Tattooingatoz.com

Privacy Policy

BEVEZETÉS

LÁSZLÓ BORSOS (8900 ZALAEGERSZEG VERŐFÉNY UTCA 16., tax-number: 54777707140, registration number: 2169471) , (further on: Service-provider, Data processor) subdues itself under the following policy.

REGULATION (EEC) No 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 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 Regulation (EC) No 95/46, the following information is provided.

The present privacy policy guide regulates privacy of the following websites: https://tattooingatoz.com

The present privacy policy guide can be found on:
https://tattooingatoz.com/en/privacy-policy

Modifications to the data become effective when they appear on the webpage above.

THE DATA MANAGER AND CONTACT INFORMATION:

Name: LÁSZLÓ BORSOS
Seat: 8900 ZALAEGERSZEG, VERŐFÉNY UTCA 16.
E-mail: info@tattooingatoz.com
Telephone: +3692347889

EXPLANATORY TERMS

1. *„personal data”*: any data that can be related to the Customer – especially the name, username of the customer and any knowledge characteristic for one or more physical, physiological, mental, economic, cultural, or social identity of the Customer – and any conclusion related to the Customer drawn from the data;

2. „data management”: the totality of any operation or operations carried out in an automated or non-automated manner on personal data or data files, such as collecting, recording, organizing, tagging, storing, modifying or modifying, querying, inspecting, using, communicating, distributing or otherwise making available, aligning or linking, limiting, deleting or destroying;

3. „data manager”: means any natural or legal person, public authority, agency or any other body that determines the purposes and means of handling personal data individually or with others, where the purposes and means of data management are defined by Union or national law, the data controller or the particular aspects of the designation of the data controller may also be defined by Union or national law;

4. „data processor”: means any natural or legal person, public authority, agency or any other body that manages personal data on behalf of the data controller;

5. „recipient”: is a natural or legal person, a public authority, agency or any other body with whom or with which personal data is communicated, whether or not it is a third party. Public authorities which have access to personal data in an individual investigation in accordance with Union or national law shall not be considered recipients; the management of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of data management;

6. „the contributor concerned”: a voluntary, specific and appropriate informed and explicit statement of the will of the person concerned by which he or she expresses the statement or confirmation by means of an inadvertent act of affirmation that he or she has consented to the processing of personal data concerning him or her;

7. „dataprotection incident”: a security breach resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise treated.

THE PRINCIPLES OF PERSONAL DATA MANAGEMENT

The personal data:

a) must be legally and fairly handled and transparent to the person concerned ("lawfulness, fairness and transparency");

b) are collected for specified, clear and legitimate purposes and are not treated in a manner incompatible with these purposes; in accordance with Article 89 (1), no further data handling ("end-use") for purposes of public interest archiving for scientific and historical research purposes or for statistical purposes shall not be considered incompatible with the original purpose;

c) must be appropriate and relevant to the purposes of data management and should be limited to the need ("saving of the data");

d) must be accurate and, if necessary, up-to-date; all reasonable measures must be taken to correct or correct inaccurate personal data for the purposes of data management ("accuracy");

e) must be stored in a form which permits the identification of the data subjects only for the time needed to manage the personal data; the retention of personal data may only take place if the personal data are processed in accordance with Article 89 (1) for public interest archiving, for scientific and historical research purposes or for statistical purposes, in accordance with the rights and subject to appropriate technical and organizational measures for the protection of their freedoms ("limited storage");

f) shall be managed in such a way as to ensure adequate security of personal data, including the protection against unauthorized, unlawful, unintentional, loss or destruction of data ("integrity and confidentiality") by means of appropriate technical or organizational measures.

The data processor is responsible for the above, and must be able to demonstrate compliance ("accountability").

The data controller declares that its data management is carried out in accordance with the principles set out in this section.

DATA MANAGEMENTS

REGISTRATION (CREATION OF USER ACCOUNT)

1. Fact of data collection, the range of managed data and the **aim of data management:**

Personal data	Aim of data management	Legal Basis
First and Last Name	It is necessary for identification and secure access to the user account.	Article 6 (1) (a) and (b).
Email address	Keeping in touch, sending system messages, logging in to a user account.	
Password	Provides secure access to the user account.	
The date of registration.	The fulfillment of techincal operation.	
The IP address at the time of registration.	The fulfillment of techincal operation.	

2. **Range of Customers:** Everybody registered on the website.

3. **Time of data handling, deadline for data deletion:** If one of the conditions set out in Article 17 (1) of the GDPR is met, it lasts until the person concerned requests cancellation. Deleting the registration will immediately delete the personal data. The controller shall inform the data subject electronically in accordance with Article 19 of the GDPR of the deletion of any personal data provided by the data subject. If the data subject's request for cancellation also covers the e-mail address provided by the data subject, the data controller will also delete the e-mail address after the notification.

4. **Possible data managers entitled to know the data, the recipients of personal data:** Personal data may be handled by authorized personnel of the Data Controller in accordance with this Prospectus.

5. **Describe the rights of data subjects involved in data management:**

   - The data subject may apply to the data controller for access to, correction, deletion or limitation of the personal data concerning him, and
   - the data subject has the right to data storage and to withdraw the consent at any time.

6. **It is possible to initiate, delete, modify or restrict access to personal data, transferability of data, and objection to data processing in the following ways**:

   - By post at the address: 8900 ZALAEGERSZEG, VERŐFÉNY UTCA 16.,
   - Via e-mail: info@tattooingatoz.com
   - By telephone: +3692347889

7. **Legal basis for data processing**: Article 6 (1) (a) and (b).

8. We inform you that:

   - Data management **necessary for your consent or to take action at your request prior to the conclusion of the contract.**
   - **You are obliged** to provide personal information to register.
   - Failure to provide the data has the **consequence** that the user account cannot be created.

DATA MANAGEMENT RELATED TO THE USE OF THE SERVICE

1. Fact of data collection, the range of managed data and the aim of data management:

Personal data	Aim of data management	Legal basis
Password	Provides secure access to the user account.	Article 6 (1) (b) of the GDPR and Electronic Commerce Act. 13 / A. § (3).
First and last name	It is necessary for contacting us, using the service, and issuing a regular invoice.	
E-mail address	Stay in touch.	
Telephone	Stay in touch, coordinate billing issues more effectively.	
Billing name and address	Issuance of a regular invoice, as well as the creation of the contract, the definition and modification of its content, the monitoring of its fulfillment, the invoicing of the fees arising from it, and the enforcement of the related claims.	Article 6 (1) (c) and Section 169 (2) of Act C of 2000 on Accounting
The date of subscription/registration.	The fulfillment of techincal operation.	Article 6 (1) (b) of the GDPR and Electronic Commerce Act. 13 / A. § (3).
The IP address at the time of subscription/registration.	The fulfillment of techincal operation.	

2. **Range of Customers**: Everybody who is subscribing to / using the service.

3. **Time of data handling, deadline for data deletion**: If one of the conditions set out in Article 17 (1) of the GDPR is met, it will last until the person concerned requests cancellation. If the data subject's request for cancellation also covers the e-mail address provided by the data subject, the data controller will also delete the e-mail address after the notification. Except in the case of accounting documents, as these data must be kept for 8 years pursuant to Section 169 (2) of Act C of 2000 on Accounting. The data subject's contractual data may be deleted at the end of the civil limitation period on the basis of the data subject's request for cancellation.

   The accounting document (including general ledger accounts, analytical and detailed records) directly and indirectly supporting the accounting records must be kept in a legible form for at least 8 years, retrievable by reference to the accounting records.

4. **Possible data managers entitled to know the data, the recipients of personal data:** Personal data may be processed by the sales and marketing staff of the data controller, respecting the above principles.

5. **Describe the rights of data subjects involved in data management:**

• The data subject may apply to the data controller for access to, correction, deletion or limitation of the personal data concerning him, and
• the data subject has the right to data storage and to withdraw the consent at any time.

6. **It is possible to initiate, delete, modify or restrict access to personal data, transferability of data, and objection to data processing in the following ways**:

- By post at the address: 8900 ZALAEGERSZEG, VERŐFÉNY UTCA 16.,
- Via e-mail: info@tattooingatoz.com
- By telephone: +3692347889

7. **Legal basis for data processing:**

7.1. Article 6 (1) (b) and (c) of the GDPR,

7.2. CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (hereinafter: Elker TV. or Ecommerce Act) 13 / A. § (3):

The service provider may manage the personal data that are technically essential for the provision of the service in order to provide the service. In the case of identity of other terms, the service provider must choose and in all cases operate the means used to provide the information society service so that the processing of personal data is only necessary if it is strictly necessary for the provision of the service and for the fulfillment of other purposes specified in this Act. necessary, but in this case only to the extent and for the time necessary.

7.3. Article 6 (1) (c) in the case of an invoice in accordance with accounting legislation.

7.4. In the event of the claim arising from the contract, Act V of 2013 on the Civil Code 6:21. § 5 years.

6:22. § [Limitation]
(1. Except as otherwise provided in this Act, claims shall expire in five years.
(2) The limitation period begins when the claim becomes due.
(3) An agreement to change the limitation period shall be in writing.
(4) The limitation period is null and void.

8. We inform you that:

• **the data management is necessary for the fulfillment of the contract, the provision of the service and the use of the website.**
• You **must** provide personal information so that we can respond to the message.
• Failure to provide data has the **consequences** of not being able to complete your request.

CUSTOMER RELATIONSHIPS

1. The fact of data collection, the range of data processed and the purpose of data management:

Personal data	The purpose of data management	Legal basis
Name, email address, phone number.	Contact, identification, fulfillment of contracts, business purpose.	6 (1) (b) and (c), in the case of enforcement of claims arising from the contract, Act V of 2013 on the Civil Code 6:21. § cent

2. Range of affecteds: All those involved in contact with the data controller by phone / e-mail / personally or in a contractual relationship.

3. Duration of data management, deadline for deletion of data: The letters containing the requests will last until the request for cancellation of the data subject, but for a maximum of 2 years.

4. Persons authorized to access the data and the recipients of the personal data: The personal data may be handled by authorized personnel of the data controller, while respecting the above principles.

5. Describe the rights of data subjects involved in data management:

- The data subject may request from the controller access, rectification, erasure or restriction of the personal data relating to him or her, and
- the data subject has the right to data storage and the withdrawal of consent at any time.

6. It is possible to initiate, delete, modify or restrict access to personal data, transferability of data, and objection to data processing in the following ways:

- By post at the address: 8900 ZALAEGERSZEG, VERŐFÉNY UTCA 16.,
- Via e-mail: info@tattooingatoz.com
- By telephone: +3692347889

7. Legal basis for data processing:

8. We inform you that:

• **Data management is necessary for the performance of the contract and for giving offers.**

• You **must** provide personal information so we are able to fulfill the contract and the vendor is able to send an offer
• Failure to provide data has the **consequences** that the selected vendor is not going to be able to send You personalized offer and we can not fulfill the contract

COMPLAINT HANDLING

1. The fact of data collection, range of managed data and the aim of **data management**:

Personal data	Aim of data management	Claim
First and last name	Identification, contact.	Article 6 (1) (c) and the CLV of 1997 on consumer protection. Act 17 / A. (7).
E-mail address.	Contact.	
Telephone number	Contact.	
Billing name and address	Identification, handling of quality objections, issues and problems related to the ordered service.	

2. The range of customers: All those who buy and complain about the webshop website and complain about the quality objection.

3. The time period of data management and the deadline of deletion of data: Copies of the record of the objection, of the transcript and of the response given to it be retained for 5 years as set out in CLV 1997 on Consumer Protection. Act 17 / A. Section 7 (7) of this Act.

4. **The potential data managers entitled to know the data, the recipients of personal data:** Personal data can be managed by the sales and marketing staff of the data manager in respect for the above principles.

5. **Describe the rights of data subjects involved in data management:**

   • The data subject may apply to the data controller for access to, correction, deletion or limitation of the personal data concerning him or her, and
   • the data subject has the right of data storage and to withdraw the consent at any time.

6. **It is possible to initiate, delete, modify or restrict access to personal data, transferability of data, and objection to data processing in the following ways:**

   - By post at the address: 8900 ZALAEGERSZEG, VERŐFÉNY UTCA 16.,
   - Via e-mail: info@tattooingatoz.com
   - By telephone: +3692347889

7. We inform you that:

   • the provision of personal data is based on a **contractual obligation**.
   • The processing of personal data is a **prerequisite** for concluding a contract.
   • **be obliged** to provide personal information to handle your complaint.
   • Failure to provide data has the consequence that we will not be able to handle your complaint.

ADDRESSES WITH WHOM PERSONAL DATA IS COMMUNICATED WITH

„Recipient": any natural or legal person, public authority, agency or any other body with which personal data are disclosed, whether or not a third party is involved.

DATA PROCESSORS (WHO PERFORM DATA MANAGEMENT ON BEHALF OF THE DATA CONTROLLER)

The Data Controller uses data processors to facilitate its own data management activities and to fulfill its obligations under contract or legislation.

The Data Controller places great emphasis on using only data processors who either provide adequate guarantees to implement data management in compliance with GDPR requirements and to ensure adequate technical and organizational measures to protect the rights of stakeholders.

The data processor and any person acting under the control of the controller or the data processor who has access to personal data shall treat the personal data contained in these regulations only in accordance with the instructions of the data controller.

The controller is responsible for the data processing activities. The data processor is only liable for damages caused by data management if he or she has not complied with the obligations specified in the GDPR specifically for processors, or if the data controller has ignored or acted contrary to the lawful instructions of the data controller.

There is no substantive decision-making on data processing by the data processor.

EACH DATA PROCESSORS

Data processing activities	**NAME**	**ADDRESS, CONTACT**
Storage-provider	Zalaszám Informatika Kft.	8900 Zalaegerszeg, Mártírok útja 53. E-mail: info@zalaszam.hu, Telefon: +3692 502 500
Accounting tasks, invoicing	Peténé Ebedli Veronika	address: 8900 Zalaegerszeg, Kápolna-hegyi út 36. tax-number: 64503219-1-40 individual business registration number: 09684887 email: veronika1975@gylcomp.hu telephone: +36203766767
Online invoicing	Billingo Billingo Technologies Zrt.	Seat: 1133 Budapest, Árbóc utca 6. III. emelet E-mail: hello@billingo.hu

TRANSMISSION OF DATA TO THIRD-PARTIES

"Third party": means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who are authorized to process personal data under the direct control of the controller or processor; they got;

Third-party data controllers process the personal data we provide on their own behalf and in accordance with their own privacy policies.

DATA PROCESS	NAME	CONTACT DETAILS
Online payment	PayPal Parent company: eBay Incorporated	Seat: San Jose, California, USA Contact: https://www.paypal.com/hu Privacy Policy: https://www.paypal.com/hu/cgi-bin/helpscr?cmd=p/gen/ua/policy_privacy-outside
	Barion Payment Zrt.	License number: H-EN-I-1064/2013 Intézmény azonosító: 14859034 Telephone: + 36 1 464 70 99 E-mail: support@barion.com Terms: https://www.barion.com/hu/vasarlok/arak-vasarloknak/

USE OF COOKIES

1. The so-called "password used for a password-protected session", "shopping cart cookies", "security cookies", "Required cookies", "Functional cookies", and "cookies responsible for managing website statistics" prior consent of the data subject is not required for its use.

2. The fact of data handling, the range of data processed: Unique identification number, times, dates.

3. The range of customers: Everybody who visits the website.

4. Aim of data management: Identify users, keep a “shopping cart” record, and track visitors..

5. Term of data management, deadline for deletion of data:

Type of cookie	Legal basis of data management	Time of data management	Managed data
Session cookies	CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (Elkertv.) 13 / A. (3)	Until the end of the relevant visitor session	Connect.sid
Permanent or saved cookies	CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (Elkertv.) 13 / A. (3)	Until the deletion of the affected person	
Statistics cookies	CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (Elkertv.) 13 / A. (3)	1 month – 2 years	

List of cookies in detail:

- ea: device ID - identifies the device being browsed itself, not the person. Character: required, Validity: cookie renewable for 1-1 years
- jwt: json web token - identifies the logged in user. Type: required, Validity: session cookie
- lang: stores the language selected by the visitor. Character: functional, Validity: session cookie
- cart: contains links to the selected product in the webshop. Character: required, Validity: 1 day
- colorTheme: Records the color scheme of the user-defined profile, Character: functional, Validity: 1 year
- lightTheme: Captures the dark / light theme of the user-defined profile, Nature: functional, Validity: 1 year
- Cookies: Records the acceptance of a cookie management statement. Character: functional, Validity: 2 months
- warningText: Copyrighted content on the Theory, Practice, and Tasks: A cookie that controls the appearance of warning text. Character: functional, Validity: 1 week
- _ga: Required, Google Analytics requires a cookie to send data to the statistical system for measuring anonymous website traffic. Character: statistical, Validity: 2 years
- gat: a functional cookie required to send data to Google Analytics' statistical system for measuring anonymous website traffic, which contains the unique identifier of the given page. Character: statistical, Validity: 1 month
- _gid: Required cookie to send data to Google Analytics' anonymous website traffic statistics system. Character: statistical, Validity: 1 day
- _fbp: This cookie helps us deliver our ads to people
  provide those who had already visited our website when they were logged in
  by logging in to Facebook or operated by Facebook Advertising
  digital platform. Character: marketing, Validity: 3 months
- ba_vid: required, Barion cookie, to detect credit card fraud based on the device's digital fingerprint and browsing habits. Its use is necessary to detect fraudsters. The cookie ensures that the service provider knows if the data from the user's browsing habits comes from a user. Nature: statistical, Validity: 1.5 years since last update
- ba_sid: required, Barion cookie, designed to detect credit card fraud based
  on the device's digital fingerprint and browsing habits. The cookie ensures that we can identify your session on different websites. Character: statistical, Validity: 30 minutes

6. The potential data managers entitled to know the data: With the use of cookies the service provider does not manage personal data.

7. Giving information on the rights of the Customers related to data management: Customers can delete cookies in the Tools/Settings menu of the browser generally at the menu item Data protection.

8. Legal basis of data management: No consent is required if the sole purpose of the use of cookies is the communication service provided through the electronic communications network or the provision of information society services expressly requested by the subscriber or user.

9. Most browsers that our users use allow you to set which cookies to save and allow (specified) cookies to be deleted again. If you restrict or save third-party cookies on specific websites, this may in some circumstances result in our website not being fully usable. Here is information on how to customize cookie settings for standard browsers:

   Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)

   Internet Explorer (https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorer-delete-manage-cookies)

   Firefox (https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn

   Safari (https://support.apple.com/kb/PH21411?locale=hu_HU)

USE OF GOOGLE AND SOCIAL SERVICES

Use of Google Ads Conversion Tracking

1. The online advertising program, called "Google Ads," is used by the data controller and includes Google's conversion tracking service. Google Conversion Tracking is an analytics service provided by Google Inc. (1600 Amphitheater Parkway, Mountain View, CA 94043, USA; "Google").

2. When a User accesses a website via a Google ad, a cookie is placed on their computer to track conversions. These cookies have a limited validity and do not contain any personal data, so the User cannot be identified by them.

3. When the User browses certain pages of the website and the cookie has not expired, both Google and the data controller may see that the User has clicked on the advertisement.

4. Each Google Ads customer receives a different cookie, so they cannot be tracked through Ads customers' websites.

5. The information obtained through conversion tracking cookies is used to generate conversion statistics for Ads conversion tracking customers. This is how customers find out the number of users who clicked on your ad and sent to the page labeled conversion tracking. However, they do not have access to information that could identify any user.

6. If you do not wish to participate in conversion tracking, you can disable it by disabling cookies in your browser. You will then not be included in your conversion tracking statistics.

7. Further information and the Google Privacy Statement can be found at www.google.de/policies/privacy/

THE SERVICE OF GOOGLE ANALYTICS

1. This website uses the service of Google Analytics, which is the webanalyser service of the Google Inc. („Google"). The Google Analytics uses so called „cookies", textiles, which are saved on your computer, and they help the analysis of the website usage of the Users.

2. The cookies of the websites which were visited by the User and their connecting informations are sent and stored on one of the Google's servers in the USA. With the activation of the IP-anonymisation on the websites the Google can shorten the time of the IP-anonymisation of the Users in the European Union or in the member states of the European Economic Region.

3. Only in unique cases the full IP-addresses are sent to the servers of Google in the USA and they get shorten there. Operators of these websites commit the

Google to use these informations for interpretations about the usage of the website, furthermore to create reports about the activity of the website, and to do their website and internet usage related duties.

4. In the Google Analytics, the forwarded IP-address of the Users will not be matched with others data by the Google. The store of the cookies can be prevented in the settings of the web browsers, but in this way it can happen, if some features of the websites will not work. You can prevent Google from collecting datas about the website usage habits of the users (including IP-addresses too), if you download and setup this web browser plugin. https://tools.google.com/dlpage/gaoptout?hl=hu

FACEBOOK PIXEL

Facebook pixel is a code that is used to report conversions on a website, compile target audiences, and provide detailed analytics data about visitors 'use of the website. With the help of the Facebook remarketing pixel tracking code, you can display personalized offers and advertisements on the Facebook interface to the visitors of the website. The Facebook remarketing list is not personally identifiable. You can find more information about Facebook Pixel / Facebook Pixel at:
https://www.facebook.com/business/help/651294705016616

SOCIAL WEBSITES

1. The fact of data collection, range of managed data: name and public profile image of the Customer registered at Facebook/Twitter/Pinterest/ YouTube/Instagram etc.

2. The range of customers: All Customers registered at Facebook/Twitter/ Pinterest/YouTube/Instagram etc. and gave like to the website.

3. Purpose of the data collection: To share, or "like", promote certain content elements, products, actions of the web site or the website itself on social networking sites.

4. Duration of data processing, deadline for deletion of data, person of possible data controllers who are able to know the data and details of the data management rights of the data subjects: Information about the source, their handling, the method of transfer and the legal basis of the data can be consulted on the given social networking site. Data management takes place on social networking sites, so the duration of the data handling, the ways of deleting and modifying the data are governed by the rules of the respective community site.

5. Legal base of data management: voluntary consent of the Customer for the management of personal data at community sites.

CUSTOMER SERVICES AND OTHER DATA MANAGEMENT

1. If you have question during using some of the services of the data processor, or the customer has some problem you can get in contact with the data processer on the website (on phone, e-mail, community sites, etc.).

2. The data processer deletes the incoming e-mails, messages, on phone, on any community site, etc. what contains the name and e-mail address or any other given personal information of the customer, after 2 years from the start of the service.

3. We give information about the privacy policy which is not in this guide at the start of the service.

4. For exceptional magisterial request, or in case of law accumulation the service provider is bound for guidance, information providing, transferring, or making documents available for these organisation.

5. In these cases the service provider only gives personal informations for the request (if they pointed out the exact aim and the necessary informations) what are essentials for the aim of the request.

CUSTOMER RIGHTS

1. The right of access

You are entitled to receive feedback from the data controller about whether your personal data is being processed and, if such processing is in progress, you have the right to have access to your personal information and the information listed in the decree.

2. The right of rectification

You are entitled to request the data controller to rectify any inaccurate personal information that he or she is required to do without undue delay. Taking into account the purpose of data management, you are entitled to request the supplementation of incomplete personal data, including by means of a supplementary statement.

3. The right to cancel

You are entitled to request that the data controller, without undue delay, disclose personal information about you, and that the data controller is obliged to delete personal information about you, without undue delay, under certain conditions.

4. The right to be forgiven

If the data controller has disclosed the personal data and is required to cancel it, taking reasonable steps, including technical measures, to take into account the cost of available technology and implementation, in order to inform the data controllers handling the data that you have applied for the personal data in question pointing links or deleting a duplicate or duplicate of these personal data.

5. The right to restrict data management

You are entitled to request that your data controller restricts your data handling if one of the following conditions is met:

- You dispute the accuracy of your personal data; in this case, the restriction applies to the period of time that the data controller can check the accuracy of personal data;
- Data handling is illegal and you are opposed to the deletion of data and instead asks you to restrict them;
- The data controller no longer needs personal data for data processing, but you require them to submit, enforce, or protect legal claims;
- You have objected to data manipulation; in this case, the restriction applies to the period when it is established that the legitimate reasons for the data controller have priority over your legitimate reasons.

6. The right to data storage

You are entitled to receive personal data that is made available to you by a data controller in a fragmented, widely used machine-readable format and is entitled to transfer this data to another data controller without this being obstructed by the data controller whose provided personal information to you (...)

7. The right ro protest

You are entitled to object to the handling of your personal information (...), including profiling based on these provisions, for any reason relating to your own situation.

8. Protest in case of direct business acquisition

If your personal data is handled for direct business, you are entitled to protest at any time against the handling of personal data relating to it, including profiling, if it is related to direct business acquisition. If you object to personal data being handled for direct business purposes, your personal information can no longer be handled for that purpose.

9. Automated decision-making in individual cases, including profiling

You are entitled to exclude the scope of any decision based solely on automated data handling, including profiling, which would have a bearing on it or affect it significantly.
The preceding paragraph shall not apply if the decision is:

- You are required to conclude or complete a contract between you and the data controller;
- the granting of the right to a data controller is subject to the law of the Union or of the Member States which also lays down appropriate measures to protect your rights and freedoms and legitimate interests; or
- you are based on your explicit consent.

DEADLINE FOR ACTION

The data controller informs you of any measures taken in response to these requests without undue delay but in any way **within 1 month** of receipt of the request.

If necessary, it may be **extended by 2 months**. The controller will inform you about the extension of the deadline by indicating the cause of the delay **within 1 month** of receipt of the request.

If the data controller fails to take action upon your request, he or she will notify you **without delay and at the latest within one month of the receipt of the request** for reasons of non-action and whether you may file a complaint with a supervisory authority and exercise its right of appeal.

SECURITY OF DATA MANAGEMENT

The data controller and the data processor shall take appropriate technical and organizational measures to take into account the state of science and technology and the costs of implementation, the nature, scope, circumstances and objectives of data management and the risk of varying probability and severity of natural persons' rights and freedoms to guarantee an adequate level of data security, including, inter alia, where appropriate:

a) the pseudonymization and encryption of personal data;

(b) ensuring, maintaining, integrity, availability and resilience of the continuing confidentiality of systems and services used to manage personal data;

(c) in the case of a physical or technical incident, the ability to restore access to personal data and the availability of data in good time;

(d) the procedure for systematic testing, assessment and evaluation of the effectiveness of technical and organizational measures taken to ensure the security of data processing.

e) The data processed must be stored in such a way as to prevent unauthorized access. In the case of paper-based data carriers, by establishing the order of physical storage, filing, and using the central authorization system for data processed in electronic form.

f) The method of storing the data using the IT method must be chosen so that it can be deleted at the end of the period for deletion of data, or if it is necessary for other reasons, subject to a different cancellation deadline. The deletion must be irreversible.

(g) Paper-based media shall be deprived of personal data by means of a document shredder or by an external document destruction organization. In the case of electronic data carriers, physical destruction shall be ensured in accordance with the rules on the disposal of electronic media and, where necessary, the safe and irrevocable deletion of data shall be made in advance.

h) The data controller will take the following specific data security measures:

In order to ensure the security of personal data handled on paper, the Service Provider applies the following measures (physical protection):

i. Place documents in a secure, lockable dry room.
ii. If digitization of paper-based personal data is done, the rules governing digitally stored documents should apply.
iii. In the course of his work, the Service Provider's employee may only leave the room where data is being processed, to block the media entrusted to him or to close the room.
iv. Personal data may only be accessed by authorized persons and not accessible to third parties.

v. The Service Provider's building and premises are equipped with fire protection and property protection equipment.

b. *IT protection*

i. Computers and mobile devices (other media) used in data management are the property of the Service Provider.
ii. A computer system containing personal data that is useful to the Service Provider is provided with virus protection.
iii. For security of digitally stored data, the Service Provider uses data backups and archives.
iv. Access to the central server machine is only granted with the appropriate authority and only by designated persons.
v. Data on computers can only be accessed with a username and password.

INFORMING THE PERSON CONCERNED ABOUT THE PRIVACY INCIDENT

If the privacy incident is likely to pose a high risk to the rights and freedoms of natural persons, the data controller shall inform the data subject of the privacy incident without undue delay.

Information given to the data subject should be **clearly and easily understood** and the nature of the privacy incident must be disclosed and the name and contact details of the Data Protection Officer or other contact person providing additional information should be disclosed; the likely consequences of a data protection incident should be described; describe measures taken or planned by the data controller to remedy a data protection incident, including, where appropriate, measures to mitigate any adverse consequences of a data protection incident.

The person concerned shall not be informed if any of the following conditions are met:

- the data controller **has implemented appropriate technical and organizational protection measures** and applied these measures to the data covered by the data protection incident, in particular the measures, such as the use of encryption, which **make it impossible for persons who are unauthorized to access personal data the data**;
- after the data protection incident, the data controller has taken further measures to **ensure that high risk for the rights and freedoms of the person concerned is no longer likely to be realized**;
- Informing **would require disproportionate efforts**. In such cases, the data subject shall be informed by means of publicly disclosed information or a similar measure shall be taken to ensure that such information is equally effective.

If the data controller has not yet notified the data subject of the data protection incident, the supervisory authority may, after considering whether the privacy incident is likely to pose a high risk, may inform the data subject.

REPORTING A PRIVACY INCIDENT TO THE AUTHORITY

The data protection incident shall be reported to the supervisory authority under Article 55 without undue delay and, if possible, no later than 72 hours after the data protection incident becomes known, unless the data protection incident is unlikely to pose a risk to the rights of natural persons and freedom. If the notification is not filed within 72 hours, the reasons for proving the delay must also be enclosed.

REVIEW FOR MANDATORY DATA MANAGEMENT

If the period of mandatory data management or the periodic review of its necessity is not specified by law, local government regulation or a binding act of the European Union, **the controller shall review at least every three years from the commencement of the data processing** that it or the processor acting on its behalf or on its instructions and if the personal data management **is necessary** for the purpose of data management.

The circumstances and **results of this review shall be documented by the Data Controller, and shall be retained for a period of ten years** after the review has been conducted and made available to the Authority at the request of the National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority).

COMPLAINT OPPORTUNITY

Complaint regarding the possible breaching of the law by the data manager can be made to the Hungarian National Authority for Data Protection and Freedom of Information:

Hungarian National Authority for Data Protection and Freedom of Information
1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1374 Budapest, P.O.Box: 603.
Telephone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

CLOSING REMARKS

The following regulations were accounted in the course of composing the guide:

- REGULATION (EEC) No 2016/67 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 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 Regulation (EC) No 95/46
- 2011 CXII. Law on information self-determination and freedom of information (hereinafter: Infotv.)
- Act CVIII of 2001 - Act on Electronic Commerce and Information Society Services (especially Section 13 / A)
- Act XLVII of 2008 - Act on the Prohibition of Unfair Commercial Practices against Consumers;
- Act XLVIII. Of 2008 – the basic conditions and certain limitations of economic advertising activity (in particular Article 6)
- XC. Law of 2005 on Eletronic Freedom of Information
- Act C of 2003 on Electronic Communications (specifically Article 155)
- No. 16/2011. an opinion on the EASA / IAB Recommendation on Best Practice in Behavioral Online Advertising
- Recommendation of the National Data Protection and Information Authority on the data protection requirements for prior information