

DATA PROCESSING INFORMATION

Fortis Distribution Limited Liability Company

1. Data controller

Name: Fortis Distribution Limited Liability Company Registered
Registered office: 1133 Budapest, Váci út 76. 3rd floor
Company registration number: 01-09-346319
Tax number: 27042063-2-41
Address of actual data processing: 1133 Budapest, Váci út 76. 3rd floor.
Website: <https://fortis-distribution.com/>
Telephone number: +36 30 851 8178
E-mail: welcome@fortis-distribution.com
Website: <https://fortis-distribution.com/>
Independently represented by: Konstantin Monakhov

2. Introduction

The Data Controller attaches great importance to the protection of personal data and continuously ensures the security of personal data. The Data Controller complies in all respects with the data protection provisions of the applicable legislation and with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

This data processing notice is available on the Data Controller's website. The Data Controller may amend the content of this notice at any time, in which case it shall inform the data subjects in a timely manner.

3. Definitions

1. **Data subject:** any natural person who is identified or can be identified, directly or indirectly, on the basis of specific personal data, e.g. an employee, a natural person applying for a job, a natural person using the Data Controller's services.
2. **Personal data:** any information relating to an identified or identifiable natural person (i.e. the data subject); 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.
3. **Special data:** any data belonging to special categories of personal data, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.
4. **Data file:** the totality of data managed in a single register.
5. **Consent:** a voluntary and definite expression of the will of the data subject, based on adequate information, by which he or she gives his or her unambiguous consent to the processing of personal data relating to him or her, either in full or for specific operations.
6. **Data controller:** the natural or legal person or organization without legal personality who, alone or jointly with others, determines the purposes of data processing, makes and implements decisions regarding data processing (including the means used), or has them implemented by a data processor commissioned by them. Under this Policy, the Data Controller is the person specified in Chapter IV.
7. **Data processing:** any operation or set of operations performed on data, regardless of the procedure used, in particular collection, recording, storage, organizing, storing, altering, using, retrieving, transmitting, disclosing, aligning or combining, blocking, erasing and destroying data, as well as preventing further use of data, taking photographs, making audio or video recordings, and recording physical characteristics suitable for identifying a person.
8. **Restriction of processing:** marking stored personal data for the purpose of restricting their future processing.
9. **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 aspects relating to the performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
10. **Pseudonymization:** processing personal data in such a manner that the personal data can no longer be attributed to a specific natural person 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.
11. **Data disclosure:** making data available to a specific third party.

-
12. **Data processing:** the performance of technical tasks related to data processing operations, regardless of the method and means used to perform the operations and the location of the application, provided that the technical task is performed on the data. E.g. performing legal advisory tasks.
 13. **Data erasure:** rendering data unrecognizable in such a way that it can no longer be recovered.
 14. **Data blocking:** marking data with an identifier for the purpose of restricting its further processing for a definite or indefinite period of time.
 15. **Data destruction:** the complete physical destruction of the data carrier containing the data. E.g. shredding of documents, destruction of hard drives.
 16. **Recording system:** a structured set of personal data organised in any manner, whether centralised, decentralised, or organised according to functional or geographical criteria, which is accessible on the basis of specific criteria.
 17. **Third party:** a natural or legal person or an organization without legal personality who or which is not the data subject, the data controller or the data processor, or persons who, under the direct authority of the data controller or data processor, are authorized to process personal data.
 18. **Data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
 19. **Partner:** legal entities and business associations without legal personality that use the Data Controller's services on a contractual basis and/or facilitate the performance of the Data Controller's services (performance assistants) to whom the Data Controller - with the consent of the data subject - may transfer or forward personal data, or which perform or may perform data storage, processing, related IT and other activities facilitating secure data management for the Data Controller;
 20. **Employee:** a natural person in a contractual, employment or other legal relationship with the Data Controller who is entrusted with the task of providing or performing the Data Controller's services and who comes into contact with personal data in the course of their data management or data processing tasks, and for whose activities the Data Controller assumes full responsibility towards the data subjects and third parties.
 21. **Data owner:** the Employee who generated the data and/or who has access to the data and/or to whom the data was transferred by another data owner or third party and/or who came into possession of the data in any other way.
 22. **Website:** the portal and all its subpages operated by the Data Controller.
 23. **Community site:** the online platform maintained by the Data Controller.

Data processing principles

1. "Principle of purpose limitation": Personal data may only be processed for a specific purpose, for the exercise of a right or for the fulfillment of an obligation. Data processing must be consistent with the purpose of the data processing at all stages, and the collection and processing of data must be fair and lawful.
2. "Principle of lawfulness, fairness and transparency": Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
3. Principle of "proportionality, necessity" or "data minimization": Only personal data that is essential for the purpose of data processing and suitable for achieving that purpose may be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose. Accordingly, the Data Controller shall only process data that is absolutely necessary.
4. Principle of "accuracy": During data processing, the accuracy, completeness and, if necessary for the purpose of data processing, the up-to-date nature of the data must be ensured, as well as the fact that the data subject can only be identified for as long as is necessary for the purpose of data processing.
5. Principle of "limited storage": Personal data must be stored in a form that allows the data subjects to be identified only for as long as is necessary to achieve the purposes of the processing of personal data; Personal data may be stored for longer periods only if the processing of personal data is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of Regulation (EU) 2016/679, for scientific and historical research purposes or for statistical purposes, subject to the implementation of appropriate technical and organizational measures provided for in this Regulation in order to safeguard the rights and freedoms of the data subjects.
6. Principle of "integrity and confidentiality": By applying appropriate security measures to protect personal data stored in automated data files, the Data Controller shall ensure that accidental or unlawful destruction or accidental loss, as well as unauthorized access, alteration or dissemination, are prevented.

-
7. Principle of "accountability": The Data Controller is responsible for compliance with the provisions of the above paragraphs and the Policy, and must be able to demonstrate such compliance.
 8. The principle of "privacy by design": a very conscious approach to data protection, which, in a nutshell, means that when determining the method of data processing and during data processing, the Data Controller implements appropriate technical and organizational measures—such as pseudonymization—with the aim of effectively implementing the above principles, fulfilling obligations, incorporation of legal safeguards, etc., and does so in a regulated and detailed manner. In practice, this mindset is promoted through employee training, data protection awareness, and impact assessments, risk analyses, and balancing tests used during the introduction and/or regular review of individual data processing operations.
 9. Personal data retains its quality during data processing as long as the relationship with the data subject can be restored. The relationship with the data subject can be restored if the data controller has the technical conditions necessary for restoration.

4. Purpose and legal basis of personal data processing, scope of data processed

A.) General provisions relating to specific data processing activities, the use of services provided by the Data Controller, and data processing based on the contractual relationship between the Parties

1. As a general rule, all data processing activities and services provided by the Data Controller are based on the voluntary consent of the data subject, and their general purpose is to ensure the provision of services and to maintain contact.
2. The above general rule is supplemented by data processing required by law, about which the Data Controller informs the data subjects when determining the specific data processing operations.
3. As a general rule:
 - for certain services, it is possible to provide additional data that helps to fully understand the data subject's needs, but this is not a condition for using the services provided by the Data Controller.
 - Personal data provided during any data processing activity shall be stored by the Data Controller in separate data files, separately from other data provided. These data files may only be accessed by the Data Controller's authorized employee(s).
 - You may request the modification, deletion, and/or blocking of data recorded and stored during any data processing activity, as well as detailed information about data processing, by sending a request to the email address indicated in Section IV/1, unless other contact details are provided in the description of the data processing activity in question.
 - The provision of data by the data subject during each data processing activity is a condition for using the services provided by the Data Controller.
4. The Company may process the following data of natural persons who have entered into a contract with it as customers for the purpose of performing the contract, concluding a legal transaction between the parties, fulfilling or terminating such transactions or orders: name, birth name, date of birth, mother's name, address, tax identification number, tax number, entrepreneur or primary producer ID number, personal ID number, personal identification number, address, registered office, business address, telephone number, email address, website address, bank account number, customer number.

This data processing is also considered lawful if it is necessary to take steps at the request of the data subject prior to entering into a contract (e.g., requesting a quote). Personal data controllers: the Company's front-office and back-office staff performing customer service tasks, staff performing accounting and tax tasks, and data processors. Duration of personal data storage: 5 years after the termination of the contract.

5. The data subject must be informed before the start of data processing that the data processing is based on the legal title of contract performance; this information may also be provided in the contract. The data processing consent related to the contract concluded with the natural person is included in the annex to this policy.
6. Contact details of natural persons representing legal entity customers, buyers, and suppliers:
 - Scope of personal data that may be processed: name, address, telephone number, e-mail address, online ID of the natural person.
 - Purpose of personal data processing: performance of a contract concluded with the Company's legal entity partner, maintaining business relations, legal basis: consent of the data subject.
 - Duration of personal data storage: for 5 years following the existence of the business relationship or the status of the data subject's representatives.

B.) Data processing related to marketing

Sending newsletters

1. Before or during the use of the services, or in any other way, you may subscribe to the newsletter with the data specified below.
2. Subscribing to the newsletter is based on voluntary consent.

3. Data subjects: Any natural person who wishes to receive regular updates from the Data Controller and therefore subscribes to the newsletter service by providing their personal data.

4. Scope and purpose of the data processed:

name	identification
e-mail address	sending newsletters

1. The purpose of data processing related to sending newsletters is to provide the recipient with comprehensive general or personalized information about the Data Controller's latest events, news, and promotional products.
2. The newsletter is sent by an employee entrusted with this task.
3. Newsletters are sent only with the prior consent of the data subject.
4. The Data Controller shall only process personal data collected for this purpose until the data subject unsubscribes from the newsletter list or gives confirmation.
5. The data subject may unsubscribe from the newsletter at any time by sending a cancellation request to the email address provided at the bottom of the electronic letters and in Section IV/1. Unsubscribing is also possible by sending a letter to the Company's registered office.
6. The Data Controller reviews the newsletter list every three years and requests confirmation of consent to send the newsletter after three years. The Data Controller will delete the data of any data subject who does not give their confirmation of consent from the database.
7. Duration of data processing: until deletion at the request of the data subject or if the data subject does not give further consent.
8. The Data Controller keeps statistics on the readability of the newsletters sent out.
9. The data subject may comment on the news feed published on social media sites, in particular on the message wall of the Facebook page, using the comment function available on the site.
You can subscribe by clicking on the "like" link and unsubscribe by clicking on the "dislike" link located in the same place. You can also delete unwanted news feeds appearing on the message wall using the message wall settings. You can find information about social media feeds, subscriptions and unsubscriptions, and data management on the social media site itself.

Presence and marketing on social media sites:

1. The Data Controller is available on Facebook and other social media sites.
2. The use of social media sites, in particular Facebook, and the use of these sites to contact and communicate with the Data Controller, as well as other activities permitted by the social media site, are based on voluntary consent.
3. Data subjects: Natural persons who voluntarily follow, share, or like the Data Controller's social media pages, in particular the page on facebook.com or the content appearing on it.
4. Scope and purpose of data processing:

public name of the data subject	identification
public photo of the data subject	identification
public email address of the data subject	contact
message sent by the data subject on a social networking site	contact
evaluation of the data subject	quality improvement

5. The Data Controller communicates with data subjects exclusively via the social media site, and thus the purpose of the scope of data processed becomes relevant only if the data subject contacts the Data Controller via the social media site.
6. The purpose of our presence on social media platforms, especially Facebook, and the related data processing is to share, publish, and market the content of our website on social media. The social media page allows data subjects to stay informed about our latest promotions.
7. Based on the terms and conditions of the social media site, the data subject voluntarily consents to following and liking the Data Controller's content.
8. The data subject may evaluate the Data Controller in writing and numerically, if the social media site allows this.
9. The Data Controller also publishes images/videos on its social media page, in particular on its Facebook page, about various events, the Data Controller's services, and other matters. The Data Controller may link its Facebook page to other social media sites in accordance with the rules of the facebook.com social media portal, so publication on the Facebook page shall also be understood to mean publication on such linked social media portals.

-
10. If the images are not mass recordings or recordings of public figures (Civil Code 2:48), the Data Controller will always request the written consent of the data subject before publishing the images.
 11. Information about data processing on a given social media site can be obtained on that social media site.
 12. Duration of data processing: until deletion at the request of the data subject.

Website visit data:

1. When visiting the website specified in Section IV/1, the web server does not record user data.
2. The Data Controller's website may also contain links to pages that are not operated by the Data Controller, but are provided for the information of visitors. The Data Controller has no influence on the content and security of websites operated by partner companies and is therefore not responsible for them. Please review the data management policy and privacy statement of the sites you visit before providing your data in any form on those sites.
3. The Data Controller uses the following cookies:
 - a.) Essential cookies: These cookies are essential for the website to function properly. Without accepting these cookies, the Data Controller cannot guarantee that the website will function as expected, nor that the user will be able to access all the information they are looking for. These cookies do not collect personal data from the data subject or data that can be used for marketing purposes.
 - b.) Functional cookies: These cookies ensure that the website is consistently tailored to the data subject's needs and remember the settings chosen by the data subject.
 - c.) Targeted cookies: Targeted cookies ensure that the advertisements displayed on the website are tailored to the data subject's interests.
4. The Data Controller places a set of codes on the website (or any of its subpages) for the purpose of making the Data Controller's advertisement advertisements to users visiting the website while they are browsing Google's websites and/or searching for terms related to the Data Controller or the Data Controller's services in the Google system. The code set does not collect, store or transmit personal data. More information on the use and operation of the code set can be found at <http://support.google.com>.
5. Based on the above, the Data Controller does not use analytical systems to collect personal data.
6. The Data Controller draws users' attention to the fact that most internet browsers automatically accept cookies, but visitors have the option to delete them or automatically reject them.

Customer database

1. On the website, the registering natural person may give their consent to the processing of their personal data by ticking the relevant box. It is prohibited to pre-tick the box.
2. The scope of personal data that may be processed: the natural person's name (surname, first name), address, telephone number, e-mail address, online identifier.
3. The purpose of processing personal data:
 - To provide the services offered on the website.
 - Contacting you by email, telephone, SMS, and post.
 - Providing information about the Company's services, terms and conditions, and promotions.
4. The legal basis for data processing is the consent of the data subject.
5. Recipients of personal data and categories of recipients: the Company's customer service and marketing staff, and the Company's IT service provider's hosting staff acting as data processors.
6. Duration of storage of personal data: until the registration/service exists or until the data subject withdraws their consent (requests deletion).

C.) Operational data processing Request for information

1. The Data Controller allows data subjects to request information from the Data Controller by providing the data detailed below.
2. The request for information is based on voluntary consent.
3. Data subjects: Any natural person who contacts the Data Controller and requests information from the Data Controller, providing their personal data.
4. Scope and purpose of data processing:

addressing	identification
name	identification
address	contact
phone	contact
e-mail address	contact
message text	required for reply

5. The purpose of data processing is to provide the data subject with appropriate information and to maintain contact.
6. The activity and process involved in data processing is as follows: The data subject may consult with the Data Controller about the Data Controller's services, products, and/or other related issues in a manner made available to them by the Data Controller. Data provided to the Data Controller via the website is sent by email. The Data Controller will respond to the data subject's question through the Employee entrusted with this task and will send it to the data subject in the same way as the request for information was received, unless the data subject specifies otherwise. In accordance with the purpose of data processing, the data subject voluntarily consents to the Data Controller contacting them via the contact details provided in the information request in order to clarify the question or respond to it.
7. Duration of data processing: until the purpose is achieved.

D.) Processing of data of job applicants

1. The Data Controller allows data subjects to apply for the job vacancy advertised by it in the manner specified in the job advertisement (e.g. electronically or on paper). Unsolicited applicants are also selected.
2. The Data Controller does not differentiate between CVs containing personal data received for the purpose of applying for a job based on the method of their receipt: CVs received in paper form and electronically are subject to the same assessment.
3. The Company stores the data of applicants electronically and/or in a lockable file cabinet.
4. The personal data of job applicants is accessible to the Data Controller's management and HR staff.
5. Applying for a job is based on voluntary consent.
6. Data subjects: Any natural person who applies for a job advertised by the Data Controller or sends their CV to the Data Controller.
7. Scope and purpose of the data processed:

name	identification
place and date of birth	identification
e-mail address	contact
address	contact
name of position applied for	Application ID
list of previous work experience	necessary for assessing the position and selecting the employee with the appropriate skills
educational qualifications	required for assessing the position and selecting an employee with the appropriate skills
Knowledge of foreign languages	necessary for assessing the position and selecting an employee with the appropriate skills
special data: e.g. health data, medical data of persons with changed working capacity	special data is only processed if it is necessary for filling the position
Other data indicated in the CV submitted	necessary for assessing the position and selecting an employee with the appropriate skills
cover letter submitted	necessary for assessing the position and selecting the employee with the appropriate skills

indication of consent to the processing of data for 2 years after application, if the data subject is not hired	necessary for the legal basis for further data processing in the event of non-selection
---	---

8. The purpose of data processing is to apply for a job, participate in the selection process, fill the advertised position, and maintain contact.

9. Activities and processes affected by data processing:

- The relevant organizational unit manager is responsible for selecting the appropriate employee and is therefore obliged to ensure the rights of the data subjects when performing tasks related to this data processing.
- The data subject submits their data to the Data Controller in accordance with the job application or for the purpose of expressing interest.
- Applications are typically, but not exclusively, submitted electronically, by email.
- During the selection process, the data controller reviews the applications and invites the most suitable candidates for a personal interview based on a comparison.
- The selection process continues with a personal interview and, where appropriate, a professional test.
- The selection process ends with the conclusion of a contract with the most suitable candidate.
- The Data Controller shall notify the applicants of the outcome of the selection process and request the consent of the unsuccessful applicants (see Annex) to the further processing of their data for a period of two years following the application for the purpose of filling a position that is the same or similar to the one applied for or that matches the skills of the data subject.
- The Data Controller may only continue to process the data of unsuccessful applicants if they have given their separate consent and requested this in a separate, verifiable manner. The Data Controller shall link such consents to the data and store them.
- The data subject acknowledges that if they have provided a reference person when applying for a job, the Data Controller may contact that person for the purpose of verifying the data subject's professional experience.
- The data subject acknowledges that the Data Controller may view the information created on the data subject's social media page that is publicly available to anyone. If data found on the internet becomes part of the evaluation, the Data Controller must provide the data subject with the opportunity to review and dispute it.

10. Duration of data processing: until the purpose is achieved, i.e. until the advertised position is filled, the employment contract is concluded, or, based on the consent of the data subject, until 2 years have elapsed since the application, or until the data subject requests deletion in the meantime.

E.) Complaint handling:

1. The Data Controller provides the data subject with the opportunity to submit complaints regarding the ordered product and/or the Data Controller's conduct, activities, or omissions verbally (in person, by telephone) or in writing (by e-mail, by post).

2. Data subjects: Any natural person who wishes to lodge a complaint about the Data Controller's activities.

3. Purpose of data processing:

To identify the data subject and the complaint, and to record the data required by law.

4. Scope and purpose of data processing:

Name	identification
complaint ID	Identification
date of receipt of the complaint	identification
telephone number	contact
personal data provided during the conversation	identification
billing/mailling address	contact
the product/activity/omission complained about	investigation of the complaint
the complaint	investigation of the complaint

5. The purpose of data processing is to ensure that complaints can be made and to maintain contact.

6. Activities and processes affected by data processing:

- The data subject communicates their complaint to the Data Controller verbally or in writing.
- If the data subject makes the complaint verbally, the Data Controller shall take minutes of it.
- The Data Controller shall investigate and respond to complaints received within a reasonable time.

-
7. Duration of data processing:
Pursuant to Section 17/A(7) of Act CLV of 1997 on Consumer Protection, the Data Controller shall retain the minutes of the complaint and a copy of the response for five years.

F.) Data processing related to online data requests

1. Data subjects: persons requesting offers or their representatives.
2. Purpose of data processing: Establishing and maintaining contact, sending personalized offers.
3. Legal basis for data processing: Data processing is necessary for taking steps at the request of the data subject prior to entering into a contract (GDPR Article 6(1)(b)).
4. Scope and purpose of data processing:

Name	identification
telephone number	contact
e-mail address	contact

5. Duration of data processing: We store data for two years after the expiry of the binding period of the offer.

5. Rights of data subjects

1. The Data Controller informs data subjects that they may exercise their rights in person or by sending a request to the Company's email address or postal address, and may also request information at these contact details.
2. The Data Controller shall examine and respond to the statement as soon as possible after receipt, but within a maximum of 25 days, and shall take the necessary steps in accordance with the statement, the Policy, and the law.
3. 5. Right to information, or otherwise known as the data subject's "right of access": at the request of the data subject, the Data Controller shall provide information on:
 - the data processed by it and the categories of personal data,
 - the purpose of the data processing,
 - the legal basis for data processing,
 - the duration of data processing,
 - the duration of data storage or, if this is not possible, the criteria for determining this duration,
 - if the data were not collected from the data subject, information about their source,
 - where applicable, automated decision-making, including profiling, and the logic involved, as well as meaningful information about the significance of such processing and the expected consequences for the data subject,
 - the details of the data processor, if a data processor has been engaged,
 - the circumstances and effects of the data breach and the measures taken to remedy it, and
 - in the case of transfer of the data subject's personal data, the legal basis, purpose and recipient of the data transfer.
4. The information is free of charge if the person requesting the information has not yet submitted a request for information to the Data Controller for the same data set in the current year. In other cases, a fee may be charged. Any fees already paid shall be refunded if the data has been processed unlawfully or if the request for information has led to a correction.
5. The Data Controller shall refuse to provide information if, on the basis of a law, an international treaty or a binding legal act of the European Union, the data controller receives personal data in such a way that the data controller transferring the data informs the data subject at the same time as the data transfer of the restriction of his or her rights under the said law or of other restrictions on the processing of the data, the external and internal security of the state, such as national defense, national security, the prevention or prosecution of criminal offenses, the security of the execution of penalties, as well as the economic or financial interests of the state or local government, the significant economic or financial interests of the European Union, and disciplinary and ethical offenses related to the practice of professions, for the purpose of preventing and detecting breaches of labor law and occupational safety obligations, including in all cases control and supervision, and for the protection of the rights of the data subject or others.
6. The data controller shall notify the National Authority for Data Protection and Freedom of Information of any rejected requests for information by January 31 of the year following the year in question.
7. Right to rectification: The data subject shall have the right to obtain from the Data Controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. If the personal data is inaccurate and

If the Data Controller has access to personal data that is accurate, the Data Controller shall correct the personal data without delay, even without a request from the data subject.

8. Right to erasure, or "right to be forgotten": The data subject has the right to request that the Data Controller erase personal data concerning him or her without undue delay, and the Data Controller is obliged to erase personal data concerning the data subject without undue delay, unless mandatory data processing precludes this. In addition to the above case, the Data Controller shall erase the data if:
 - the processing of the data is unlawful;
 - the data is incomplete or incorrect - and this situation cannot be remedied lawfully - provided that the deletion is not excluded by law;
 - the purpose of the data processing has ceased to exist or the statutory time limit for storing the data has expired;
 - it has been ordered by a court or the Authority;
 - the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
 - the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
 - the personal data must be erased for compliance with a legal obligation in the law applicable to the Data Controller;
 - the personal data has been collected in relation to the offering of information society services referred to in Article 8(1) of Regulation (EU) 2016/679, which are directly addressed to children.
9. Where the Data Controller has made the personal data public for any reason and is obliged to erase it in accordance with the above, it shall take reasonable steps, taking into account the available technology and the cost of implementation, including technical measures, to inform other data controllers processing the data that the data subject has requested the deletion of links to, or copies or replications of, the personal data in question.
10. The data controller draws the attention of data subjects to the limitations of the right to erasure or "right to be forgotten" under EU regulations, which are as follows:
 - exercising the right to freedom of expression and information;
 - compliance with an obligation laid down by Union or Member State law to which the controller is subject, or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - public interest in the area of public health;
 - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of Regulation (EU) 2016/679, in so far as the right to erasure is likely to render impossible or seriously impair such processing; or
 - the establishment, exercise, or defense of legal claims.
11. Right to restriction of processing and blocking: The data subject has the right to request that the Data Controller restrict the processing of their data. If, based on the information available, it can be assumed that erasure would prejudice the legitimate interests of the data subject, the data must be blocked. Personal data blocked in this way may only be processed for as long as the purpose of the processing that precluded the erasure of the personal data exists. If the data subject disputes the accuracy or correctness of the personal data, but the inaccuracy or incorrectness of the disputed personal data cannot be clearly established, the data shall be blocked. In this case, the restriction shall apply for a period enabling the Data Controller to verify the accuracy of the personal data. The data shall be blocked if the data processing is unlawful and the data subject opposes the erasure of the data and requests the restriction of their use instead, or the Data Controller no longer needs the personal data for the purposes of the processing, but the data subject requires them for the establishment, exercise, or defense of legal claims, or the data subject has objected to the processing; in this case, the restriction applies for the period until it is determined whether the legitimate grounds of the Data Controller take precedence over the legitimate grounds of the data subject. Where processing is restricted (blocked), such personal data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.
12. The data controller draws the attention of data subjects to the fact that their right to rectification, erasure, and blocking may be restricted by law in the interests of external and internal security, including national defense, national security, the prevention or prosecution of criminal offenses, the security of the execution of penalties, as well as the economic or financial interests of the state or local government, the significant economic or financial interests of the European Union, and disciplinary and ethical offenses related to the practice of professions, the prevention and detection of breaches of labor law and occupational safety obligations, including in all cases control and supervision, and the protection of the rights of the data subject or others.
13. The Data Controller shall, without undue delay, within a maximum of 25 days from receipt of the request, inform the data subject of the details specified in the request and/or correct the data and/or delete and/or restrict (block) the data, or take other steps in accordance with the request, unless there are grounds for exclusion.
14. The Data Controller shall notify the data subject in writing of the rectification, erasure or restriction of data processing, as well as all those to whom the data had previously been transferred or disclosed for data processing purposes. At the request of the data subject, the Data Controller shall inform the data subject of these recipients. The notification may be omitted if, in view of the purpose of the data processing, it does not prejudice the legitimate interests of the data subject, or if the provision of information proves impossible or would involve a disproportionate effort. The Data Controller shall also notify the data subject in writing if the data subject's exercise of his or her rights cannot be realized for any reason, and shall specify the factual and legal reasons and the legal remedies available to the data subject: the possibility of recourse to the courts and the National Data Protection and Freedom of Information Authority.
15. The "right to data portability": The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the Data Controller, in a structured, commonly used and machine-readable format, and to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent and is carried out by automated means. The data

When exercising their right to portability, the data subject shall have the right to request the direct transfer of personal data between controllers, where technically feasible. The exercise of this right shall not affect the right to erasure. This right shall not apply if 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 controller. The exercise of this right shall not adversely affect the rights and freedoms of others.

16. Right to object: The data subject may object to the processing of his or her personal data, including profiling, if
 - the processing (transfer) of personal data is necessary solely for the enforcement of the rights or legitimate interests of the data controller or data recipient, except in the case of mandatory data processing;
 - the personal data is used or transferred for the purposes of direct marketing, public opinion polling, or scientific research;
 - the exercise of the right to object is otherwise permitted by law.The data subject may also object to the processing of personal data for direct marketing purposes pursuant to Article 21(3) of Regulation (EU) 2016/679, in which case the personal data may no longer be processed for this purpose.
Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject shall have the right to object, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
17. The Data Controller shall examine the objection within the shortest possible time, but no later than 25 days from the date of submission of the request, and shall inform the applicant in writing of the outcome. If the applicant's objection is justified, the Data Controller shall terminate the data processing, including further data collection and data transfer, and shall block the data, and shall notify all those to whom the personal data concerned by the objection has been previously transferred, and who are obliged to take measures to enforce the right to object.
18. If the data subject disagrees with the decision of the Data Controller, or if the Data Controller fails to meet the deadline referred to, the data subject shall be entitled to appeal to the court within 30 days of notification.
19. Rights of the data subject in relation to automated decision-making, including profiling: Decisions based solely on automated processing of personal data evaluating the personal characteristics of the data subject may only be made if the decision is made in the course of concluding or performing a contract, provided that it is initiated by the data subject or is permitted by a law that also establishes measures to safeguard the legitimate interests of the data subject.
In the case of a decision made by automated data processing, the data subject shall be informed, upon request, of the method used and its essence, and the data subject shall be given the opportunity to express his or her opinion.
20. Enforcement by the courts: The data subject may bring the matter before the courts if their rights have been infringed. The court shall deal with the matter as a matter of priority. The data controller shall be responsible for proving that the data processing complies with the provisions of the law.
21. In case of violation of your right to self-determination regarding information, you may file a report or complaint with: National Authority for Data Protection and Freedom of Information Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c Telephone: +36 (1) 391-1400 Fax: +36 (1) 391-1410 www: <http://www.naih.hu> e-mail: ugyfelszolgalat@naih.hu
22. In the event of content that is offensive to minors, incites hatred, or is exclusionary, or in the event of a violation of the rights of a deceased person or defamation, you may file a report or complaint with: National Media and Communications Authority 1015 Budapest, Ostrom u. 23-25. Postal address: 1525. Pf. 75 Tel: (06 1) 457 7100 Fax: (06 1) 356 5520 E-mail: info@nmhh.hu
23. Legal rules on compensation and damages: In the event that the Data Controller violates the personal rights of the data subject by unlawfully processing their data or violating data security requirements, the data subject may claim damages from the Data Controller.

If the Data Controller has engaged a data processor, the Data Controller shall be liable to the data subject for any damage caused by the data processor and shall also be obliged to pay the data subject compensation for the violation of personal rights caused by the data processor. The Data Controller shall be exempt from liability for the damage caused and from the obligation to pay compensation if it proves that the damage or the infringement of the data subject's personal rights was caused by an unavoidable reason outside the scope of data processing.

No compensation shall be payable and no damages shall be claimed if the damage or the infringement of the personal rights of the data subject resulted from the intentional or grossly negligent conduct of the data subject.

6. Data transfer

The data subject agrees that the Data Controller may transfer their personal data to its affiliated companies and data processors.

In order to perform its administrative tasks, the Data Controller may transfer all or part of the personal data to a data processor, subcontractor, or performance assistant appointed by it as a data processor for the purpose of performing certain data processing operations.

If the Data Controller entrusts a third party with accounting, legal tasks, hosting/server services, system administration or other tasks that qualify as data processing tasks, the details of this partner, as a data processor, are specified in the annex to this information notice, together with the members of the affiliated companies.

7. Data security

1. The Data Controller shall ensure the security of the data. To this end, it shall take the necessary technical and organizational measures with regard to the data files stored on IT equipment.
2. The data controller shall ensure that the data security rules laid down in the relevant legislation are enforced.
3. It shall ensure the security of data, take the technical and organizational measures and establish the procedural rules necessary to enforce the applicable laws and data and confidentiality protection rules.
4. The Data Controller shall protect the data by appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction and damage, and against inaccessibility resulting from changes in the technology used.
5. When determining and applying measures to ensure data security, the Data Controller shall take into account the current state of technology and shall choose from among several possible data management solutions the one that ensures a higher level of protection of personal data, unless this would involve disproportionate difficulty.

10. Information about the website

Customers can visit the website free of charge without providing any personal data. However, access to certain parts of the website is subject to registration, during which the customer provides information that qualifies as personal data.

By submitting and sending the data and visiting the website, the customer consents to the data controller processing the data provided in accordance with the law and this policy, and also consents to the automated individual decision-making described below.

Under no circumstances will the data controller make the personal data obtained during registration available to others without the express consent of the data subject, except in cases of legal obligation or official proceedings, as well as to members of the group of companies and data processors.

Certain parts of the website use so-called "cookies" – files that are stored on the data subject's hard drive for the purpose of data recording and to facilitate the identification of the data subject and their subsequent visits. The data subject can set their browser to notify them when someone wants to send a cookie and can decide whether to accept it (for more information about cookies, visit <http://www.cookiecentral.com>).

The website logs the Internet addresses of computers, IP addresses, to record user visits. By analyzing this data, the data controller compiles statistics, for example, to determine which parts of the website are visited most frequently by users and how much time they spend there on each occasion. The Data Controller does not link IP addresses to any other data that could personally identify the data subject; the data is used for statistical purposes only.

The data controller may display advertisements on the website. The system collects personal data about users who click on the advertisement for this purpose. Google's Privacy Policy provides more information about the scope of this data and how it is used.

The Data Controller excludes all liability for damages resulting from the destruction, delayed arrival, or other errors of messages transmitted in electronic form.

Unless otherwise indicated, the content of the Website is the property of the Data Controller and is protected by copyright. The Data Controller reserves all rights in this regard.

The content of the website does not constitute tax or legal advice in any case; it is provided by the Data Controller for informational purposes only, and the Data Controller excludes any liability.

The Data Controller also excludes any compensation for damages arising from downloading or the unavailability of the website.

The Data Controller has no control over content downloaded by following external links on the website.

The Data Controller reserves the right to ban users and terminate their registration without prior notice or justification.

I. Appendix No. Data processors

Pozderka Law Office

1146 Budapest, Erzsébet Királyné útja 1/C, Building B, 4th floor