

Data Protection and Privacy Statement

Purpose of Data Protection and Privacy Statement

Ferenc Bálint sole proprietor (Address: 1122 Budapest, Krisztina krt. 27. 3rd floor, apartment No 35. hereinafter, "Service Provider", "Data Controller") as a data controller, acknowledges the content of this legal notice as binding on him.

It undertakes that all data processing related to its activities complies with the requirements set out in these regulations and in the applicable national legislation, as well as in the legal acts of the European Union.

This privacy statement covers the following domains and their subdomains:

<https://ferencbalint.com>

The privacy policies that apply to the data controller's privacy practices are available at <https://ferencbalint.com/privacy-policy>.

The Privacy policy can be downloaded from the following link: [Privacy policy](#).

The data controller reserves the right to amend this prospectus at any time. Stakeholders will be informed of the changes in due time.

The data controller is committed to the protection of the personal data of its customers and partners and considers it extremely important to respect the right of its customers to self-determination of information. The data controller shall treat the personal data confidentially and shall take all security, technical and organizational measures that guarantee the security of the data.

The data controller describes his data management practices below.

Data of the data controller

Name: Ferenc Bálint sole proprietor

Head office: 1122 Budapest, Krisztina krt. 27. 3rd floor, apartment No. 35.

Tax number: 56705447-1-43

Community tax number: HU56705447

Registration number: 55380649

Mobile Phone number: +36303050028

Email: info@ferencbalint.com

Data Protection Officer

The data controller shall not engage in any activity that would justify the appointment of a data protection officer.

Scope of personal data processed

Technical details

The data controller selects and operates the IT tools used to manage personal data during the provision of the service in such a way that the managed data (are):

- accessible to those entitled to it (availability);
- authenticity and authentication are ensured (authenticity of data management);
- its invariability can be verified (data integrity);
- are protected against unauthorized access (data confidentiality).

The data controller shall take appropriate measures to protect the data against unauthorized access, alteration, transmission, disclosure, deletion or destruction, and accidental destruction.

The data controller shall ensure the protection of the security of data processing with technical, organizational and operational measures that provide a level of protection appropriate to the risks associated with the data processing.

The data controller maintains confidentiality during data management: he protects the information so that only those who have the right to access it can access it; integrity: protects the accuracy and completeness of information and the method of processing; availability: ensures that when an authorized user needs it, they can actually access the information they want and have the tools to do so.

Cookies

The purpose of cookies

A cookie is a small amount of information that's downloaded to your computer or device when you visit our Site. We use a number of different cookies, including functional, performance, advertising, and social media or content cookies. Cookies make your browsing experience better by allowing the website to remember your actions and preferences (such as login and region selection). This means you don't have to re-enter this information each time you return to the site or browse from one page to another. Cookies also provide information on how people use the website, for instance whether it's their first time visiting or if they are a frequent visitor.

We use the following cookies to optimize your experience on our Site and to provide our services.

Essential session cookies

The purpose of these cookies is for visitors to fully and seamlessly browse <https://ferencbalint.com>, use its features and the services available there. These types of cookies last until the end of the session (browsing), and when you close the browser, these types of cookies are automatically deleted from your computer or other device used for browsing.

Cookies Necessary for the Functioning of the Store

Name	Function
<i>_ab</i>	Used in connection with access to admin.
<i>_secure_session_id</i>	Used in connection with navigation through a storefront.
<i>cart</i>	Used in connection with shopping cart.

Name	Function
<i>cart_sig</i>	Used in connection with checkout.
<i>cart_ts</i>	Used in connection with checkout.
<i>checkout_token</i>	Used in connection with checkout.
<i>secret</i>	Used in connection with checkout.
<i>secure_customer_sig</i>	Used in connection with customer login.
<i>storefront_digest</i>	Used in connection with customer login.
<i>_shopify_u</i>	Used to facilitate updating customer account information.

Third-party cookies (analytics)

Https://ferencbalint.com and its subdomains also use Google Analytics as a third-party cookies on their websites. Using Google Analytics for statistical purposes, the websites of https://ferencbalint.com and its subdomains collect information about how visitors use the websites. Use the data to improve the website and improve the user experience. These cookies also remain on the visitor's computer or other device used for browsing, in its browser or until the visitor deletes them until they expire.

Reporting and Analytics

Name	Function
<i>_tracking_consent</i>	Tracking preferences.
<i>_landing_page</i>	Track landing pages
<i>_orig_referrer</i>	Track landing pages
<i>_s</i>	Shopify analytics.
<i>_shopify_fs</i>	Shopify analytics.
<i>_shopify_s</i>	Shopify analytics.
<i>_shopify_sa_p</i>	Shopify analytics relating to marketing & referrals.
<i>_shopify_sa_t</i>	Shopify analytics relating to marketing & referrals.
<i>_shopify_y</i>	Shopify analytics.
<i>_y</i>	Shopify analytics.

The length of time that a cookie remains on your computer or mobile device depends on whether it is a “persistent” or “session” cookie. Session cookies last until you stop browsing and persistent cookies last until they expire or are deleted. Most of the cookies we use are persistent and will expire between 30 minutes and two years from the date they are downloaded to your device.

You can control and manage cookies in various ways. Please keep in mind that removing or blocking cookies can negatively impact your user experience and parts of our website may no longer be fully accessible.

Most browsers automatically accept cookies, but you can choose whether or not to accept cookies through your browser controls, often found in your browser's "Tools" or "Preferences" menu. For more information on how to modify your browser settings or how to block, manage or filter cookies can be found in your browser's help file or through such sites as www.allaboutcookies.org.

Additionally, please note that blocking cookies may not completely prevent how we share information with third parties such as our advertising partners. To exercise your rights or opt-out of certain uses of your information by these parties, please follow the instructions in the "Behavioural Advertising" section above.

Do Not Track

Please note that because there is no consistent industry understanding of how to respond to "Do Not Track" signals, we do not alter our data collection and usage practices when we detect such a signal from your browser.

Legal basis for cookie handling

The legal basis for the handling of cookies is the consent of the website visitor, in accordance with Article 6 (1) (a) of the relevant Regulation.

If you do not accept the use of cookies, then 3.2.3. Some features of the websites listed in section 3.2.3. will not be available when you use the websites, or some features may not work properly. You can find more information about deleting cookies for the most common browsers at the following links:

Firefox: Clear cookies and site data in Firefox

<https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox>

Chrome: Clear cache & cookies

<https://support.google.com/accounts/answer/32050?co=GENIE.Platform%3DDesktop&hl=en>

Safari: Manage cookies and website data in Safari on Mac <https://support.apple.com/en-gb/guide/safari/sfri11471/mac>

General data management guidelines, Data Processing Title, Use of Data, Legal Basis and Retention Period

If you are a resident of the EEA, you have the right to access the Personal Information we hold about you, to port it to a new service, and to ask that your Personal Information be corrected, updated, or erased. If you would like to exercise these rights, please contact Shopify through the contact information below.

Your Personal Information will be initially processed in Ireland and then will be transferred outside of Europe for storage and further processing, including to Canada and the United States. For more information on how data transfers comply with the GDPR, see Shopify's GDPR Whitepaper: <https://help.shopify.com/en/manual/your-account/privacy/GDPR>.

The data management of the data controller's activity is based on voluntary consent or legal authorization. In the case of data management based on voluntary solutions, the consent and the authorization can be revoked at any stage of the data management.

In some cases, the management, preservation, and transfer of particular sets of data is being done according to mandatory legislation of which our customers must be specifically notified. We would like to hereby draw the attention of data providers to the fact that if they do not provide their own personal data, it is the data controller's duty to obtain the consent of the affected person. The principles of our data management and data protection comply with the following:

- The Hungarian 2011 CXII. Act on the Right to Information Self-Determination and Freedom of Information (Infotv.);
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the substantial protection of natural persons and the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 (General Data Protection Regulation, GDPR);
- Act V of 2013 - on the Civil Code (Civil Code);
- Act C of 2000 - on Accounting (Accounting Act);
- 2017 LIII. Act on the Prevention and Targeting of Money Laundering and Terrorist Financing (Pmt.); 2013 CCXXXVII. Act on Credit Institutions and Financial Enterprises (Hpt.).

Preparation of data maps of the data controller, on the basis of which the scope of the processed data, their use, legal basis and retention period were determined.

CCPA

If you are a resident of California, you have the right to access the Personal Information we hold about you (also known as the 'Right to Know'), to port it to a new service, and to ask that your Personal Information be corrected, updated, or erased. If you would like to exercise these rights, please contact us through the contact information below:

info@ferencbalint.com

If you would like to designate an authorized agent to submit these requests on your behalf, please contact us at the address below.

info@ferencbalint.com

Behavioural Advertising

As described above, we use your Personal Information to provide you with targeted advertisements or marketing communications we believe may be of interest to you. For example:

- We use Google Analytics to help us understand how our customers use the Site. You can read more about how Google uses your Personal Information here: <https://policies.google.com/privacy?hl=en>. You can also opt-out of Google Analytics here: <https://tools.google.com/dlpage/gaoptout>.
- We share information about your use of the Site, your purchases, and your interaction with our ads on other websites with our advertising partners. We

collect and share some of this information directly with our advertising partners, and in some cases through the use of cookies or other similar technologies (which you may consent to, depending on your location).

- For more information about how targeted advertising works, you can visit the Network Advertising Initiative's ("NAI") educational page at <http://www.networkadvertising.org/understanding-online-advertising/how-does-it-work>.

You can opt out of targeted advertising by:

- **FACEBOOK** - <https://www.facebook.com/settings/?tab=ads>
 - **GOOGLE** - <https://www.google.com/settings/ads/anonymous>
 - **BING** - <https://advertise.bingads.microsoft.com/en-us/resources/policies/personalized-ads>
 - **KLAVIYO** - <https://www.klaviyo.com/privacy/policy>
-
- *Additionally, you can opt out of some of these services by visiting the Digital Advertising Alliance's opt-out portal at: <http://optout.aboutads.info/>.*

Data related to online purchase

Options available on the website for ordering products, personal data during the order:

Name (required field)

Email address (required field)

Phone number (required field, use in case of problem with delivery of the ordered product)

Address (required field, place of delivery of the product)

Billing address (required field, otherwise from Address)

Newsletter subscription (optional, insurance required)

The purpose of data management, the use of managed data: The data is used to fulfill the order.

The legal basis for data management is the assignment of a contract.

Retention period: the duration of a business relationship or a cancellation request.

Data related to online administration

Personal data requested during the contact registration:

Name (required field)

Email address (required field)

Phone number (optional field, optional, to initiate a callback)

The purpose of data management, the use of the managed data: The full use of the data is for contacting and ordering.

The legal basis for data management is voluntary consent.

Retention period: the duration of a business relationship or a cancellation request.

Data related to telephone-based customer service

Personal data requested during the contact registration:

Name (required field)

Phone number (optional field, if initiation of a callback is required by the data provider)

Intended use of the managed data: The data will be used for contact and fulfillment of the order.

The legal basis for data management is voluntary consent.

Retention period: the duration of a business relationship or a cancellation request.

Newsletter related information

Personal data requested during the newsletter subscription:

Name (required field)

Email address (required field)

The newsletter is available after reading and accepting the data management policy. The data management policy is accepted by ticking the mandatory check box.

After subscribing, the subscriber will receive an email informing them of the subscription, which must be confirmed, after which their subscription will take effect.

During all related processes, the customer still has the option to unsubscribe, the option to unsubscribe is included in each letter in the form of a link, it is easily accessible with one click.

As the newsletter contains the name of the company and the contact details of its website, it is considered advertising, eDM.

Purpose of data management and intended use of the managed data: The data will be used to send out a newsletter including advertising. The newsletter contains the address of the website, so it is already considered an advertisement.

The legal basis for data management is voluntary consent.

Retention period: until unsubscribing.

Personal information to be provided during registration

Registration is an available option in the webshop module of the website, which makes it easier to use the additional service, make it unnecessary to re-enter data. Personal data processed during registration:

Name

E-mail address

Address:

Phone number:

Purchase information (product, date, etc.)

Purpose of data management, intended use of the managed data: invoicing and fulfillment of contractual order.

The legal basis for data management is voluntary consent.

Retention period: until revoked.

Personal information to be provided during purchase

If you want to place an order in the webshop module, data management and the provision of data during the purchase is essential for the fulfillment of the contract.

Name

E-mail address

Address

Phone number

Purchase information (product, date, etc.)

The purpose of data management, the intended use of the managed data: fulfillment of a contractual order.

The legal basis for data management is a contractual mandate.

Retention period: according to legal regulations, current year + 5 years

Invoice related information

The data controller enters into a contract with its customers for the ordered services, during which it stores the following data:

Name

E-mail address

Address

The purpose of data management, the intended use of the managed data: invoicing.

Legal basis for data management: legal requirement.

Retention period: according to legal regulations, current year + 5 years

Guarantee service

If you initiate warranty administration, data management and the provision of data are essential for administration.

Name

E-mail address

Phone number

Complaint

The purpose of data management, the intended use of the managed data: guarantee administration.

The legal basis for data management is voluntary consent.

Retention period: subject year + 5 years according to the Consumer Protection Act

Dealing with consumer complaints

If you submit a consumer protection complaint, data management and the provision of data are essential for the administration.

Name

E-mail address

Phone number

Complaint

The purpose of data management, the intended use of the processed data: administration of consumer protection complaints.

The legal basis for data management is voluntary consent.

Retention period: subject year + 5 years according to the Consumer Protection Act.

Physical data preservation locations

Your personal data (that is data that may be associated with you) may be processed by us in the following ways:

- On the one hand, in connection with the maintenance of the Internet connection, the technical data related to the computer, browser, Internet address and pages visited by you are automatically generated in our computer system,

- On the other hand, you may also provide your name, contact information or other details if you wish to contact us personally while using the website. Data to be technically recorded during the operation of the system: data of the computer of the affected login, which is recorded by the systems of the domain <https://ferencbalint.com> and its subdomains as an automatic result of the technical processes.

The data that is automatically being recorded at login and logout without the specific consent of the data provider.

This data may not be linked to other personal user data, except in cases required by law. Only <https://ferencbalint.com> domains and subdomains have access to the data.

Data transmission, data processing, the circle of those who get to know the data

As part of its business activities, the data controller uses the following data processors:

Hosting service:

Shopify International Limited

Address: 2nd Floor Victoria Buildings, 1-2 Haddington Road, Dublin 4, D04 XN32, Ireland

Attn: Data Protection Officer

Website: <https://shopify.com>

The scope of the data: the content of the websites on the <https://ferencbalint.com> domain and its subdomains

Invoicing:

Bilingo Technologies Private Limited Company

Address: 1133 Budapest, Árbóc utca 6. 3. em.

Email: hello@bilingo.hu

Tel: +3615009491

Scope of known data: issued invoices, billing data

Book keeping:

Prevent Financial, Informatics Bt./Prevent Financial Ltd.

Address: 1196 Budapest, Nagysándor József u. 196.

Email: fokk.zsolt@preventbt.hu

Scope of information: invoices issued

Newsletter:

Klaviyo, Inc.

Address: 125 Summer Street, Boston, Massachusetts 02111

Phone: (800) 338 1744

Email: privacy@klaviyo.com.

Scope of information: subscriber name and email address.

Google Analytics:

Google Inc., Mountain View, California, USA

The scope of the data: the IP address of the visitors of the website

<https://ferencbalint.com> - anonymised, non-personal.

Google Workspace:

Google Inc., Mountain View, California, USA
Range of information: emails sent to email addresses related to the
<https://ferencbalint.com> domain

Transfer of data to a third country

The data will be transferred to the United States, with which a decision on compliance was taken on 12 July 2016 (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en).

The compliance decision is available from Klaviyo (<https://www.klaviyo.com/privacy/policy>), Google (<https://policies.google.com/privacy/frameworks?hl=en>) and Facebook (<https://www.facebook.com/about/privacysshield>) also applies to data handlers.

Rights and enforcement options of the data provider

The data provider may request information on the processing of their personal data, as well as request the correction or deletion or revocation of their personal data, except for mandatory data processing. They may exercise their right by contacting the data provider in the manner and through the contact channels indicated above.

Right to information

The data controller shall take appropriate measures to provide the data subject with all information concerning the processing of personal data referred to in Articles 13 and 14 of the GDPR and Articles 15 to 22. and Article 34 shall be provided in a concise, transparent, comprehensible and easily accessible form, in a clear and comprehensible manner.

The data provider's right to access data

The data provider shall have the right to receive feedback from the controller as to whether their personal data are being processed and, if such processing is in progress, to have access to the personal data and the following information:

- the purposes of data management;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom or with whom the personal data have been or will be communicated, including in particular third country recipients or international organizations;
- the planned duration of the storage of personal data;
- the right to rectify, erase or restrict data processing and to protest;
- the right to lodge a complaint with the supervisory authority;
- information on data sources;
- the fact of automated decision-making, including profiling, and comprehensible information on the logic used and the significance of such data management and the expected consequences for the data provider.

The data controller shall provide the information no later than one month after the submission of the request.

Right of Data Correction

The data provider may request the correction of inaccurate personal data processed by the Data Controller and the completion of incomplete data.

Right of cancellation

The data provider shall have the right to ask the Data Controller to delete their personal data immediately should the following reasons occur: personal data are no longer required for the purpose for which they were collected or otherwise processed; the data provider withdraws their consent on which the processing is based and there is no other legal basis for the processing; the data provider objects to the processing and there is no overriding legitimate reason for the processing; personal data have been processed unlawfully; personal data must be deleted in order to fulfill a legal obligation under Union or Member State law applicable to the controller; personal data was collected in connection with the provision of information society services.

Deletion of data may not be initiated if the processing is necessary: for the purpose of exercising the right to freedom of expression and information; for the purpose of fulfilling an obligation under Union or Member State law governing the processing of personal data or performing a task carried out in the public interest or in the exercise of official authority vested in the controller; in the field of public health, or for archival, scientific and historical research or statistical purposes, in the public interest; or to bring, assert or defend legal claims.

Right to restrict data processing

At the request of the data provider, the Data Controller shall restrict the data processing if one of the following conditions is occur: the data provider disputes the accuracy of the personal data, in which case the restriction shall apply for a period that allows the accuracy of the personal data to be verified; the processing is unlawful and the data provider opposes the deletion of the data and instead requests that their use be restricted; the controller no longer needs the personal data for the purpose of data processing, but the data provider requests them in order to make, enforce or protect legal claims; or the data provider has objected to the processing; in that case, the restriction shall apply for as long as it is established whether the legitimate reasons of the data controller take precedence over the legitimate reasons of the data provider. If the processing is restricted, personal data other than storage may be processed only with the consent of the data provider or for the purpose of bringing, enforcing or protecting legal claims, protecting the rights of another natural or legal person or in the important public interest of the European Union or a Member State.

Right to transfer data

The data provider shall have the right to receive their personal data made available to the data controller in a structured, widely used, machine-readable format and to transmit these data to another data controller.

Right for objection

The data provider shall have the right to object at any time, for reasons related to their situation, to the processing of their personal data in the public interest or in the exercise of public authority or to the processing of data subjects or third parties, including profiling based on those provisions. is. In the event of an objection, the controller may not further process the personal data, unless justified by compelling legitimate reasons which take precedence over the interests, rights and freedoms of the data subject or which relate to the submission, enforcement or protection of legal claims.

Automated decision making in individual cases, including profiling

The data subject shall have the right not to be covered by a decision based solely on automated data processing, including profiling, which would have legal effects on them or would be similarly significant.

Right of withdrawal

The data subject has the right to withdraw their consent at any time.

Right to apply to the courts

In the event of a breach of his rights, the data subject may take legal action against the data controller. The court is acting out of turn in the case. Data protection authority proceedings can be lodged with the Hungarian National Data Protection and Freedom of Information Authority (NMHH)

Name: National Data Protection and Freedom of Information Authority (NMHH)

Headquarters: 1125 Budapest, Szilágyi Erzsébet avenue 22 / C.

Mailing address: 1530 Budapest, Pf .: 5.

Phone: 0613911400

Fax: 0613911410

E-mail: ugyfelszolgalat@naih.hu

Website: <http://www.naih.hu>

Other provisions

Information on data processing not listed in this statement will be provided at the time of data collection. We inform our clients that the court, the prosecutor, the investigating authority, the infringement authority, the administrative authority, the Hungarian National Data Protection and Freedom of Information Authority, the Magyar Nemzeti Bank, or other bodies are authorized to provide information, disclose data, transfer or documents they may contact the data controller to make it available. The data controller shall

provide personal data to the authorities, provided that the authority has indicated the exact purpose and scope of the data, only to the extent and to the extent strictly necessary for the purpose of the request.

(This data management information has been prepared on the recommendation of the Budapest Chamber of Commerce and Industry.)