact for Data Subjects with concerns regarding the processing of their Personal Data, including requests to exercise their rights.

12.3 Independence and Resources

The DPO must be able to perform their duties and tasks independently and must not be instructed by the Company on how to carry out these tasks. The DPO must not be penalized or dismissed for performing their role, except in cases of misconduct unrelated to data protection.

The Company ensures that the DPO is provided with the necessary resources, including financial, technical, and human resources, to effectively fulfill their obligations. This includes

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

access to Personal Data and processing activities, as well as the ability to maintain their professional knowledge through continuous training.

12.4 Reporting

The DPO reports directly to the highest management level of the Company to ensure that data protection issues are addressed at the appropriate level. The DPO is involved, in a timely manner, in all matters concerning the protection of Personal Data.

12.5 Confidentiality

The DPO is bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.

12.6 Conflicts of Interest

The DPO must not hold a position within the Company that could result in a conflict of interest. For example, the DPO cannot simultaneously hold a decision-making role within the Company's IT, legal, or HR departments, as these roles could involve determining the purposes and means of processing Personal Data.

13. Fines and Compensation

13.1 Administrative Fines

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The Company is subject to administrative fines for violations of data protection laws, particularly the General Data Protection Regulation (GDPR). The amount of these fines depends on the nature, severity, and duration of the infringement. The fines are imposed in addition to, or instead of, other measures such as warnings or orders to bring data processing into compliance.

Fines can be imposed for violations including, but not limited to:

- (I) Failure to implement appropriate technical and organizational measures to ensure data security.
- (II) Failure to obtain valid consent where necessary.
- (III) Failure to comply with Data Subject rights, such as access, rectification, or erasure of Personal Data.
- (IV) Failure to notify the supervisory authority or Data Subjects in the event of a data breach.
- (V) Unlawful transfer of Personal Data to third countries without appropriate safeguards.

Administrative fines are tiered based on the type of violation:

- For less severe violations (such as failing to maintain adequate documentation or failing to cooperate with the supervisory authority), fines may amount to **up to €10 million**, or **2% of the Company's total worldwide annual turnover**, whichever is higher.
- For more severe violations (such as breaches of Data Subject rights or unlawful processing of Personal Data), fines may reach **up to €20 million**, or **4% of the Company's total worldwide annual turnover**, whichever is higher.

The supervisory authority considers various factors when determining the amount of the fine, including:

- The nature, gravity, and duration of the infringement.
- The number of Data Subjects affected and the level of harm caused.
- Whether the infringement was intentional or negligent.
- Actions taken by the Company to mitigate the damage.
- Previous infringements by the Company.
- Cooperation with the supervisory authority.
- Adherence to approved codes of conduct or certification mechanisms.

13.2 Compensation

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

If a Data Subject suffers material or non-material damage (e.g., financial loss or emotional distress) as a result of an infringement of data protection laws, the Data Subject has the right to receive compensation from the Company.

The Company, as the Data Controller, is liable for any damage caused by unlawful processing of Personal Data. If the Company uses a Data Processor to handle Personal Data, the Data Processor may also be liable for damages if it fails to comply with its legal obligations.

In order to receive compensation, the Data Subject must prove that the damage suffered was caused by an infringement of data protection laws.

The Company may avoid liability for compensation if it can demonstrate that it is not in any way responsible for the event that gave rise to the damage. This could be the case, for example, if the damage was caused by an event beyond the Company's control, or if the Company took all reasonable steps to comply with data protection regulations but was nevertheless affected by an external breach or cyberattack.

13.3 Joint and Several Liability

In cases where multiple parties (e.g., both a Data Controller and a Data Processor) are involved in the same processing activity and are responsible for an infringement, they may be held jointly and severally liable for any damages. This means that a Data Subject may claim full compensation from either the Data Controller or the Data Processor, who can then seek to recover a share of the compensation from the other liable party.

Appendix 1: The Company's Data Protection Measures

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The Company has implemented the following technical and organizational measures to ensure the protection of Personal Data and to comply with GDPR requirements:

1. Physical Security Measures

- **Controlled Access**:
  The Company's offices and any locations where Personal Data is stored are secured with controlled access. Only authorized personnel are allowed to enter these premises.
- **Locked Storage**:
  Personal Data in paper form is stored in locked cabinets or rooms. Access to these storage areas is limited to authorized employees.
- **Surveillance**:
  Security cameras may be used to monitor access to the Company's premises to prevent unauthorized entry.

2. Technical Security Measures

- **Encryption**:
  The Company uses encryption to protect Personal Data stored electronically, especially sensitive or special categories of data. Encryption ensures that data cannot be accessed by unauthorized individuals in the event of a security breach.
- **Firewalls and Anti-Virus Software**:
  The Company uses firewalls and up-to-date anti-virus software to prevent unauthorized access to its IT systems and to protect against malware and cyberattacks.
- **Data Backup**:
  Regular backups are conducted to protect against data loss. Backups are stored securely, and access is restricted to authorized personnel.
- **Password Protection**:
  All IT systems that store or process Personal Data are password-protected. Passwords are complex, regularly updated, and only known to authorized users.

3. Organizational Security Measures

- **Data Protection Policies**:
  The Company maintains comprehensive internal data protection policies, which are reviewed and updated regularly. These policies outline the Company's approach to Personal Data processing, security, and compliance with GDPR.
- **Access Control**:
  The Company ensures that only employees who need access to Personal Data for their

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

work are granted access. Access rights are regularly reviewed and updated to ensure compliance.

- **Training and Awareness**:
  Employees who handle Personal Data receive regular training on data protection laws, security measures, and the Company's internal policies. This ensures that employees are aware of their obligations and the risks associated with data processing.

4. Data Retention and Disposal

- **Data Retention Policy**:
  The Company has a defined data retention policy, which sets out the length of time Personal Data is kept before being securely deleted or destroyed. The retention period depends on the purpose for which the data was collected and any legal obligations to retain certain types of data.
- **Secure Disposal**:
  When Personal Data is no longer required, the Company ensures that it is securely deleted from electronic systems and securely destroyed if held in physical form (e.g., shredding paper documents). The disposal process is documented to ensure compliance with the data retention policy.

5. Data Breach Response Plan

The Company has a data breach response plan in place to handle potential data breaches. The plan includes:

- **Immediate Reporting**:
  Employees must report any suspected data breaches to the designated Data Protection Officer or responsible person immediately.
- **Investigation and Containment**:
  Upon notification of a data breach, the Company investigates the cause of the breach and takes steps to contain the breach and prevent further unauthorized access or data loss.
- **Notification**:
  If a data breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will notify the affected Data Subjects and the relevant supervisory authority without undue delay.
- **Remediation**:
  Following a data breach, the Company implements measures to mitigate the damage and prevent future incidents.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

6. Regular Audits and Reviews

The Company conducts regular audits and reviews of its data protection practices to ensure compliance with GDPR and other relevant laws. These audits assess the effectiveness of the Company's security measures and identify any areas for improvement.

Appendix 2: Records of Personal Data Handling

The following section outlines the Company's records of Personal Data handling activities. These records cover various categories of Personal Data and detail the purpose of processing, legal basis, data retention periods, and security measures in place.

1. Handling of Personal Data in Corporate Documents

- **Purpose of Processing**:
  The Personal Data is processed to comply with legal obligations regarding the creation and storage of corporate documents, such as contracts, meeting minutes, resolutions, and internal communications.
- **Categories of Data**:
  Names, contact details, job titles, signatures, identification numbers, and other data necessary for corporate documentation.
- **Legal Basis**:
  The processing is necessary to comply with legal obligations and for the legitimate interest of the Company in maintaining proper corporate governance.
- **Data Retention Period**:
  The data is retained for the duration required by applicable laws (e.g., business and tax regulations), typically **5 to 10 years** after the documents are no longer active.
- **Security Measures**:
  Documents are stored securely in locked cabinets, and access is restricted to authorized personnel.

2. Handling of Employee Data for Legal Compliance

- **Purpose of Processing**:
  Employee Personal Data is processed to fulfill legal obligations, such as complying with labor laws, social security regulations, and tax obligations.
- **Categories of Data**:
  Name, address, social security number, tax identification number, employment history, and other employment-related data.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Legal Basis**:
  The processing is necessary to fulfill legal obligations under labor law, tax law, and social security regulations.
- **Data Retention Period**:
  Data is retained for **5 to 10 years** after the termination of employment, depending on legal requirements.
- **Security Measures**:
  Data is stored in secure systems with restricted access, and physical documents are kept in locked storage.

3. Handling of Employee Data for Contact Purposes

- **Purpose of Processing**:
  Employee contact details are processed for internal communications and operational purposes, such as disseminating important information or coordinating work activities.
- **Categories of Data**:
  Name, phone number, email address, job title.
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to ensure efficient internal communication.
- **Data Retention Period**:
  Data is retained for the duration of the employment relationship and deleted upon termination unless otherwise required by law.
- **Security Measures**:
  Contact details are stored in a secure internal system with access limited to relevant personnel.

4. Handling of Personal Data in Employee Attendance Records

- **Purpose of Processing**:
  Employee attendance records are processed to ensure compliance with labor regulations, including working hours, rest periods, and overtime.
- **Categories of Data**:
  Name, employee ID, attendance dates, working hours, overtime records.
- **Legal Basis**:
  The processing is necessary to fulfill legal obligations under labor laws and for the legitimate interest of the Company in monitoring employee attendance.
- **Data Retention Period**:
  Data is retained for **5 years** after the records are no longer relevant, in compliance with labor laws.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Security Measures**:
  Data is stored electronically with secure access controls, and physical records are kept in locked storage.

5. Handling of Personal Data in Employee Vacation Records

- **Purpose of Processing**:
  Employee vacation records are processed to manage and track leave entitlements, including annual leave, sick leave, and other types of statutory leave.
- **Categories of Data**:
  Name, employee ID, vacation dates, type of leave.
- **Legal Basis**:
  The processing is necessary to comply with labor laws and for the legitimate interest of the Company in managing employee leave.
- **Data Retention Period**:
  Data is retained for **5 years** after the termination of employment, as required by labor regulations.
- **Security Measures**:
  Vacation records are stored in a secure internal system with access limited to authorized personnel.

6. Handling of Personal Data Related to Fire, Work, and Accident Safety Training

- **Purpose of Processing**:
  The Company processes employee data to ensure compliance with health and safety regulations, including training in fire safety, work safety, and accident prevention.
- **Categories of Data**:
  Name, job title, training records, certifications.
- **Legal Basis**:
  The processing is necessary to comply with legal obligations under health and safety regulations.
- **Data Retention Period**:
  Data is retained for **5 years** after the training is completed, unless otherwise required by law.
- **Security Measures**:
  Training records are stored in secure internal systems with restricted access, and physical records are kept in locked cabinets.

7. Handling of Employee Bank Account Information

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Purpose of Processing**:
  Employee bank account details are processed for the purpose of salary payments and reimbursement of expenses.
- **Categories of Data**:
  Name, bank account number, bank name.
- **Legal Basis**:
  The processing is necessary for the performance of the employment contract.
- **Data Retention Period**:
  Data is retained for **5 years** after the termination of employment, in compliance with financial regulations.
- **Security Measures**:
  Bank account details are securely stored with access limited to payroll personnel.

8. Handling of Personal Data Related to Company-issued Equipment

- **Purpose of Processing**:
  The Company processes Personal Data related to the allocation and management of equipment issued to employees, such as computers, mobile phones, and other devices. This processing is necessary for asset management and ensuring compliance with company policies.
- **Categories of Data**:
  - Employee name
  - Job title
  - Device type (e.g., laptop, mobile phone)
  - Device serial number
  - Date of issuance
  - Return date of the equipment
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company in managing its assets and ensuring proper usage of company-issued equipment.
- **Data Retention Period**:
  Personal Data related to company-issued equipment is retained for the duration of the employee's employment and for **5 years** after the return of the equipment, unless otherwise required by law.
- **Security Measures**:
  Data regarding company-issued equipment is stored in a secure asset management system with restricted access. Regular audits are conducted to ensure that all issued equipment is accounted for.

9. Handling of Employee Data Related to Company-issued Mobile Phones

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Purpose of Processing**:
  The Company processes Personal Data associated with company-issued mobile phones to manage device allocation and monitor usage.
- **Categories of Data**:
  - Employee name
  - Job title
  - Mobile phone number
  - Usage logs (e.g., call records, data usage)
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company in managing mobile phone usage and associated costs.
- **Data Retention Period**:
  Personal Data related to mobile phone usage is retained for **2 years** from the date of usage unless otherwise required by applicable regulations.
- **Security Measures**:
  Access to usage data is limited to authorized personnel managing mobile phone accounts and expenses, and mobile devices are protected with security measures like passwords and remote wiping capabilities.

10. Handling of Personal Data in Resumes (CVs)

- **Purpose of Processing**:
  Resumes submitted by job applicants are processed to facilitate recruitment and selection.
- **Categories of Data**:
  - Name
  - Contact information (phone number, email)
  - Education history
  - Employment history
  - Skills and qualifications
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to assess and select candidates for employment.
- **Data Retention Period**:
  Resumes of unsuccessful candidates are retained for **6 months** after the recruitment process, unless the candidate agrees to a longer retention period for future job openings.
- **Security Measures**:
  Resumes are stored securely in HR management systems, and access is restricted to authorized HR personnel.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

11. Handling of Employee Data Related to Access Cards

- **Purpose of Processing**:
  The Company processes Personal Data related to access cards to manage and monitor entry to its premises.
- **Categories of Data**:
  - Employee name
  - Employee ID
  - Access card number
  - Access logs (entry and exit times)
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to ensure the security of its facilities.
- **Data Retention Period**:
  Access logs are retained for **1 year**, after which they are deleted unless required for security or audit purposes.
- **Security Measures**:
  Access control systems are secured, and access logs are stored in a secure database with limited access to authorized personnel.

12. Handling of Personal Data in the Record of Individual Alarm Codes

- **Purpose of Processing**:
  The Company processes data related to individual alarm codes to control and monitor access to secure areas of its premises.
- **Categories of Data**:
  - Employee name
  - Employee ID
  - Alarm code
  - Access logs (entry and exit times)
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to secure sensitive areas.
- **Data Retention Period**:
  Data related to alarm codes and access logs is retained for **1 year**.
- **Security Measures**:
  Alarm codes and access logs are stored securely, and access is restricted to security personnel.

13. Handling of Contact Information

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Purpose of Processing**:
  The Company processes Personal Data related to business contacts to maintain professional relationships and effective communication with clients, partners, and suppliers.
- **Categories of Data**:
  - Name
  - Job title
  - Company name
  - Email address
  - Phone number
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to engage in business communication.
- **Data Retention Period**:
  Contact information is retained as long as the business relationship exists or until the Data Subject requests deletion.
- **Security Measures**:
  Contact details are stored in secure customer relationship management (CRM) systems with access restricted to authorized personnel.

14. Handling of Data in Issued and Received Accounting Documents

- **Purpose of Processing**:
  The Company processes Personal Data contained in invoices, contracts, and other accounting documents for financial and tax compliance.
- **Categories of Data**:
  - Name
  - Company name
  - Address
  - Tax identification number
  - Bank account details
- **Legal Basis**:
  The processing is necessary to comply with legal obligations under financial regulations.
- **Data Retention Period**:
  Data is retained for **5 to 10 years**, in compliance with financial regulations.
- **Security Measures**:
  Accounting documents are stored in secure financial management systems, with access restricted to authorized financial personnel.

15. Handling of Personal Data on Business Cards

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Purpose of Processing**:
  The Company processes Personal Data provided on business cards for establishing and maintaining business contacts.
- **Categories of Data**:
  - Name
  - Job title
  - Company name
  - Email address
  - Phone number
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to foster business relationships.
- **Data Retention Period**:
  Business card information is retained as long as the business relationship exists or until the Data Subject requests deletion.
- **Security Measures**:
  Business card information is stored in secure systems, with access limited to relevant personnel.

16. Handling of Personal Data through the Company's Surveillance Systems

- **Purpose of Processing**:
  The Company uses surveillance systems to monitor its premises for security purposes.
- **Categories of Data**:
  - Video recordings of individuals on the Company's premises.
- **Legal Basis**:
  The processing is based on the legitimate interest of the Company to secure its property and ensure employee safety.
- **Data Retention Period**:
  Video recordings are retained for **30 days** unless needed for an ongoing investigation.
- **Security Measures**:
  Video footage is stored in secure systems, with access restricted to security personnel.

17. Handling of Personal Data on the Company's Website

- **Purpose of Processing**:
  Personal Data collected through the Company's website is processed for various purposes, including responding to inquiries and managing user accounts.
- **Categories of Data**:
  - Name
  - Email address

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

  - Phone number
  - IP address
  - Other data provided by users.
- **Legal Basis**:
  The processing is based on the consent of the user or the legitimate interest of the Company in operating its website.
- **Data Retention Period**:
  Data is retained for as long as necessary to fulfill the purpose for which it was collected or as required by law.
- **Security Measures**:
  Personal Data collected through the website is stored securely, and access is restricted to authorized personnel.

18. Handling of Personal Data Related to Sweepstakes

- **Purpose of Processing**:
  Personal Data is processed to organize and manage sweepstakes and promotional events.
- **Categories of Data**:
  - Name
  - Contact details
  - Other data necessary for participation.
- **Legal Basis**:
  The processing is based on the consent of the participants.
- **Data Retention Period**:
  Data is retained for the duration of the event and a reasonable period thereafter, unless otherwise required by law.
- **Security Measures**:
  Data related to sweepstakes is securely stored, with access limited to personnel managing the event.

19. Handling of Personal Data Related to Newsletters

- **Purpose of Processing**:
  Personal Data is processed to send newsletters and marketing communications to subscribers.
- **Categories of Data**:
  - Name
  - Email address
  - Other contact details.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Legal Basis**:
  The processing is based on the consent of the subscriber.
- **Data Retention Period**:
  Data is retained for as long as the subscription is active or until the Data Subject unsubscribes.
- **Security Measures**:
  Data is securely stored in email marketing systems, with access restricted to authorized personnel.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Appendix 3: Record of Data Protection Incidents

The Company maintains a record of all data protection incidents to ensure compliance with data protection regulations and to facilitate investigations and audits. This record includes details about each incident, its impact, and the response actions taken.

1. Structure of the Record

The record of data protection incidents includes the following information:

- **Incident Description**:
  A detailed description of the incident, including the nature of the breach (e.g., unauthorized access, data loss).
- **Date of Incident**:
  The date and time when the incident occurred or was discovered.
- **Categories of Personal Data Involved**:
  A list of the types of Personal Data affected by the incident (e.g., names, contact details, sensitive data).
- **Number of Data Subjects Affected**:
  An estimate of the number of individuals affected by the incident.
- **Impact Assessment**:
  An assessment of the potential impact on the rights and freedoms of affected Data Subjects.
- **Actions Taken**:
  A description of the actions taken to contain the incident, mitigate risks, and remediate any issues.
- **Notification**:
  Details about whether the incident was reported to the supervisory authority and/or affected Data Subjects, including dates of notifications.
- **Follow-up Actions**:
  Any follow-up actions taken to prevent future incidents and to improve data protection measures.

2. Process for Recording Data Protection Incidents

- **Immediate Reporting**:
  All employees must report suspected data protection incidents immediately to the designated Data Protection Officer or responsible individual.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Investigation**:
  Upon receiving a report of an incident, the Company will investigate to determine the cause, scope, and impact of the incident.
- **Documentation**:
  The details of the incident will be documented in the record, including all relevant information as outlined above.
- **Review and Update**:
  The record of incidents will be reviewed regularly to identify trends, evaluate the effectiveness of response measures, and inform training and awareness initiatives.

3. Storage and Access to the Record

- **Confidentiality**:
  The record of data protection incidents is stored securely and is accessible only to authorized personnel involved in data protection and compliance activities.
- **Retention Period**:
  The record of incidents will be retained for a minimum of **5 years** from the date of the incident, unless otherwise specified by applicable regulations.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Appendix 4: Balancing of Interests Tests

The Company conducts balancing of interests tests to ensure that the processing of Personal Data is justified when it relies on legitimate interests as the legal basis for processing. This process evaluates whether the interests of the Company outweigh the rights and freedoms of Data Subjects.

1. Handling of Employee Data for Contact Purposes

- **Purpose of Processing**:
  The Company processes employee contact details to facilitate internal communication and ensure efficient workflow within the organization.
- **Legitimate Interest**:
  The Company's legitimate interest is to maintain effective communication with its employees, ensuring smooth operational activities and timely coordination among team members.
- **Impact on Data Subjects**:
  The processing of contact information is limited to business purposes and does not infringe on the privacy rights of employees. The data is used strictly for work-related communications and is not shared externally without consent.
- **Mitigation Measures**:
  The Company implements access controls to limit the availability of contact details to authorized personnel only. Employees are informed about the use of their contact details, and data security measures are in place to protect this information.
- **Conclusion**:
  The legitimate interest of the Company in processing employee contact details outweighs the minimal impact on employee privacy. Therefore, this processing is justified.

2. Handling of Data Related to Company-issued Equipment

- **Purpose of Processing**:
  The Company processes data related to the allocation and monitoring of company-issued equipment (e.g., laptops, mobile phones) to ensure responsible usage and asset management.
- **Legitimate Interest**:
  The Company has a legitimate interest in protecting its property, monitoring the use of its equipment, and ensuring compliance with internal policies.
- **Impact on Data Subjects**:
  The processing involves minimal interference with the employee's privacy since it

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

pertains only to equipment provided for professional use. There is no tracking of personal activities or private use.

- **Mitigation Measures**:
  Data related to company-issued equipment is stored securely and access is limited to personnel responsible for asset management. Employees are informed about the monitoring of equipment use, and clear policies are in place regarding acceptable use.
- **Conclusion**:
  The Company's legitimate interest in protecting its assets and ensuring responsible usage of company-issued equipment outweighs the limited impact on employee privacy. This processing is justified.

3. Handling of Employee Data Related to Access Cards

- **Purpose of Processing**:
  The Company uses access cards to control entry to its premises, monitor attendance, and ensure the security of its facilities.
- **Legitimate Interest**:
  The Company has a legitimate interest in protecting its premises, securing sensitive areas, and ensuring employee attendance is recorded accurately.
- **Impact on Data Subjects**:
  The processing of access card data is limited to monitoring entry and exit from the premises and does not involve excessive tracking of employees' movements. It only applies to work hours and business-related activities.
- **Mitigation Measures**:
  Access card data is stored securely and only accessible to authorized personnel. Employees are informed about the use of access cards and their purpose.
- **Conclusion**:
  The Company's legitimate interest in securing its premises and monitoring attendance outweighs the minimal impact on employee privacy. Therefore, this processing is justified.

4. Handling of Personal Data in the Record of Individual Alarm Codes

- **Purpose of Processing**:
  The Company processes data related to individual alarm codes to control access to restricted areas within its premises and ensure security.
- **Legitimate Interest**:
  The Company has a legitimate interest in maintaining the security of its premises, particularly sensitive areas that require restricted access.
- **Impact on Data Subjects**:
  The processing involves minimal intrusion into the privacy of employees since it

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

pertains to securing workspaces and is limited to work hours and areas requiring enhanced security.

- **Mitigation Measures**:
  Alarm code data is stored securely and accessible only to authorized security personnel. Employees are informed of the need for alarm codes and the purpose of monitoring access.
- **Conclusion**:
  The Company's legitimate interest in securing sensitive areas outweighs the limited impact on employee privacy. This processing is justified.

5. Handling of Personal Data through the Company's Surveillance Systems

- **Purpose of Processing**:
  The Company uses surveillance systems to monitor the premises and ensure the safety and security of employees, visitors, and property.
- **Legitimate Interest**:
  The Company's legitimate interest is to protect its property, prevent unauthorized access, and ensure the safety of everyone on its premises.
- **Impact on Data Subjects**:
  The use of surveillance systems may impact the privacy of individuals, but this is mitigated by limiting surveillance to common areas, entrances, and exits. No surveillance is conducted in private or sensitive areas such as restrooms.
- **Mitigation Measures**:
  Clear signage informs individuals of the presence of surveillance cameras. The data is stored securely and only accessible to authorized personnel. Video footage is retained for a limited period (typically 30 days) unless required for investigating an incident.
- **Conclusion**:
  The Company's legitimate interest in ensuring security outweighs the potential impact on the privacy of individuals. Therefore, the processing of surveillance data is justified.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Appendix 5: Sample Balancing of Interests Test

Example of a Balancing Test for Employee Contact Information

- **Purpose of Processing**:
  To facilitate internal communications and support business operations, the Company processes employee contact details (phone numbers, email addresses).
- **Legitimate Interest**:
  The Company's legitimate interest is to maintain effective communication between employees and departments to ensure smooth business operations.
- **Impact on Data Subjects**:
  The processing of contact information has minimal impact on the privacy of employees as it is strictly for business purposes and not shared externally.
- **Mitigation Measures**:
  The Company limits access to contact information to authorized personnel only, implements data security measures, and ensures that employees are informed about the use of their data.
- **Conclusion**:
  The legitimate interest of the Company in maintaining internal communications outweighs the minimal privacy impact on employees. The processing is justified.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Appendix 6: Sample Data Protection Impact Assessment

A **Data Protection Impact Assessment (DPIA)** is carried out when the processing of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. This includes assessing the risks, describing the processing activity, and identifying mitigation measures.

Example DPIA Structure:

- **1. Overview of Processing Activity**:
  Description of the data processing activity (e.g., the introduction of a new monitoring system for company vehicles).
- **2. Purpose and Legal Basis**:
  Explanation of why the processing is necessary, including the legitimate interest or legal obligation.
- **3. Risks to Data Subjects**:
  Identification of potential risks to the rights and freedoms of individuals (e.g., privacy invasion, data misuse).
- **4. Mitigation Measures**:
  A list of measures to mitigate these risks (e.g., restricting access to data, encrypting sensitive information, ensuring transparency with employees).
- **5. Data Retention and Security**:
  A description of how long the data will be retained and the security measures in place to protect it.
- **6. Consultation with Supervisory Authority (if required)**:
  If the DPIA reveals high risks that cannot be mitigated, the Company may consult the supervisory authority for advice before proceeding with the processing.

1. Description of Processing Activity

1.1 Purpose

The Company is implementing a new system for tracking company vehicles to optimize logistics and improve operational efficiency. This system will collect GPS data to monitor the location of company-owned vehicles in real time.

1.2 Categories of Data

The system will process the following categories of Personal Data:

- Vehicle location (GPS coordinates)
- Employee identification (driver)
- Driving behavior (speed, routes, stops)

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

1.3 Legal Basis
The processing is necessary for the legitimate interest of the Company in managing its fleet efficiently, ensuring safety, and reducing operational costs. Additionally, monitoring is essential to comply with internal security protocols.

2. Assessment of Necessity and Proportionality

2.1 Necessity of Processing
The collection of GPS data is necessary to ensure that vehicles are being used appropriately and efficiently, to monitor routes for safety, and to provide support in case of vehicle theft or accidents.

2.2 Proportionality of Processing
The Company will limit the scope of data collection to what is strictly necessary. Only vehicle-related data will be collected, and no other personal activities of the employee will be tracked. Monitoring will only occur during working hours and for company vehicles.

3. Risks to Data Subjects

3.1 Identification of Risks
The processing presents the following risks to the rights and freedoms of employees:

- **Privacy concerns**: Employees may feel that their movements are being excessively monitored.
- **Data misuse**: There is a risk that GPS data could be used for purposes not initially intended (e.g., performance evaluations or disciplinary measures).
- **Data security**: The data could be exposed to unauthorized access, leading to privacy violations or misuse.

4. Mitigation Measures

The Company will implement the following measures to mitigate risks:

- **Transparency**: Employees will be informed of the purpose of the GPS tracking and how the data will be used. Clear policies will be established, and consent will be obtained where necessary.
- **Access Controls**: Only authorized personnel will have access to the GPS data, and access will be logged and monitored to prevent misuse.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

- **Data Minimization**: Data collection will be limited to essential information (location of vehicles and driving patterns). No personal data unrelated to the use of the company vehicle will be collected.
- **Data Retention**: GPS data will be retained for a limited period (e.g., 6 months) and will be deleted unless needed for legal purposes (e.g., in case of an accident or theft investigation).
- **Encryption**: GPS data will be encrypted both in transit and at rest to protect it from unauthorized access.
- **Anonymization**: Where possible, data will be anonymized to reduce the risk of identifying individual employees.

5. Evaluation of Residual Risks

After implementing the above measures, the Company assesses that the risks to employees' rights and freedoms have been sufficiently minimized. The remaining risks are considered low and manageable with the implemented safeguards.

6. Data Protection Officer (DPO) Consultation

The DPO has reviewed the DPIA and concurs that the risks have been adequately addressed through the proposed mitigation measures. The DPO has also verified that the processing complies with GDPR requirements and that employees' rights are respected.

7. Consultation with Supervisory Authority (if required)

If any residual high risks are identified that cannot be mitigated (e.g., if GPS tracking is deemed to significantly impact the privacy of employees), the Company will consult with the relevant data protection authority before proceeding with the processing.

8. Final Decision

The Company will proceed with the implementation of the GPS tracking system, subject to the implementation of all recommended mitigation measures. Regular audits will be conducted to ensure compliance, and the DPIA will be reviewed annually or when significant changes occur in the processing activities.

CLAIR
creating the flow.

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

Appendix 7: Records of Data Processing Activities as a Data Processor

The Company maintains a record of all data processing activities carried out as a Data Processor, in accordance with Article 30 of the General Data Protection Regulation (GDPR). This appendix details the Company's obligations and responsibilities when processing Personal Data on behalf of another Data Controller.

1. Structure of Records

The records of data processing activities as a Data Processor must include the following information:

- **Name and Contact Details of the Data Controller**:
  The identity and contact details of the Data Controller or Controllers on whose behalf the processing is carried out. If applicable, details of the Data Protection Officer (DPO) and any representative must also be included.
- **Categories of Processing**:
  A description of the categories of processing carried out on behalf of the Data Controller, including the type of Personal Data processed, the categories of Data Subjects, and the purposes of processing.
- **Transfers to Third Countries or International Organizations**:
  Details of any transfers of Personal Data to third countries or international organizations, including the identification of such countries or organizations and any safeguards applied to protect the data during the transfer.
- **Retention Period**:
  The periods for which the Personal Data is stored, in accordance with the instructions of the Data Controller and relevant legal requirements.
- **Security Measures**:
  A general description of the technical and organizational security measures in place to ensure the protection of Personal Data. These measures must align with the Data Controller's instructions and GDPR requirements.

2. Data Processor Obligations

As a Data Processor, the Company is obligated to adhere to the following principles:

- **Processing Instructions**:
  The Company will process Personal Data only based on documented instructions

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

from the Data Controller, including with respect to any transfers to a third country or international organization.

- **Confidentiality**:
  The Company ensures that all personnel authorized to process Personal Data are subject to a strict confidentiality obligation. Only authorized personnel who need access to the data for their duties are granted such access.
- **Security of Processing**:
  The Company implements appropriate technical and organizational measures to ensure the security of the processing, in accordance with the requirements set out by the Data Controller.
- **Sub-processors**:
  The Company may engage sub-processors only with prior authorization from the Data Controller. The Company ensures that any sub-processor complies with the same data protection obligations by entering into a contract that mirrors the conditions set out in the contract between the Data Controller and the Company.
- **Assistance to the Data Controller**:
  The Company provides assistance to the Data Controller to facilitate the exercise of Data Subjects' rights (e.g., access, rectification, erasure) and ensure compliance with data protection obligations, including data security, data protection impact assessments (DPIA), and reporting data breaches.
- **Erasure or Return of Data**:
  Upon termination of the contract or upon the Data Controller's request, the Company will either delete or return all Personal Data processed on behalf of the Data Controller, unless retention is required by law.
- **Audit Support**:
  The Company will make available all necessary information to the Data Controller to demonstrate compliance with data processing requirements and allow audits or inspections by the Data Controller or an authorized third party.

3. Documentation of Processing

The Company is responsible for maintaining accurate and up-to-date documentation of all data processing activities carried out on behalf of the Data Controller. This documentation must be available to the supervisory authorities upon request and should include:

- A description of the processing activities, including the categories of data processed and the purposes for which the processing occurs.
- Details about any sub-processors involved in the data processing.
- Information about the security measures in place to protect Personal Data.

4. Review and Updates

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

The Company regularly reviews and updates its records of processing activities to ensure compliance with GDPR requirements. Any significant changes to the processing activities or the security measures implemented by the Company are documented and reported to the Data Controller as required.

Client Name	Data Processing Description	Location/Format	Categories of Personal Data Processed	Purpose of Processing	Duration
Henkel Magyarország Kft.	Fa AP Code Sweepstakes	Microsite focipromo.hu	Name, Email Address, IP Address	Participation in sweepstakes and drawing	Duration of sweepstakes (June 8)
Henkel Magyarország Kft.	Barnangen AP Code Sweepstakes	Microsite livelagom.hu	Name, Email Address, IP Address	Participation in sweepstakes and drawing	Duration of sweepstakes (July 31)
Henkel Magyarország Kft.	Syoss AP Code Sweepstakes	Microsite ilovesyoss.hu	Name, Email Address, IP Address	Participation in sweepstakes and drawing	Duration of sweepstakes (July 7)
újHÁZ Centrum	Vespa AP Code Sweepstakes	Microsite vespa.ujhazcentrum.hu	Name, Email Address, IP Address, City of residence	Participation in sweepstakes and drawing	Duration of sweepstakes (May 31)
újHÁZ Centrum	Pöttöm Fürdő Program	Microsite pottomfurdo.ujhazcentrum.hu	Contact details, personal data required for application	Participation in program	Until closure or completion
újHÁZ Centrum	Facebook Page Content	Facebook	Facebook	Communication and community	Ongoing / as per

claircommunication.com
info@claircommunication.com

H-1025 Budapest,
Szemlőhegy u. 36.
B. I.ház., fsz 1.

	and Community Management		Username	management tasks	contract duration
újHÁZ Centrum	Instagram Content and Community Management	Instagram	Instagram Username	Communication and community management tasks	Ongoing / as per contract duration
újHÁZ Centrum	Newsletter	SalesAutopilot	Name, Email Address	Sending newsletters	Until unsubscription

STIHL	Facebook Page Content and Community Management	Facebook	Facebook Username	Communication and community management tasks	Sweepstakes duration (June 8)
STIHL	Instagram Page Content and Community Management	Instagram	Instagram Username	Communication and community management tasks	Sweepstakes duration (July 31)
STIHL	Newsletter	SalesAutopilot	Name, Email Address, IP Address	Sending newsletters	Until unsubscription
Clair & Curtis	RPM Testing	realpeoplemarketing.hu	Contact details, answers to questionnaire	Selection of testers, market research	Until project completion