XBody Hungary Kft.

Shop.xbodyworld.com Policy Privacy

XBody Hungary Kft.
Privacy Policy

Contents

INTRODUCTION

XBody Hungary Kft. (1125 Budapest, György Aladár utca 35-39. , tax number: 11731324-2-43, company number: 0109194874), (hereinafter: Service-provider, Data processor) submits to the following policy.

The following Privacy Policy is provided in line with REGULATION (EU) 2016/679 of the EUROPEAN PARLIAMENT AND COUNCIL of 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 Directive 95 /46/EC (General Data Protection Regulation.

This Privacy Policy regulates the data processing of the following websites: https://shop.xbodyworld.com, https://xbodyworld.com, https://partnerportal.xbodyworld.com

This Privacy Policy can be found on: https://shop.xbodyworld.com/adatvedelem, https://shop.xbodyworld.com/privacy

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

THE DATA CONTROLLER AND CONTACT INFORMATION:

Name: XBody Hungary Kft.

Seat: 1125 Budapest, György Aladár utca 35-39.

E-mail: helpdesk@xbodyworld.com

Telephone: +3696200183

EXPLANATORY TERMS

1. “*personal data*”: any information relating to an identified or identifiable natural person ("data subject"); identifiable by a natural person who, directly or indirectly, in particular by virtue of one or more factors such as name, number, position, online identification or physical, physiological, genetic, intellectual, economic, cultural or social identity of the natural person identified;
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, organising, tagging, storing, modifying or modifying, querying, inspecting, using, communicating, distributing or otherwise making available, aligning or linking, limiting, deleting or destroying personal data;
3. “*data controller*”: 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 processing are defined by EU or national law, the data controller or the particular aspects of the designation of the data controller may also be defined by EU or national law;
4. “*data processor*”: any natural or legal person, public authority, agency or any other body that manages personal data on behalf of the data controller;
5. “*recipient*”: 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 EU 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. “*data protection 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

Personal data:
1. must be legally and fairly handled and transparent to the person concerned ("*lawfulness, fairness and transparency*");
2. is collected for specified, clear and legitimate purposes and is 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 that shall be considered incompatible with the original purpose;
3. must be appropriate and relevant to the purposes of data management and should be limited to the need ("*saving of the data*");
4. 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*");
5. must be stored in a form that 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 organisational measures for the protection of their freedoms ("*limited storage*");
6. shall be managed in such a way as to ensure adequate security of personal data, including the protection against unauthorised, unlawful, unintentional, loss or destruction of data ("*integrity and confidentiality*") by means of appropriate technical or organisational measures.
The Data Controller is responsible for the above, and must be able to demonstrate compliance ("*accountability*").
The Data Controller declares that data management is carried out in accordance with the principles set out in this section.

Data management related to the webshop operation/use of 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**
Username	Identification, enabling registration.	Article 6 (1) (b) GDPR and 13 / A. (3) of Act on E-commerce.
Password	It is for secure access to the user account.	
First name and last name	It is necessary for you to contact, to purchase and to issue a regular invoice.	
E-mail address	It is necessary for contact.	
Telephone	It is necessary for contact and more efficient matching of billing or shipping issues.	
Billing name and address	The issuance of a regular invoice, the creation of the contract, the definition, modification, fulfillment of the contract, the billing of the charges arising therefrom and the enforcement of the related claims.	Article 6 (1) (c) and Article 169 (2) of Act C of 2000 on Accounting
Delivery name and address	Allowing home delivery.	Article 6 (1) (b) GDPR and 13 / A. (3) of Act on E-commerce.
The date of purchase / registration.	The fulfillment of techincal operation.	
The IP address at the time of purchase / registration.	The fulfillment of techincal operation.	

It is not necessary for the username, nor the email address to contain any personal data.

2. Range of Customers: Everybody registered/making a purchase on the website.

3. Duration of data handling, deadline for data deletion: If one of the conditions set out in Article 17 (1) of the GDPR is met, the person concerned shall continue to apply for cancellation. Any deletion of any personal data provided by the data subject shall be communicated to the data subject electronically in accordance with Article 19 of the GDPR. If the data subject's cancellation request also covers the email address specified by him / her, the data manager will also delete the email address after the

notification. Except in the case of accounting documents, under § 169 (2) of Act C of 2000 on Accounting, these data must be retained for eight years.
The accounting document (including general ledger accounts, analytical and accounting records) supporting the accounts directly and indirectly must be kept in a legible form for at least 8 years, retrievable by reference to the accounting records.

4. Possible persons working as Data Controllers that are entitled to know the data, the recipients of personal data: Personal data may be handled by the sales and marketing staff of the Data Controller, respecting the above principles.

5. 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: 1125 Budapest, György Aladár utca 35-39.
- Via e-mail: helpdesk@xbodyworld.com
- By telephone: +3696200183

7. Legal basis for data management:
7.1. Article 6 (1) (b) and (c) of the GDPR,
7.2. In accordance with the CVIII Act of 2001 on certain aspects of electronic commerce services and information society services, (hereinafter referred to as Act on E-commerce) 13 / A. Section (3):
The service provider may manage the personal data that is technically necessary for the provision of the service in order to provide the service. The Service Provider shall, in the event that the other conditions are identical, select and in any case operate the tools used in the provision of the information society service in such a way that personal data will be processed only if it is strictly necessary for the service however, 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) Save 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. Please be advised

- that data management is **required for the performance of the contract** and for **the submission of an offer.**
- It is **required** to provide personal information so that we can fulfill your order.
- Failure to provide data **will mean** that we will not be able to process your order.

Newsletter, DM activity

1. According to § 6 of Act XLVIII of 2008 on the fundamental conditions of economic advertising activity the Customer may give consent in advance to the Service Provider for sending him/her advertisements and other consignments via the addresses given at registration.
2. Furthermore, the Customer may give consent to the Service Provider for managing the personal data for sending advertisements bearing in mind the regulations of the present guide.
3. The Service Provider shall send no unwanted advertisements and the Customer has the option to unsubscribe to the sending of advertisements without any limitations and without having to provide justification. In such case, the Service Provider shall delete all information – required for sending the messages – from the register and send no further offers. Customer can unsubscribe from receiving advertisements by clicking on the link in the message.
4. The fact of data collection, range of managed data and the **aim of data management**:

Personal data	**Aim of data management**	**Legal basis**
Name, e-mail address.	Identification, admit of subscription on the newsletter.	The consent of the data subject, Article 6 (1) (a) Section 6 (5) of the Act XLVIII. On the basic conditions and certain limitations of the economic advertising activity.
Date of subscription	The fulfillment of technical operation.	
IP address at the time of subscription	The fulfillment of technical operation.	

5. Stakeholders: All stakeholders who subscribe to the newsletter.
6. The aim of data collection: sending electronic messages (email, text message, push notification) containing advertisements to the Customer giving information on actual products, discounts, new functions, etc.
7. The time period of data management and the deadline of deletion of data: until the withdrawal of the consent, i.e. unsubscribing from the newsletter.
8. 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.
9. 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
- may object to the handling of such personal data as well
- the data subject has the right to data storage and to withdraw the consent at

any time.

10. 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: 1125 Budapest, György Aladár utca 35-39.
- Via e-mail: helpdesk@xbodyworld.com
- By telephone: +3696200183

11. The users are **free to unsubscribe** from the newsletters at any time, with no cost.

12. We inform you

that

· **Data management is based on your consent**.

· 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.

· We inform you that you can withdraw your consent at any time by clicking on unsubscribe.

· Withdrawal of consent does not affect **the legality of the consent-based prerevocation data management**.

Complaint handling

1. The fact of collecting data, the scope of the data processed and the **aim of data management**:

Personal data	Aim of data management	Legal basis
First name and last name	Identification, contact.	Article 6 (1) (c) and Act 17 / A. (7) of CLV 1997 on Consumer Protection.
E-mail address	Keeping contact.	
Telephone	Keeping contact	
Name and address for invoice	Identification, handling quality concerns, issues, and issues with the ordered service.	

2. Range of Customers: Anyone who buys on the website and makes a valid complaint about the quality.
3. Time of data handling, deadline for data deletion: Copies of the record of the objection, of the transcript and of the response thereto shall be given in accordance with the CLV of 1997 on Consumer Protection. Act 17 / A. Section 7 (7) of this Act shall be retained for five years.
4. Possible data controlelrs entitled to know the data, the recipients of personal data: Personal data can be managed by the sales and marketing staff of the Data Controller in respect for the above principles.
5. 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. You may initiate access, deletion, modification, or limitation of the handling of personal data, and the portability of data in the following ways:

- By post at the address: 1125 Budapest, György Aladár utca 35-39.
- Via e-mail: helpdesk@xbodyworld.com
- By telephone: +3696200183

7. We inform you that:

- the provision of personal data is **based on a legal 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.

Use of Cookies

1. Webshop-specific cookies are so-called "password-protected session cookies", "shopping cart cookies", and "security cookies", "Cookies required", "Functional cookies", and "Cookies that are responsible for managing the stats of a website", that require no prior consent from users.
2. The fact of data handling, the range of data processed: Unique identification number, times, dates.
3. The range of customers: All the people who visiting the website.
4. Aim of data management: Identifying users, to register your "shopping cart" and tracking visitors.
5. Term of data management, deadline for deletion of data:

Type of cookie	**Legal basis for data handling**	**Duration of data management**
Session cookies	Article 6 (1) point f) of the GDPR. The legitimate interest of the data controller is to operate the website, to ensure the functionality and basic functions of the website, and the security of the computer system.	The relevant session until the end of a visitor's session
Permanent or saved cookies	Article 6 (1) point f) of the GDPR. The legitimate interest of the data controller is to operate the website, to ensure the functionality and basic functions of the website, and the security of the computer system.	until the affected person is deleted
Statistical cookies	Article 6 (1) point a) of the GDPR	1 month - 2 years

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=en
Edge / Internet

Explorer: https://support.microsoft.com/en-us/windows/delete-and-manage-cookies-168dab11-0753-043d-7c16-ede5947fc64d
Firefox: https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox
Safari: https://support.apple.com/guide/safari/manage-cookies-sfri11471/mac

USING THE GOOGLE ADS CONVERSION TRACKING

1. The online advertising program called "Google Ads" is used by the Data Controlelr and uses the Google conversion tracking feature within its framework. Google conversion tracking is Google Inc.'s analytics service (1600 Amphitheater Parkway, Mountain View, CA 94043, USA; "Google").
2. When a User accesses a web site through a Google Ad, a conversion tracking cookie is placed on your computer. These cookies have limited validity and do not contain any personal information, so the User can not be identified by them.
3. When the User browses on certain pages of the website and the cookie has not expired, Google and the Data Controller will also see that the User clicked on the ad.
4. Each Google Ads customer receives a different cookie so that they can not be tracked through Ads clients' websites.
5. The information you receive through conversion tracking cookies is intended to make conversion statistics for your Ads conversion tracking customers. Customers will then be informed about the number of users who have been submitted to their ad and click on a conversion tracking tag. However, they do not have access to information that could identify any user.
6. If you do not want to participate in conversion tracking, you can disable this by blocking cookies from being installed on your browser. Then you will not be included in conversion tracking statistics.
7. For more information and Google Privacy Statement, visit:
www.google.de/policies/privacy/

USE OF THE GOOGLE ANALYTICS

1. This website uses Google Analytics, which is the webanalyser service of Google Inc. (“Google”). Google Analytics uses so called “cookies”, which are word files that are saved on your computer, and that help the analysis of the website usage of = Users.
2. The information generated by the cookies associated with the User's use of the Site is typically stored and stored on a Google server in the US. By activating the IP anonymization web site, Google will shorten the User's IP address within the Member States of the European Union or other States party to the European Economic Area Agreement.
3. The full IP address will only be forwarded to Google's server in the US and shortened there only in exceptional cases. On behalf of the operator of this website, Google will use this information to evaluate how the user has used the website, to provide the website operator with reports related to the web site activity, and to provide the website operator with reports related to the activity of the website and to provide additional services related to the use of the website and the internet.
4. Within Google Analytics, the IP address transmitted by the User's browser is not reconciled with other Google data. The User may prevent the storage of cookies by properly configuring his / her browser, however, please note that in this case not all features of this website may be fully utilized. You may also prevent Google from collecting and processing the User's information on your use of the Website (including your IP address) by downloading and installing the browser plug-in at the following link. https://tools.google.com/dlpage/gaoptout?hl=hu

RECIPIENTS, ADDRESSED WITH THE PERSONAL DATA

„*Recipient*”: means 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 are managing data in the name of the data manager)

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 rules only in accordance with the instructions of the 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.
The data controller can use a hosting provider to deliver the IT back-office, as well as a courier service to deliver the ordered products as a data processor.

Particular data processors

Data management activity	**Name, address, contact**
Storage-provider	KingSol Zrt. Seat: 1084 Budapest, Tolnai Lajos utca 18 3. em 4. Company reg. number: 01-09-948538 Tax number: 23004122-2-42, erdeklodes@kingsol.hu
Data processer used during the data management	Salesforce, Salesforce.com EMEA Limited, village 9, floor 26 Salesforce Tower, 110 Bishopsgate, London, UK, EC2N 4AY (task: receive and send messages)

Transmission of data to third parties

„*third party*" means any natural or legal person, public authority, agency or any other body which is not the same as the data subject, the controller, the data processor or the persons empowered to process personal data under the direct control of the controller or processor; they got;
Third-party data controllers, in their own name, manage their personal data in accordance with their own privacy policies.

Data management activity	Name, address, contact
Transport	UPS Magyarország Kft., Lőrinci utca 154. Airport City Logistic Park, G épület 2220 Vecsés Hungary (+3618770000) DHL Express Magyarország Kft., 1185 Budapest, BUD Nemzetközi repülőtér, terminál 1., DHL Express épület 302.
Online Payment	CIB Bank Zrt. CIB Bank Ltd. H-1027 Budapest, Medve utca 4–14. H-1995 Budapest Telefon: (06 1) 423 1000 Fax: (06 1) 489 6500 Nyilvántartó cégbíróság: Fővárosi Törvényszék Cégbírósága Cégjegyzékszám: Cg. 01-10-041004 Adószám: 10136915-4-44 CSASZ: 17781028-5-44 Közösségi adószám: HU17781028 Tőzsdetagság: Budapesti Értéktőzsde Zrt. Tevékenységi engedély száma: 957/1997/F, III/41. 044-10/2002. BIC (SWIFT) kód: CIBHHUHB

SOCIAL WEBSITES

1. The fact of data collection, range of managed data: name and public profile image of the Customer registered at Meta/Twitter/Pinterest/YouTube/Instagram etc.
2. Concerning: Anyone who has registered on Meta/Twitter/Pinterest/Youtube/Instagram etc. social networking sites and "liked" the Service Provider's social networking site or contacted the Data Controller through a social networking site.
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. Should you have any questions or problems in using our data management services, you may contact the Data Controller in the ways specified on the website (telephone, e-mail, social networking sites, etc.).
2. The Data Controller deletes the incoming emails, messages, on phone, or anything on any social media site, etc. that contains the name and email address or any other given personal information of the customer, after 2 years from the start of the service.
3. Data handling not listed in this policy will be provided at the time of data collection.
4. The Service Provider is obliged to provide guidance, information, data and documents upon exceptional request of the authorities or upon request of other bodies authorised by law.
5. In these cases, the Service Provider will provide the requester with personal data only to the extent and to the extent necessary to fulfill the purpose of the request, provided that the exact purpose and scope of the data have been indicated.

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 deletion

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 delete it, it shall 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 European Union or of the Member States which also lays down appropriate measures to protect your rights and freedoms and legitimate interests; or
- 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 one month** of receipt of the request.
If necessary, it may be **extended by two months**. The controller will inform you about the extension of the deadline by indicating the cause of the delay within one 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 organisational 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:

1. the pseudonymization and encryption of personal data;
2. ensuring, maintaining, integrity, availability and resilience of the continuing confidentiality of systems and services used to manage personal data;
3. 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;
4. the procedure for systematic testing, assessment and evaluation of the effectiveness of technical and organisational measures taken to ensure the security of data processing.
5. 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.
6. 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.
7. Paper-based media shall be deprived of personal data by means of a document shredder or by an external document destruction organisation. 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.
8. 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*):

1. Place documents in a secure, lockable dry room.
2. The Service Provider's building and premises are equipped with fire protection and property protection equipment.
3. Personal data may only be accessed by authorised persons and not accessible to third parties.
4. 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.
5. If digitization of paper-based personal data is carried out, the rules governing

digitally stored documents should apply.

IT protection

1. The computers and mobile devices (other data carriers) used for data management are the property of the Service Provider.
2. The computer system containing personal data used by the Service Provider is virus-protected.
3. The Service Provider uses data backups and archives to ensure the security of digitally stored data.
4. The central server machine may be accessed only by duly authorized persons.
5. The data on the 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 realised**;
- 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 is managed 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

A 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:

Nemzeti Adatvédelmi és Információszabadság Hatóság
1055 Budapest, Falk Miksa utca 9-11.
Levelezési cím: 1363 Budapest, Pf. 9.
Telefon: +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 (EU) 2016/679 of the EUROPEAN PARLIAMENT AND COUNCIL of 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 Directive 95 /46/EC (General Data Protection Regulation
- 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