Privacy Policy

Privacy Policy

he Webshop Logisztika Limited Liability Company (hereinafter referred to as the "Data Controller"), as the operator of the website accessible under the domain name www.lovesexshop.co.uk/ (hereinafter referred to as the "Website"), hereby publishes the rules, data protection principles, and information related to the processing of the data of visitors to the Website and users of the services available on the Website (hereinafter collectively referred to as "Data Subjects").

In connection with data processing, the Data Controller hereby informs the Data Subjects about the personal data it processes on the Website, the principles and practices it follows in the processing of personal data, as well as the means and possibilities for Data Subjects to exercise their rights.

The Data Controller undertakes to ensure that all data processing related to its activities complies with the requirements set forth in this policy and in applicable laws.

The data protection principles related to the Data Controller’s data processing are continuously available at the following address: https://www.lovesexshop.co.uk/shop_help.php?tab=privacy_policy

If the Data Subject has any questions that are not clear based on this notice, please contact us at (adatvedelem@webshoplog.hu), and our colleague will answer your question.

We draw the attention of individuals providing data to the Data Controller that if they do not provide their own personal data, it is their responsibility to obtain the consent of the Data Subject.

By using the Website, the Data Subject accepts the contents of this Privacy Policy and consents to the data processing specified below.

1. Definitions

a) **"Data Controller"**: the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

b) **"Personal Data"**: any information relating to an identified or identifiable natural person ("Data Subject" in this document referred to as "loyal customer"). 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

c) **"Processing"**: any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated or non-automated means, such as collection, recording, organization, structuring, storage, alteration or modification, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

d) **"Restriction of Processing"**: the marking of stored personal data with the aim of limiting its processing in the future.

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

f) **"Processor"**: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.

g) **"Recipient"**: a natural or legal person, public authority, agency, or other body to whom personal data is disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a specific inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of such data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

h) **"Consent of the Data Subject"**: any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

i) **"Personal 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.

2. Data Controller´s information

Webshop Logisztika Kft.

Registered office: 14–16 Ecseri út, 1097 Budapest, Hungary

Company registration number: 01-09-953952

Court of registration: Budapest-Capital Regional Court as the Court of Registration

Tax number: 23121076-2-43

Data processing ID: 03327-0001

For data protection requests and deletions: adatvedelem@webshoplog.hu

Data processing registration number: NAIH-60933/2012

Registration number for data processing related to direct marketing: NAIH-60934/2012

3. Legal basis, purpose, and duration of data processing

Data Subjects can provide information about themselves on the Website in two ways:

1. **Personal data explicitly provided or made available** during the use of the services of the Website (see Section 3.1).
2. **Information made available to the Data Controller** in connection with the use of the Website, provided during visits to and usage of the Website (see Section 3.2).

The legal basis for data processing is always determined in accordance with Article 6 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council ("Regulation") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The legal basis

for data processing is indicated for each case of data processing.

The Data Subject is entitled, by means of a written notification addressed to the Data Controller, to withdraw their consent to data processing either partially or entirely, or to request the deletion of their data.

3.1. Special Categories of Data

The Data Controller processes personal data falling within the special categories referred to in **Article 9** of the GDPR (data concerning sexual life), as the Data Controller operates an adult content Webshop, and therefore the range of orderable products constitutes special data once the Data Subject has placed an order. The Data Controller will process such personal data exclusively with the explicit consent of the Data Subject and for the purposes defined in this privacy notice.

3.2 Processed Personal Data

	Data processed:	Retention period:	Purpose:	Legal basis:
Registration and Order Processing	First name, Last name, Phone number, Email address, Billing address (Country, Postal code, City, Street, House number)	Data is processed from the time of registration and continues until the Data Subject requests deletion. If no deletion request is made, the data will be deleted no later than 30 days after the Website is shut down.	Providing access to services that require registration (e.g., purchasing, participation in loyalty programs, invoicing, delivery).	Voluntary consent of the Data Subject.
Issuing Invoices	Name, Address, Tax number (for company orders)	Data is retained for 8 years from the issuance of the invoice.	Identification of the purchaser and display of necessary information on the invoice.	Legal obligation based on the Accounting Act and VAT Act.
Order Fulfillment	First name, Last name, Phone number, Email address, Billing address (Country, Postal code, City, Street, House number)	Data is retained for the duration of the civil statute of limitations (usually 5 years, but this may be extended).	Fulfillment of contracts and delivery of products.	Contractual obligation.
Contact via Email or Other Channels	Name, Email address, and any other information voluntarily provided by the Data Subject during contact.	Data is retained for 10 years unless the Data Subject requests deletion. Complaint letters are retained for 3 years.	Maintaining contact with the Data Subject.	Voluntary consent of the Data Subject.
Complaint Handling and Warranty Services	Complaint letters and associated data.	Data is retained for 3 years after the resolution of the complaint.	Investigating and handling complaints or warranty claims.	Legal obligation based on consumer protection laws.

3.3 Other Purposes of Data Processing

	Data processed:	Retention period:	Purpose:	Legal basis:
Loyalty Program (Lovesexshop club) and Direct Marketing (DM Activities)	Name, Email address, Phone number.	Data is processed until the Data Subject unsubscribes from newsletters or electronic messages. The Data Subject can unsubscribe via the unsubscribe link in newsletters or by requesting removal via email or postal mail.	Sending promotional messages and personalized offers related to products and services.	Voluntary consent of the Data Subject.
Profiling for Personalized Offers	Name, Email address, Purchase history.	Data is processed until the Data Subject objects to profiling by written request.	Analyzing shopping habits to send personalized offers and advertisements.	Voluntary consent of the Data Subject.
Partner Program (Affiliate)	Name, Email address, Phone number, Contact person, Billing name and address.	Data is processed until the Data Subject requests deletion.	Providing partners the opportunity to place ads on their website or blog and receive commissions for purchases made through those ads.	Voluntary consent of the Data Subject.
Sweepstakes and Promotions	First name, Email address, Phone number.	Data is processed until the end of the promotion or sweepstakes. For winners, data is retained for 8 years.	Organizing sweepstakes and providing promotional offers.	Voluntary consent of the Data Subject.

3.4 Data Collected During Website Use

3.4.1 Technical Data and Website Visits

Data processed:

Date, time, IP address of the Data Subject's computer, visited page URL, and data related to the user's age.

Purpose:

Monitoring the functionality of the service, providing personalized service, and preventing abuse.

Retention period:

30 days from the time of the website visit.

3.4.2 Cookie Management

Temporary cookies:

Purpose: Ensuring the effective operation of the Website.

Retention period: Active during the session, deleted after the session ends.

Persistent cookies:

Purpose: Enhancing the user experience (e.g., navigation).

Retention period: 1-5 days, depending on browser settings.

3.4.3 External Service Providers

- The Website contains links to external service providers who may collect user data through their own servers and cookies.

3.4.4 Google Analytics Cookies

Google Analytics collects web traffic data through cookies for analyzing Website interactions. The data collected includes anonymized information such as IP addresses. Data retention is 26 months.

3.4.5 Google Adwords

Google Adwords uses remarketing tags to track website visitors and display personalized ads on the Google Display network. Visitors can disable these cookies via Google's ad settings.

3.4.6. Barion (Online Bank Card Payment System)

Service Provider:
Barion Payment Zrt.
1117 Budapest, Irinyi József utca 4-20. 2. emelet

Privacy Policy: https://www.barion.com/hu/adatvedelmi-tajekoztato

Cookie Policy: https://www.barion.com/hu/suti-tajekoztato

Cookies:

ba_vid:
Purpose: To prevent bank card fraud by tracking the digital fingerprint of your device and your browsing habits. This cookie ensures that data originating from your browsing habits can be identified as coming from a single user. The cookie is placed on both our site and other merchants' websites using Barion Smart Gateway.

ba_vid.xxx:
Purpose: To track your browsing behavior across sessions on the same site, assisting in identifying fraud through your device's digital fingerprint and browsing patterns. Data collected includes user-related ID generated from browser properties, timestamps of your first, current, and last visits, session ID, and permission for third-party cookies. This cookie is also placed on merchants' websites using Barion Smart Gateway.

Barion One-Click Payment (Saved Card Data)

The Barion system offers customers the option to use "One-Click" payment, where credit card data is securely stored in a tokenized form. The advantage of this feature is that future purchases can be completed faster without re-entering card details. Saved card data can be deleted at any time by the customer through their account in the UNAS system or via the Barion platform. The payment service is provided by Barion Payment Inc., a financial institution licensed by the Central Bank of Hungary.

3.4.7. Trustindex

Service:
Trustindex is an online tool that enables businesses to display user reviews and ratings on their website from various sources, such as Google, Facebook, TripAdvisor, etc. The goal is to increase visitor trust by showcasing genuine user feedback.

Data Processed:
Name, Email address

Data Retention:
Until withdrawal of consent

Cookies Used:
_ga, _fbp, _ga_DGL6KLFTVT

Service Provider:
Trustindex Ltd.
Address: 2724 Ujlengyel, Nyári Pál utca 15.
Established: 2018
Hungarian VAT ID: 26281186-2-13
EU VAT ID: HU26281186
Registration number: 13 09 223096
Email: info@trustindex.com
Website: www.trustindex.com

Privacy Policy:
The Trustindex privacy policy can be accessed via the following link: Privacy Policy.

3.4.8. Molin

This website uses the Molin chat platform to connect users with the customer support service of lovesexshopco.uk. We collect only email addresses, names, and telephone numbers with the explicit consent of the user. Messages and exchanged data are stored within the Molin application.

We have integrated Molin, our advanced AI-based customer support assistant, to better understand user needs and provide optimal service. Molin uses the latest technologies to analyse user interactions, preferences, and feedback, helping us to continuously improve our services. Its functionalities include the use of cookies and other technologies to collect data such as IP addresses, screen size, browser information, and geographic location at country level. These data are securely stored in anonymised profiles, and Molin AI strictly adheres to its contractual obligations. Our goal is to provide excellent customer service while safeguarding your data.

Processed data: Data provided by the user during the contact process.
Retention period: Data are processed only until the contact process is completed.
Legal basis: User consent.
Provider:

Address: 48 Overton Road, London, SE2 9SD, United Kingdom
Postal address: 48 Overton Road, London, SE2 9SD, United Kingdom

Email: hey@molin.ai
Website: Molin

3.4.9. Clarity – Microsoft Corporation
Registered office: 1 Microsoft Way, Redmond, WA 98052, USA
Postal address: 1 Microsoft Way, Redmond, WA 98052, USA
Website: https://clarity.microsoft.com/
Activity: Website analytics

4. Data Processing

Based on Article 28 of the GDPR, the Data Controller entrusts the following organizations with the processing of personal data:

MediaCenter Hungary Kft.
Address: 6000 Kecskemét, Sosztakovics u. 3, 2nd floor/6.
Mailing address: 6001 Kecskemét, Pf. 588.
Phone: 76/575-023
Fax: 76/575-024
Website: www.mediacenter.hu
Activity: Domain and email services

Websupport Magyarország Kft.
Address: 1132 Budapest, Victor Hugo utca 18-22.
Email: support@websupport.hu
Website: www.websupport.hu
Activity: Domain and email services

Online Comparison Shopping Kft.
Address: 1074 Budapest, Rákóczi út 70-72.
Tax number: 24868291-2-42
Company registration number: 01-09-186759
Email: info@arukereso.hu
Website: www.arukereso.hu
Activity: Operator of the Trusted Store program, sending questionnaires to customers, processing feedback, rating of the Data Controller and the website based on customer feedback, purchasing through the shopping cart program.
Personal data collected: name, email address, phone number, shipping and billing information.

REISSWOLF Budapest Adat- és Dokumentumkezelő Kft.
Address: 1097 Budapest, Illatos út 6.
Phone: +36-1-219-5670
Website: www.reisswolf.hu
Email: info@reisswolf.hu
Activity: Confidential document and data carrier destruction, provision of closed-system security services.

UNAS Online Kft.
Address: 9400 Sopron, Kőszegi út 14.
Email: unas@unas.hu
Activity: Provider of online store systems, hosting provider.

VIVABANK SINGLE MEMBER BANKING S.A. (VIVABANK S.A.), a Viva Wallet Group
Address: 18-20 AMAROUSIOU-CHALANDRIOU AVE, MAROUSI
Email: support@viva.com
Activity: providing an online credit card acceptance system
Data protection: https://www.viva.com/en-hu/privacy-notice

Lead Media s.r.o. (Dognet)
Address: 811 05 Pozsony, Karpatská 6, Slovakia
Phone: +421 948 483 365
Email: info@edognet.hu
Activity: Marketing software.

Tharanis Ügyvitel Kft.
Address: 2724 Újlengyel, Nyári Pál utca 15.
Email: info@tharanisugyvitel.hu
Activity: Invoicing, processing courier data, tax authority reporting.

Barion Payment Zrt.
Address: 1117 Budapest, Irinyi József utca 4-20, 2nd floor.
Email: info@barion.hu
Activity: Online card acceptance system.

Stripe, LLC
Address: 354 Oyster Point Boulevard, South San Francisco, CA 94080, United States
Email: dpo@stripe.com
Web: https://stripe.com/
Activity: Payment processing and online payment infrastructure services

PayPal, Inc.
Address: 2211 North First Street, San Jose, CA 95131, United States
Email: privacy@paypal.com
Web: https://www.paypal.com/

Activity: Online payment processing and digital payment services

Evri Limited
Registered office / Headquarters: Capitol House, 1 Capitol Close, Morley, Leeds, LS27 0WH, United Kingdom
Email: data.protection@evri.com
Web: https://www.evri.com/
Activity: Parcel delivery and logistics services

Global Payments Inc

Headquarters: 3550 Lenox Road, Atlanta, GA 30326, United Sta
Email: https://company.globalpayments.com/
Web: media.relations@globalpay.com
Activity: Providing online credit card acceptance system

SupportBox s.r.o.
Company name: SupportBox s.r.o.
Registered office: V Celnici 1031/4, Nové Město, 110 00 Prague 1, Czech Republic
Company ID (IČO): 04308697
VAT ID (DIČ): CZ04308697
Email: info@supportbox.cz
Website: https://www.supportbox.cz
Activity: Provision of customer support and chat system services

Retino.cz s.r.o.
Company name: Retino.cz s.r.o.
Registered office: Václavské náměstí 846/1, Nové Město, 110 00 Prague 1, Czech Republic
Company ID (IČO): 08913040
VAT ID (DIČ): CZ08913040
Email: hello@retino.cz
Website: https://www.retino.cz
Activity: Provision of return and complaint management system

Cash on Delivery Inspector – Utánvét Ellenőr Kft.

Registered office: 8640 Fonyód, Szigligeti Street 10, Hungary
Postal address: 8640 Fonyód, Szigligeti Street 10, Hungary
Website: utanvet-ellenor.hu
Email: hello@utanvet-ellenor.hu
Phone: +36 20 923 8883
Activity: Buyer reputation verification

The Data Controller reserves the right to engage additional data processors in the future. Any such changes will be communicated to the Data Subjects by updating this Privacy Policy.

Legal Labs Kft.
Address: 1054 Budapest, Honvéd utca 8, 1st floor 2.
Email: hello@payee.tech
Activity: First and last name, address, email address, phone number, amount of debt, legal basis for the debt, date of contract formation.

The Data Controller reserves the right to involve additional data processors in the future, and the Data Subjects will be informed of this by modifying this Data Processing Information.

5. Data Transfer

The Data Controller will only transfer data that can identify the Data Subject to third parties with the explicit consent of the Data Subject, unless a specific legal provision requires otherwise.

6. Access to Data and Data Security Measures, Data Transfer

6.1. Access to Data and Data Transfer

The employees of the Data Controller may access personal data only for the purpose of performing their duties.

The Data Controller shall only transfer the personal data it manages to other entities or public authorities in accordance with the manner and purposes defined by law.

The Data Controller informs the Data Subject that courts, prosecutors, investigative authorities, administrative authorities, the National Authority for Data Protection and Freedom of Information, or other bodies authorized by law, may request information, disclose data, transfer information, or make documents available to the Data Controller.

The Data Controller will only release personal data to authorities, provided that the authority specifies the exact purpose and scope of the requested data, and only to the extent that is strictly necessary to achieve the objective of the request.

7. Rights of the Data Subject

7.1. Right to Information and Access to Personal Data

The Data Subject has the right to access their personal data stored by the Data Controller and obtain information related to its processing. The Data Subject may request access to their data, verify what information the Data Controller holds about them, and obtain access to the personal data at any time. Requests for access to data must be submitted in writing (via email or post) to the Data Controller. The Data Controller will provide the requested information in a widely used electronic format. No verbal information will be provided over the phone when exercising access rights.

When exercising the right of access, the following information will be provided:

- The scope of the processed data: name, billing name, billing address, email address, telephone number, depending on the service used.
- The purpose, duration, and legal basis of data processing.
- Data transfer: to whom the data has been transferred or will be transferred in the future.
- The source of the data.

The Data Controller will provide a paper or electronic copy of the personal data to the Data Subject free of charge the first time. For additional copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs. If the Data Subject requests the information electronically, it will be provided via email in a widely used electronic format.

If, after receiving the information, the Data Subject disagrees with the data processing or the accuracy of the processed data, they may request rectification, completion, deletion, or restriction of their personal data, or object to the processing of such data according to section 6. They may also initiate the procedure outlined in section 7.

7.2. Right to Rectification and Completion of Processed Personal Data

Upon request, the Data Controller will promptly rectify any inaccurate personal data indicated by the Data Subject in writing, and will complete any incomplete data according to the content provided by the Data Subject. The Data Controller will inform all recipients of the rectification and completion of personal data, except where it is impossible or requires disproportionate effort. The Data Subject will be informed of these recipients upon request.

7.3. Right to Restrict Data Processing

The Data Subject has the right to request the restriction of data processing in writing if:

- The Data Subject contests the accuracy of the personal data, in which case the restriction applies for the period necessary for the Data Controller to verify the accuracy of the personal data.
- The data processing is unlawful, and the Data Subject opposes the deletion of the data and requests the restriction of their use instead.
- The Data Controller no longer needs the personal data for processing purposes, but the Data Subject requires them for the establishment, exercise, or defense of legal claims.
- The Data Subject has objected to data processing; in this case, the restriction applies until it is determined whether the legitimate grounds of the Data Controller override those of the Data Subject.

The Data Controller will inform the Data Subject who requested the restriction before lifting the restriction on data processing.

7.4. Right to Erasure ("Right to be Forgotten")

The Data Subject may request that the Data Controller delete their personal data without undue delay if one of the following grounds applies: i) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed; ii) the Data Subject withdraws their consent, and there is no other legal ground for processing; iii) the Data Subject objects to the processing, and there are no overriding legitimate grounds for processing; iv) the Data Subject objects to the processing of their personal data for direct marketing purposes, including profiling related to direct marketing; v) the personal data has been processed unlawfully; vi) the personal data was collected in connection with the offer of information society services directly to children. The Data Subject cannot exercise the right to erasure if the data processing is necessary i) for the exercise of the right to freedom of expression and information; ii) for reasons of public interest in the area of public health; iii) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, if the right to erasure would seriously impair or prevent the achievement of the processing purposes; or iv) for the establishment, exercise, or defense of legal claims.

7.5. Right to Data Portability

Data portability allows the Data Subject to obtain and reuse their "own" personal data provided to the Data Controller for their own purposes and across different service providers. This right is limited to the data provided by the Data Subject and does not apply to other data (e.g., statistics, transaction data, loyalty program data, etc.).

The Data Subject may request:

- The personal data related to them (e.g., from a course or newsletter subscription) in a structured, widely used, and machine-readable format.
- The transfer of their data to another data controller.
- The direct transfer of their data to another data controller if technically feasible within the Data Controller’s system.

The Data Controller will fulfill portability requests only upon receiving a written request by email or post. The Data Controller will verify the identity of the Data Subject before fulfilling the request. This may require the Data Subject to appear in person at the Data Controller’s headquarters for identification purposes using the data stored in the system. The Data Subject may request the portability of their name, email address, and other data they have provided to the Data Controller. Exercising the right to data portability does not automatically lead to the deletion of data from the Data Controller’s system, and the Data Subject may continue to use the Data Controller’s services after exercising this right.

7.6. Right to Object to Data Processing

The Data Subject may object to the processing of their personal data, including profiling, at any time for reasons related to their particular situation. The Data Subject may also object to the processing of their personal data for direct marketing purposes, including profiling related to direct marketing. If the Data Subject objects to data processing for direct marketing purposes, the Data Controller will no longer process their data for such purposes.

The Data Subject may object in writing (by email or post), or by clicking the unsubscribe link provided in newsletters or other electronic messages sent to them.

7.7. Rights of Deceased Data Subjects

Within five years of the death of a Data Subject, the rights to access, rectification, deletion, restriction of processing, data portability, and objection, which the deceased would have had in life, may be exercised by the person authorized by the deceased in a public document or private document of full probative value, or by their close relative under the Civil Code. If multiple close relatives exist, the one who exercises this right first has priority.

Close relatives, as defined in the Civil Code, include spouses, direct descendants, adopted, step, and foster children, adoptive, step, and foster parents, and siblings. The close relative must provide:

- Proof of the deceased Data Subject's death, such as a death certificate or court ruling, and
- Proof of their own identity and, if necessary, their close relationship to the deceased, using official documents.

The person exercising the rights of the deceased is entitled to the same rights and obligations under the Data Protection Act and the Regulation as the deceased.

Upon written request, the Data Controller must inform the close relative of the actions taken unless the deceased explicitly prohibited this in their declaration.

7.8. Deadline for Processing Requests

The Data Controller will provide information to the Data Subject regarding actions taken in response to any request made under sections 6.1–6.6 without undue delay and within one month of receiving the request. This period may be extended by two additional months, considering the complexity and number of requests. If the extension is necessary, the Data Controller will notify the Data Subject of the delay and the reasons within one month of receiving the request. If the Data Subject submitted their request electronically, the information will also be provided electronically unless otherwise requested.

7.9. Right to Compensation and Damages

Any person who has suffered material or non-material damage as a result of a breach of the Regulation is entitled to compensation from the Data Controller or data processor. The data processor is only liable for damages if they did not comply with the specific obligations imposed on data processors by law or acted contrary to the lawful instructions of the Data Controller. The Data Controller and data processor are exempt from liability if they can prove that they were in no way responsible for the event causing the damage.

8. Options for Exercising Rights

The Data Subject may exercise their rights by submitting a request via email or postal mail. There is no possibility to exercise any rights over the phone.

The Data Subject can exercise their rights using the following contact details:

Name: Webshop Logisztika Kft.
Mailing address: 1097 Budapest, Ecseri út 14-16.
Email address: adatvedelem@webshoplog.hu

The Data Subject cannot enforce their rights if the Data Controller proves that it is unable to identify the Data Subject. If the Data Subject's request is clearly unfounded or excessive (especially considering its repetitive nature), the Data Controller may charge a reasonable fee for processing the request or refuse to act on the request. The burden of proof lies with the Data Controller. If the Data Controller has doubts about the identity of the individual making the request, they may request additional information necessary to confirm the requester's identity.

If the Data Subject disagrees with the decision of the Data Controller, they may:

1. Contact the National Authority for Data Protection and Freedom of Information (www.naih.hu; address: 1055 Budapest, Falk Miksa utca 9-11., Postal address: 1363 Budapest, Pf.: 9.; Phone: +36 (1) 391-1400)
2. Enforce their rights in court based on the Information Act, the Regulation, and the Civil Code (Act V of 2013).

9. Handling of Data Breaches

A data protection incident refers to a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data that has been transmitted, stored, or otherwise processed. The Data Controller keeps a record of data protection incidents for monitoring the measures taken, informing the supervisory authority, and notifying the Data Subject. This record includes the scope of the personal data affected, the categories and number of data subjects, the date and circumstances of the incident, its effects, and the measures taken to mitigate it. If the Data Controller deems that a particular incident poses a high risk to the rights and freedoms of the data subjects, they must inform the Data Subject and the supervisory authority of the data breach without undue delay, but no later than within 72 hours.

10. Data Provision to Authorities

The Data Controller may be contacted by the court, the prosecutor, the investigating authority, the misdemeanor authority, the administrative authority, the National Authority for Data Protection and Freedom of Information, or other bodies authorized by law to provide information, disclose data, transfer data, or make documents available.

The Data Controller will only disclose personal data to authorities if the authority specifies the exact purpose and the scope of the required data. The Data Controller will only release as much personal data as is strictly necessary to fulfill the purpose of the request.

11. Links

The Data Controller is not responsible for the content, data, and information protection practices of external websites accessible through links on the Website. If the Data Controller becomes aware that any linked site or link infringes on the rights of third parties or violates applicable laws, the link will be promptly removed from the Website.

12. Method of Data Storage and Security of Data Processing

The Data Controller commits to ensuring the security of data, taking technical and organizational measures, and establishing procedural rules that guarantee the protection of collected, stored, and processed data, and prevent their destruction, unauthorized use, or unauthorized alteration. The Data Controller also commits to informing any third parties to whom data are transferred or disclosed with the consent of the Data Subject to comply with data security requirements.

The Data Controller takes all possible precautions to prevent accidental damage or destruction of data. The above commitment also applies to the employees involved in the data processing activities of the Data Controller.

The IT systems and other data storage facilities of the Data Controller are located at its headquarters, offices, data processors, at Shoprenter Kft. (4028 Debrecen, Kassai út 129.), as well as at MediaCenter Hungary Kft. (6000 Kecskemét, Sosztakovics u. 3. II/6.), and in the server room at 1132 Budapest, Victor Hugo u. 18-22.

The Data Controller selects and operates IT tools used for processing personal data during service provision in such a way that:

a. the data is accessible to authorized persons (availability);
b. its authenticity and verification are ensured (data integrity);
c. its immutability is verifiable (data integrity);
d. it is protected against unauthorized access (data confidentiality).

The Data Controller protects the data with appropriate measures, particularly against unauthorized access, modification, transfer, disclosure, deletion, or destruction, as well as against accidental destruction, damage, and inaccessibility resulting from changes in technology.

To protect the electronically managed data sets in various records, the Data Controller uses appropriate technical solutions to ensure that stored data – except where permitted by law – cannot be directly linked to the data subject.

Considering the current level of technology, the Data Controller ensures the security of data processing by taking technical, organizational, and procedural measures that provide a level of protection appropriate to the risks related to data processing.

During data processing, the Data Controller ensures:

a) Confidentiality: protecting information to ensure that only authorized persons can access it;
b) Integrity: protecting the accuracy and completeness of the information and the processing methods;
c) Availability: ensuring that the authorized user can access the required information when needed, and that the necessary tools are available.

The IT systems and networks of the Data Controller and its partners are protected against computer-assisted fraud, espionage, sabotage, vandalism, fire, flood, computer viruses, computer intrusion, and attacks leading to denial of service. The operator ensures security through server-level and application-level protection procedures.

Data Subjects are informed that electronically transmitted messages over the internet, regardless of the protocol (email, web, FTP, etc.), are vulnerable to network threats that may result in fraudulent activities, contract disputes, or the disclosure or modification of information. To protect against such threats, the Data Controller takes all reasonable precautions. Systems are monitored to record any security deviations and provide evidence of any security incidents. Furthermore, system monitoring allows for verifying the effectiveness of the security measures implemented.

13. Other Provisions

The Data Controller reserves the right to unilaterally modify this Privacy Notice by providing prior notification to the Data Subjects through the website www.lovesexshop.co.uk. After the modifications take effect, the Data Subject – except in the case of objections – implicitly accepts the provisions of the modified Privacy Notice by continuing to use the website or services.

Complaints related to data processing can be submitted to the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság) at the following contact points:

- **In person:** The Authority's customer service at 1055 Budapest, Falk Miksa utca 9-11.
- **By mail:** 1363 Budapest, Pf.: 9.
- **By email:** kozerdekubejelentesek@naih.hu
- **Other contact information:** Tel: +36 (1) 391-1400, Fax: +36 (1) 391-1410, Email: ugyfelszolgalat@naih.hu, Website: www.naih.hu

This Privacy Notice is effective from May 25, 2018.

Last updated: June 06, 2025.