Privatlivspolitik

Privacy Policy

www.ecotrendwebshop.com

Effective: as of 18.06.2025 until further notice

Veres és Társai Kft. (Registered seat: 9700 Szombathely, Kárpáti Kelemen utca 19/A., Company registration number: 18-09-103666, VAT identification number: 11513898-2-18, Email: info@eco-trend.hu, Represented by: Magdolna VERES and István András ANTAL, managing directors) as the **Data Controller** fulfils its obligations in relation to the processing of personal data within the framework of this Privacy Policy.

1. Introductory Provisions, Purpose of the Privacy Policy

In order to comply with the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") and the Act CXII of 2011 on the Right to Informational Self-Determination and on the Freedom of Information (hereinafter: "Info Act"), the Data Controller sets out in this Privacy Policy the applicable data protection rules and the procedures related thereto, as well as expresses its respect for and protection of the principles set out in the Regulation.

The Controller acknowledges that it is bound by the contents of this Privacy Policy. The purpose of this Privacy Policy is to inform the Data Controller's customers, partners and clients about the processing of their personal data. The Data Controller shall process personal data only in accordance with the legal provisions in force and in strict compliance with their provisions, taking into account the principles set out in Article 5 of the GDPR:

- Principle of lawfulness, fairness and transparency,
- Principle of purpose limitation,
- Principle of data minimisation,
- Principle of accuracy,
- Principle of storage limitation.

The Data Controller is committed to the protection of the personal data of data subjects, and places utmost importance on respecting the right of the data subjects to self-determination. It processes the recorded personal data confidentially in accordance with data protection legislation. In addition, it will take all technical and organisational measures to ensure the secure storage of data. The data shall be protected by appropriate measures against unauthorised access, alteration, transmission, disclosure, erasure or destruction, as well as against accidental destruction and damage, and from becoming inaccessible due to changes in the technology used.

Personal, Material and Temporal Scope of the Privacy Policy:

The personal scope of this Privacy Notice applies to the Data Controller and the natural persons whose data are included in the processing covered by this Policy, as well as to persons whose rights or legitimate interests are affected by the processing.

Definitions:

Personal data means 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.

Processing of special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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.

Processing means, regardless of the procedure applied, any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data transfer means making the data available to a specific third party.

Disclosure means making the data available to anyone.

Data erasure means making data unrecognisable in such a way that data restoration is no longer possible.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Controller means the person who – alone or jointly with others – determines the purposes and means of the processing.

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

Data subject means any natural person identified or identifiable, directly or indirectly, on the basis of personal data.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

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

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

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Email means electronic mail. Its name refers to the method of writing or transmitting, which takes place entirely by electronic means using computer networks.

Internet (Internetworking System) is a global system of interconnected computer networks (a so-called meta-network) that connects the entire Earth, connecting government, military, commercial, business, educational, research, and other institutions, as well as individual users.

Website, webpage, web portal, homepage mean an electronic interface suitable for display and communication of information, which is typically located on servers connected to the Internet (Webserver). These sites, pages have a unique address (link) that is

used to navigate to the given site by typing it into a browser application. The technology of the websites allows hyperlinks between individual content elements and links (hypertext).

Cookies means code components used to provide convenience features for websites. There are two basic types. One is stored on the visitor's own machine, the other is stored on the server side; a so-called session cookie. From a processing point of view, the processing of session cookies must be regulated. The websites must inform visitors about the use of cookies and request their consent.

Electronic newsletter means information sent to the e-mail address of persons subscribed to the address list, typically created automatically and sent by an application designed for this purpose, for transactional, advertising or other campaign purposes.

2. Legal Basis and Purpose of Processing

Processing of personal data may be lawful only if and to the extent that at least one of the following conditions is met in accordance with Article 6 of the GDPR:

- the **data subject has given consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a **legal obligation** to which the controller is subject;
- processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
- 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;
- processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The Data Controller must verify the lawfulness of data processing at all stages of its activities, and may only process data and only to the extent, for which it can justify the purpose and legal basis. If the legal basis for the processing is no longer applicable, the processing is only lawful if another legal basis can be demonstrated, failing which the data must be deleted.

Hosting of the Website

Server and hosting provider: Unas Online Kft.

Address: 9400 Sopron, Kőszegi út 14.

The server and hosting service provider stores the personal data in its possession, but is not entitled to use it.

Information about the Cookies Used on the Website

Cookies are data files that are created by websites you visit. They make online navigation easier by saving the browsing data. Cookies allow websites to do the following:

- they keep you logged in;
- they allow websites to remember the website settings;
- they make it possible for the websites to recommend you locally relevant content.

Some cookies expire when the website is closed and some have a longer expiry date.

Legal Background of Cookies:

The background to processing is set out in the provisions of the GDPR, the Info Act and the Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services.

Legal Basis for Cookies:

The legal basis for processing is Article 6 (1) (f) of the GDPR for session cookies, Article 6 (1) (a) of the GDPR for other cookies (e.g. secure, analytics) and your consent in accordance with Section 5 (1) (a) of the Info Act.

Please note that the data subject declares by accepting the use of cookies on the website of the Data Controller that they are over 16 years of age. No person under the age of 16 may opt in or opt out of the use of cookies by this website. Pursuant to Article 8 (1) of the GDPR, the validity of declaration of consent to data processing by such person below the age of 16 requires the consent of their legal representative. The Data Controller is not in a position to verify the age and eligibility of the person giving consent, so the Data Subject guarantees that the data they provide is accurate.

The Following Cookies are Used on the Website:

Session cookie: These cookies are temporarily activated while browsing. That is, from the moment the user opens the browser window until the moment it is closed. As soon as the browser closes, all session cookies are deleted. No personal data is stored in a session cookie.

The website uses the following cookie for its operation: PHPSESSID.

Erasure of Cookies

The cookies placed by websites may be deleted from your device at any time using your browser. For details on how to delete or manage cookies, please, refer to your browser's Help menu. Also, you can set the browser to block cookies or request a notification each time your browser receives a new cookie. Blocking cookies may technically prevent you from using our website.

If you do not accept the use of cookies, certain features will not be available.

Initiating Contact, Enquiring via the Website

The Data Controller makes it possible for an interested party to contact it using any of the contact details indicated on the website. The data provided will only be used to contact the interested party.

The purpose of data processing is for the operator of the website to establish contact with interested parties and to provide them with a quotation.

Legal basis for processing:

In the case of enquiries and requests for information, data processing is based on voluntary consent pursuant to Article 6 (1) (a) of the GDPR. In the case of a quotation, the processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into the contract under Article 6 (1) (b) of the GDPR.

Duration of processing:

The personal data provided will be processed for different periods of time depending on the nature of the contact.

In the case of an inquiry or a contact initiated, the Data Controller will not store the data after the necessary information has been provided, unless the subject matter of the ad hoc initiated contact gives rise to a legally enforceable claim, in which case the data can be stored for a maximum of 5 years for the purpose of supporting the claim.

In the case of a given quotation, the data retention period is the period of the offer's validity, which is defined in Section 6:64-69 of the Civil Code.

If a business relationship is established, the data must be retained for 8 years in accordance with Section 169 (2) of the Accounting Act.

Product Order

The website of the Data Controller also offers interested parties the possibility to order products marketed by the Data Controller.

To order the selected products, the Customer will be asked to provide the following personal data:

- Name
- Email address
- Telephone number
- Company name
- EU VAT number
- Address(es): both invoicing and delivery addresses, if different

Data processor:

- National Tax and Customs Administration of Hungary (online invoicing)
- Delivery to door: DPD Hungary Kft., Magyar Posta Zrt., DACHSER Hungary Kft.
- Kereskedelmi és Hitelbank Zrt.
- Online invoicing software: Billingo (Billingo Technologies Zrt.)
- Accounting (V&T Vezetés és Tanácsadás Kft.)

Legal basis for processing: The processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into the contract under Article 6 (1) (b) of the GDPR.

In the case of issuing an invoice, the legal basis for data processing is the fulfilment of a legal obligation under Article 6 (1) (c) of the GDPR, which obligation is set out in the provisions of the Accounting Act.

Duration of processing:

The accounting documents issued must be retained for 8 years in accordance with Section 169 (2) of the Accounting Act.

3. Data Transfer to a Third Country

Data Transfer to a Third Country

On 10 July 2023, the European Commission adopted an adequacy decision for the new EU-US Data Privacy Framework, stating that personal data can be transferred securely from the European Union to organisation in the USA participating in the new framework as the United States ensures an adequate level of protection for personal data transferred from the EU to participating organisations in the USA. A prerequisite for joining the Trans-Atlantic Data Privacy Framework is that organisations in the USA, as data controllers, commit to implementing GDPR-compliant data protection measures. A list of organisation in the USA that have joined can be found at the following link: https://www.dataprivacyframework.gov/s/participant-search

The US authorities have access to personal data of EU citizens for law enforcement and national security purposes under the Trans-Atlantic Data Privacy Framework, subject to safeguards and must always bear in mind the principles of necessity and proportionality. The safeguards put in place by the USA also make transatlantic data flows in a more general sense easier, as they are applicable even if the transfer is facilitated by using other instruments, such as general terms and conditions and binding corporate rules.

One of the key safeguards of the **Trans-Atlantic Data Privacy Framework** is the two-tiered complaint mechanism for European citizens: on the one hand, they can appeal to the Civil Liberties Protection Officer at the National Security Agency (NSA) of the USA and can lodge an appeal against his or her negative decision to an independent specialised three-member panel, the Data Protection Review Court (DPRC), which can review the legality of data use and access by intelligence services. EU citizens can use the DPRC's redress mechanisms by submitting a request to the competent EU data protection authority, which must then be transmitted through secure channels to the European Data Protection Board, and the complaint is "mailed" in this way. The decision in the case follows the same path.

Useful link: https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court/

General information on data transfers to the US after 10 July 2023 is available in English at:

https://www.edpb.europa.eu/system/files/202307/edpb_informationnoteadequacydecisionus_en.pdf

Information on the redress mechanism in relation to alleged violations with regard to data processing for national security purposes involving data transferred to the US within the Trans-Atlantic Data Privacy Framework after 10 July 2023 is available in English at:

https://www.edpb.europa.eu/system/files/2024-04/edpb_information-note_dpf-redress-mechanism-national-security-purposes_en.pdf

Template complaint form for alleged violations with regard to data processing for national security purposes involving personal data transferred to the US within the Trans-Atlantic Data Privacy Framework after 10 July 2023 is available in English at:

https://www.edpb.europa.eu/system/files/2024-04/edpb_dpf_template-complaint-form_national-security-purposes_en.pdf

Template complaint form for alleged violations with regard to data processing for commercial purposes involving personal data transferred to the US within the Trans-Atlantic Data Privacy Framework after 10 July 2023 – in cases of transfers for employment purposes, or where the controller voluntarily submits to cooperate with the EU data protection authorities – is available in English at:

https://www.edpb.europa.eu/system/files/2024-04/dpf_template-complaint-form_commercial-complaints_en.pdf

Rules of procedure of European Data Protection Authorities regarding the submission of complaints in the redress mechanism in relation to alleged violations with regard to data processing for national security purposes involving data transferred to the US within the Trans-Atlantic Data Privacy Framework is available in English at:

https://www.edpb.europa.eu/system/files/2024-04/edpb_rules-of-procedure_national-security-purposes_en.pdf

Rules of procedure of European Data Protection Authorities with regard to data processing for commercial purposes involving personal data transferred to the US within the Trans-Atlantic Data Privacy Framework – in cases of transfers for employment purposes, or where the controller voluntarily submits to cooperate with the EU data protection authorities – is available in English at:

https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf

4. Personal Data Breach

Personal Data Breach

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material

damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

Notification of a Personal Data Breach to the Supervisory Authority

In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

The notification shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Obligation to Communicate the Personal Data Breach to the Data Subject Pursuant to Article 34 of the GDPR

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33 (3).

The communication to the data subject shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to above are met.

5. Rights of the data Subject pursuant to the GDPR

In connection with the data processing and through the Data Controller, the data subject has the right to:

– **request information** about the processing and access to the data processed concerning them,

– request the **rectification** of inaccurate data and to have **incomplete personal data completed**,

– request the **erasure** of personal data processed based on their consent,

– **object** to the processing of their personal data,

– exercise their right to **data portability**

– request the **restriction of processing**.

On the basis of a request for information, the data subject has the right to, unless it is restricted by a legitimate interest, find out whether their personal data are being processed by the controller and has the right to obtain information about the data processed concerning them with regard to: – the purposes for which the data are processed, – the legal basis for the processing of the data, – from when and for how long the data are processed (duration), – what data are processed and a copy of these data shall be provided to the data subject, – the recipients or categories of recipients of the personal data, – transfers to third countries or international organisations, – the data subject's rights in relation to the processing, – the data subject’s rights of redress. The employer as data controller shall respond to requests for information and for access within 30 days at the latest. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. In some cases, the data controller may refuse to provide information on the basis of a legal authorisation, for example to prevent or prosecute criminal offences, in which

case the response shall include information about the legal provision the refusal is based on and the legal remedy.

In the case of a request for rectification (amendment) of data, the data subject must substantiate the accuracy of the data requested to be amended and must also certify that the person entitled to request the rectification is the person who requests the amendment. If it is not certain that the data processed is correct or accurate, the data controller does not amend the data, but only flags it, i.e. indicates that the data subject has contested it, but the data may not be incorrect. The data controller shall, without undue delay, correct inaccurate personal data or complete incomplete data concerned by the request, after confirming the authenticity of the request. The data controller shall notify the data subject of the rectification or the flagging of personal data.

The data controller complies with the request to restrict processing if one of the following conditions is met:

– the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

– the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

– the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; – the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, personal data shall, with the exception of storage, only be processed:

– with the data subject's consent,

– for the establishment, exercise or defence of legal claims,

– 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.

The Data Controller shall inform the Data Subject before the restriction of processing is lifted.

Remedies:

If the data subject alleges that the processing is in breach of the provisions of the GDPR or the controller's processing of the data subject's personal data is prejudicial, they should contact the Data Protection Officer or, if the controller does not employ a Data Protection Officer, the company's representative with the complaint. The complaint will always be investigated. If, despite the response to the complaint, the data subject still maintains their objection to the way their data is handled by the data controller or wishes to contact the data protection authority directly, the data subject can lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa u. 9-11., 1363 Budapest. Pf. 9.).

The data subject can also turn to the courts, which will rule on the case in extraordinary expeditious proceedings. In this case, the data subject can decide whether to file their claim in the court of their domicile (permanent address) or the court of their residence (temporary address) (https://birosag.hu/torvenyszekek). Courts with their territorial jurisdiction are listed at https://birosag.hu/birosag-kereso.

Legitimate Interest Assessment Test

with regard to the session cookies used on the Data Controller's website

Pursuant to Article 6 (1) (f) of the GDPR – "***processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child***" – the Data Controller, **Veres és Társai Kft.** (Registered seat: 9700 Szombathely, Kárpáti Kelemen utca 19/A., Company registration number: 18-09-103666, VAT identification number: 11513898-2-18, Email: info@eco-trend.hu, Represented by: Magdolna VERES and István András ANTAL, managing directors) uses the session cookie "PHPSESSID" on its website at www.ecotrendwebshop.com.

In order to determine whether the aforementioned conditions of the General Data Protection Regulation (GDPR) are met in relation to the personal data being subject of the Legitimate Interest Assessment Test, it is necessary to carry out this Legitimate Interest Assessment Test.

When carrying out the legitimate interest assessment test, the Data Controller shall

- establish its legitimate interest in the processing of the personal data being subject of the legitimate interest assessment test
- establish the interests and fundamental rights of the Data Subject in relation to the personal data being subject of the legitimate interest assessment test
- carry out a comparison and assessment of the legitimate interests of the Data Controller and of the interests and fundamental rights of the Data Subject, and on this basis, determine whether the Data Subject's personal data can be processed on this legal basis.

In any case, the Data Controller must inform the Data Subject of the result of the legitimate interest assessment test.

The legitimate interest assessment test must be concluded before data processing is started.

The purpose of the legitimate interest assessment test is for the Data Controller to demonstrate in detail its legitimate interest as website operator in the use of session cookies on the www.ecotrendwebshop.com **website.**

Applicable Legislation:

With regard to the processing of personal data, the main applicable acts of legislation for natural persons are the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council on the processing of personal data ("GDPR"), the Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Info Act") and the Act CVIII of 2001 on Certain Issues of Electronic Commerce and Information Society Services ("Electronic Commerce Act").

Comparison of the Interests of the Data Controller and the Data Subject:

The www.ecotrendwebshop.com website is an internet site presenting the services of Veres és Társai Kft.

In order to comply with the principle of purpose limitation, the www.ecotrendwebshop.com website uses a session cookie. The use of cookies is strictly necessary for the basic functioning of the website in accordance with Article 6 (1) (f) of the GDPR, as the use of these cookies supports the basic functioning of the website, without which the smooth operation of the website cannot be ensured. Session cookies are cookies that are essential for the technical functioning of the website (e.g. navigation on the site). The session cookie is strictly necessary for the Supplier to provide the information society service explicitly requested by the user and is linked to the user's activity (e.g. filling in a form, pressing a button). Ensuring the proper functioning of the website is required by the e-commerce services and by Section 13/A (3) of the Electronic Commerce Act, according to which the Supplier, in this case the website operator, processes personal data that are technically necessary for the provision of the service. Even if the other conditions are identical, the Supplier must choose and in any case operate the tools used to provide the service in such a way that personal data are processed only if necessary for the provision of the service and for the fulfilment of the other purposes set out in the Electronic Commerce Act, but even then only for the time and to the extent necessary.

In accordance with the principle of purpose limitation and the legitimate interest assessment test, the website operator must demonstrate its legitimate interest in the use of the session cookie.

Legal Basis for Using Session Cookie: Pursuant to Article 6 (1) (f) of the GDPR, processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Purpose of data processing: the use of session cookies on the www.ecotrendwebshop.com internet site. The session cookie is used to track user data input.

Compliance with the principle of purpose limitation of processing: the Data Controller processes the session cookie in order to fulfil its obligations under Article 13/A(3) of the Electronic Commerce Act and does not process it in a manner incompatible with these purposes.

The Legitimate Interests Providing Legal Basis for the Processing:

The use of session cookies on the website of the Data Controller at www.ecotrendwebshop.com, and the processing of data strictly necessary for the provision of the service, as authorised by Section 13/A (3) of the Electronic Commerce Act.

The Scope of Personal Data Processed by the Session Cookies: No personal data relating to the user is recorded, only the data and activity that occurs during a session on the website.

Duration of Data Processing: The session cookie is created for the duration of the visit and is automatically deleted when the session ends or the browser is closed.

The Data Controller will provide adequate information about the use of the session cookie to the data subjects in a way that is accessible to everyone, and the cookies will be present on the site in a way that is necessary and proportionate to achieve the purpose and will be created only for the minimum time necessary – they will be automatically deleted at the end of the session or when the site is closed.

In connection with the data processing the data subject has the right to:

– **request information** about the processing and access to the data processed concerning them,

– request the **rectification** of inaccurate data and to have **incomplete personal data completed**,

– request the **erasure** of personal data processed based on their consent,

– **object** to the processing of their personal data,

– exercise their right to **data portability**

– request the **restriction of processing**.

Result of the Legitimate Interest Assessment Test:

The purpose of data processing is to enable the use of a session cookie on the website of the Data Controller at www.ecotrendwebshop.com, which is necessary for the smooth operation of the site, without which the smooth use of the website cannot be guaranteed. Session cookies are cookies that provide basic functionality to support basic functions that are essential for the technical operation of the website. The proper functioning of the website is ensured and the related data is processed in accordance with the statutory authorisation set out in Article 13/A (3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce and Information Society Services. Furthermore, session cookies have a short lifetime, are limited to the user's actual session and are automatically deleted at the end of the session or when the browser is closed. They also prevent data loss.

In relation to the use of session cookies on the www.ecotrendwebshop.com website, the legal basis for the processing is the legitimate interest referred to in Article 6 (1) (f) of the GDPR, and the rights and interests of data subjects are not affected adversely to such an extent that these would override the legitimate interests of the controller.

Szombathely, 18.06.2025

Veres és Társai Kft.

controller