DATA PRIVACY STATEMENT EFFECTIVE FROM 2026-06-01

Download

1. INTRODUCTION

1.1.Shiver Korlátolt Felelősségű Társaság (registered office: 3508 Miskolc, Csaba vezér út 129.) as data controller – hereinafter: Data Controller – informs data subjects about the following facts and circumstances based on **Article 12(1) of Regulation (EU) 2016/679 of the European Parliament and of the 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** – hereinafter: **GDPR**, and **Section 20 of Act CXII of 2011 on the freedom of information** – hereinafter: **Info Act**, in order to **implement the GDPR** and the **Info Act** by way of this **Data Privacy Statement** before starting to control their personal data.

Data control that is subject to the **GDPR** and the **Info Act applies only to the data of natural persons**, they do not apply to controlling the data of legal persons and other business entities. Data control performed by natural persons only in the framework of their personal or home activities, that is, data control that cannot be associated with any professional or business activities, is not subject to the **GDPR** and the **Info Act**. The contents of this statement apply to automated data control, i.e. performed electronically, simply by computer, as well as to manual data control.

1.1. Data of the data controller

Company name	**Shiver Korlátolt Felelősségű Társaság**
Registered office	3508 Miskolc, Csaba vezér út 129.
Company registration number	05-09-023947

Tax number	23890833-2-05
Statistical number	23890833-4511-113-05
Account managing bank, bank account number	OTP Bank Nyrt. 11734004-20499598
Contact person’s name and contact details	Ágnes Kovács, https://oem-bike-parts.com/contact

1.3. Websites where data control actually takes place

- https://oem-bike-parts.com/

hereinafter: **Websites**
The **data controller’s task** is to respect the privacy of natural persons and to determine fundamental rules for data control in order to do so. The effect of the **GDPR** and the **Info Act** applies to all data controlling and data processing of data of natural persons. The provisions of the **GDPR** and the **Info Act** shall apply to data control and data processing both using a fully or partly automated tool and done manually. The provisions of the **GDPR** and the **Info Act** need not be applied to data control by natural persons solely for their personal purposes.

1.4. List of applicable legislation:

1. Regulation (EU) 2016/679 of the European Parliament and of the 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 (**GDPR**);
2. Act CXII of 2011 on informational self-determination and the freedom of information (Info Act);
3. The Fundamental Law of Hungary;
4. Act V of 2013 on the Civil Code ();
5. Act CXXXVI of 2007 on the prevention and combating of money laundering and terrorist financing ();
6. Act CLV of 1997 on consumer protection (**Fgy tv.**);

7. Act CVIII of 2001 on electronic commerce and the information society (**Eker tv.**);
8. Act XLVIII of 2008 on the basic requirements and certain restrictions of commercial advertising activities (**Advertising Act**);
9. Act C of 2000 on accounting (**Accounting Act**).

1.5. Definitions of terms

For the purposes of this statement:

1. **data controller:**Shiver Kft.
2. **Authority: National Authority for Data Protection and Freedom of Information**(1125 Budapest, Szilágyi Erzsébet fasor 22/c, phone: 1/391-1400, e-mail: ugyfelszolgalat@naih.hu)
3. **personal data:**any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
4. **data control:**any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
5. **restriction of processing:**the marking of stored personal data with the aim of limiting their processing in the future;
6. **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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
7. **pseudonymisation:**the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
8. **filing system:**any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
9. **controller:**the natural or legal person, public authority, agency or other body which, alone

or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

10. **processor:**a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
11. **recipient:**a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
12. **third party:**a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
13. **consent of the data subject:**any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
14. **personal data breach:**a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
15. **biometric data:**personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
16. **data concerning health:**personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
17. **main establishment:**

1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

18. **representative:**a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
19. **enterprise:**a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
20. **group of undertakings:**a controlling undertaking and its controlled undertakings;
21. **binding corporate rules:**personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
22. **supervisory authority:**an independent public authority which is established by a Member State pursuant to Article 51;
23. **supervisory authority concerned:**a supervisory authority which is concerned by the processing of personal data because:

    1. the controller or processor is established on the territory of the Member State of that supervisory authority;
    2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
    3. a complaint has been lodged with that supervisory authority;

24. **cross-border processing:**

1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

25. **relevant and reasoned objection:**an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
26. **information society service:**a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;
27. **international organisation:**an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

1.6. The controller will not collect and control genetic data, biometric data and data related to health, that is, collectively: special data, and personal data of minors below the age of 16 years. The consent or subsequent approval of the legal representative of a minor who has reached 16 years of age is not required for the minor’s legal statement containing their consent to data controlling to be valid.

2. THE PURPOSE AND LEGAL GROUNDS FOR DATA CONTROL

DATA CONTROL ACTIVITIES CARRIED OUT BY THE CONTROLLER:

1. Consent given in a contract concluded with the data subject
2. Recording of phone conversations
3. Payment by bank card
4. Website visitor data
5. Website cookies management
6. Registrations on websites
7. Building data bases for marketing and commercial purposes
8. Data control for newsletter subscription

9. Mandatory data control
10. Other data control

2.1. Consent given in a contract concluded with the data subject

The controller operates a webstore at the following websites, through which a contract for the sale and purchase of products may be concluded electronically between the controller as seller and the data subject as buyer with or without registration in the webstore. The purpose of operating the webstore is the conclusion of a sale and purchase contract for a product electronically between the parties, and delivery of the sale and purchase contract. The procedure for the electronic conclusion of the sale and purchase contract, and the rights and obligations of the parties are governed by the General Terms and Conditions available on the controller's web pages.
The webstores are accessible on the websites listed in section 1.3.

The purpose of data control
In the event that a contract for the sale and purchase of products is concluded electronically between the controller as seller and the data subject as buyer, the purpose of data control is the delivery of the contract concluded between the parties.
Legal grounds for data control:
Data subject's consent according to Article 6(1)b) of the GDPR, Section 5(1)a) of the Info Act.

Scope of data controlled:

Details of the contracting party:	**Delivery details:**	**Invoicing details:**	**Other:**
a) name (family name, given name)	a) recipient's name	a) name of person requesting the invoice	a) IP addresses

b) e-mail address	b) delivery address (country, county, postal code, city, district, street name, street type, house number/topographic lot number, building, stairwell, floor, door number)	b) invoicing address (country, county, postal code, city, district, street name, street type, house number/topographic lot number, building, stairwell, floor, door number)	b) date of last visit
c) phone number			c) GEO code (based on delivery and invoicing address, to verify the correct address)

Consequences of failure to provide data
The sale and purchase contract for the product is not concluded between the parties.

Duration of data control:
The controller will store the data until the following goals are met:

1. when the price of the product ordered is paid;
2. in the event the data subject failed to pay the price of the product, until the dispute concerning the claim is concluded with final and conclusive effect, the claim reaches its statute of limitations;
3. the contract is terminated in whatever manner.

Processor:

Company name	Registered office, website	Data processing activity	Scope of data processed
Billingo Technologies Zrt.	1133 Budapest, Árbóc utca 6. 3rd floor, https://billingo.hu/	Invoicing of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and "Invoicing details" columns of the "Scope of data controlled" table set out in section 2.1.
N-Ware Informatikai és Tanácsadó Kft	1139 Budapest, Gömb utca 26., https://billzone.eu/	Invoicing of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and "Invoicing details" columns of the "Scope of data controlled" table set out in section 2.1.
GLS General Logistics Systems Hungary Csomag-Logisztikai Kft.	2351 Alsónémedi GLS Európa u. 2., https://gls-group.eu/	Delivery of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and “Delivery details" columns of the "Scope of data controlled" table set out in section 2.1.

UPS Magyarország Kft.	2220 Vecsés, Lőrinci utca 154. Airport City Logistic Park, G épület, https://www.ups.com/hu/	Delivery of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and “Delivery details" columns of the "Scope of data controlled" table set out in section 2.1.
DHL Express Magyarország Szállítmányozó és Szolgáltató Kft.	1185 Budapest, BUD International Airport airport building 302, http://www.dhl.hu/hu/	Delivery of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and “Delivery details" columns of the "Scope of data controlled" table set out in section 2.1.
DPD Hungária Kft.	1134 Budapest, Váci út 33. 2nd floor, https://www.dpd.com/hu/	Delivery of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and “Delivery details" columns of the "Scope of data controlled" table set out in section 2.1.
FedEx Express International B.V.	Taurusavenue 111, 2132 LS Hoofddorp, The Netherlands, https://www.fedex.com/	Delivery of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and “Delivery details" columns of the "Scope of data controlled" table set out in section 2.1.

FedEx Corporation	11000 Ridgeway Loop Road, Ste 600, Memphis, TN 38120, United States of America, https://www.fedex.com/	Delivery of the products ordered to the data subjects.	Details listed in the "Details of the contracting party" and “Delivery details" columns of the "Scope of data controlled" table set out in section 2.1.

Data processing technology: manual and automated data processing.

Data transmission: In order to enforce its claim, the processor may transmit personal data - name, address, e-mail address, phone number - to the following third parties:

1. legal counsel providing legal representation for the controller;
2. Hungarian Chamber of Notaries (MOKK);
3. competent court;
4. competent independent court foreclosure agent;
5. controller’s account managing bank (in case of payment by bank card).

2.2. Recording of phone conversations

Based on the data subject’s consent, the controller will record conversations with the call centre based on acceptance of the verbal information provided upon receiving the call.

Purpose of controlling and call registration:

1. verbal statements made by way of the telephone call centre should be possible to confirm ex post in order to prove the justified interests of the data subject and the controller;

2. listening to and use of the voice recording to confirm statements and reports made to the call centre lter on.

Data subjects may request a copy of the voice recording. The controller shall fulfill requests within **15 days** of receiving a request for each request, free of charge, and send the copy of the voice recording by mail, on single-write media. Data subjects have the possibility of listening to the voice recording at the controller's customer service.

Legal grounds for data control: Data subject's consent according to **Article 6(1) paragraphs a) and b) of the GDPR, Section 5(1)a) of the Info Act.**

Article 6(1)b) of the GDPR:
"Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

The **consent** granted to data controlling on the basis of **Article 6(1)a) of the GDPR may be withdrawn at any time**. The withdrawal will not affect the lawfulness of data control carried out on the basis of consent before the withdrawal.

Scope of data controlled:

1. name (family name, given name)
2. phone number

Duration of data control: Voice recordings are stored by dynamic use of the available storage capacity in the IT system developed especially for this purpose. When the storage capacity is full, the voice recording recorded earliest will be deleted. The controller will store the voice recordings made for **5 years** from the closure of the claim or termination of the contractual relationship.

2.3. PAYMENT BY BANK CARD

Purpose of data control: in case of payment by bank card, the controller will control and transmit to its account managing bank, if necessary, the following data based on the data subject who is the payer:

1. name of the paying data subject as shown in the bank card;
2. amount paid;
3. bank card number, validity details;
4. security data required for verification of payment validity.

Legal grounds for data control: Data subject's consent according to Article 6(1)b) of the GDPR, Section 5(1)a) of the Info Act.

Processor:

Company name	**Registered office, website**	**Data processing activity**	**Scope of data processed**

SimplePay - OTP Mobil Kft.	1093 Budapest, Közraktár u. 30-32., https://simplepay.hu	Payment page operator, execution of payment transaction.	Details shown in section 2.3. paragraphs a), b), c) and d)
Adyen online payment - ADYEN NV	1011 DJ Amsterdam, Simon Carmiggeltstraat 6-50, P.O. Box 10095, 1001 EB AMSTERDAM, The Netherlands https://www.adyen.com/	Payment page operator, execution of payment transaction.	Details shown in section 2.3. paragraphs a), b), c) and d)
Google Pay - Google Ireland Limited.	Gordon House, Barrow Street, Dublin, D04 E5W5, Dublin, Ireland https://payments.google.com/	Payment page operator, execution of payment transaction.	Details shown in section 2.3. paragraphs a), b), c) and d)

Duration of data control: the controller controls the above data for the purposes of enforcing claims, in line with the requirements of the Accounting Act, for the period specified in the Act. The account managing bank will control the above data for the purpose and duration defined in effective legislation and its own regulations.

2.4. Website visitor data

Website visits are realised by clicking on the controller’s web pages.

The purpose of data control: During visits to the website, the controller records visitor data in order to verify the functioning of services, to ensure custom service and to prevent abuse.

Legal grounds for data control: Data subject's consent according to **Article 6(1)a) of the GDPR, Section 5(1)a) of the Info Act** and **Section 13/A(3) of the Eker tv.**

The **consent** granted to data controlling on the basis of **Article 6(1)a) of the GDPR may be withdrawn at any time**. The withdrawal will not affect the lawfulness of data control carried out on the basis of consent before the withdrawal.

Scope of data controlled:

1. identification number;
2. date;
3. time;
4. address of the page visited;
5. IP address of the user's computer;
6. properties of the user's platform (e.g. type of browser, operating system, etc.)

The controller will not link the data arising in the course of checking log files with other information and will not attempt to identify users.

Duration of data control: 1 year

Data control by external service providers: The portal's html code contains links coming in from and pointing to external servers that are independent from the controller. Servers of external service providers are connected directly to the user's computer, so the providers of these links are able to collect user data due to direct communication with the user's browser. Custom contents are served by the servers of external service providers. The connection between the servers of the controller and of the external service providers extends solely to the

insertion of the codes of the latter, so that no personal data are transferred or transmitted.

The following controllers are able to provide detailed information on the controlling of data by servers of external service providers: Independent measurement and audit of website visits and other web analytics data are assisted by the servers of Google Analytics, Hotjar, Smartlook and Facebook. Detailed information on the treatment of measurement data is available to the controller from www.google-analytics.com, www.hotjar.com, www.smartlook.com and facebook.com In order to track users and to display customised recommendations, the tracking codes of Google Analytics, Hotjar, Smartlook and Facebook were embedded in the website code.

In order to ensure customised service, external service providers place and read a small data package, a so-called cookie. If the browser returns a cookie saved earlier, the service providers managing that cookie have an opportunity to link the user’s current visit to their earlier visits, but only in respect of their own content.

The user is able to delete the cookie from their own computer or may block the use of cookies in the browser. In general, cookies can be managed in the Tools/Settings menu of the browser under Privacy settings, under the label Cookies.

2.5. Website cookies management

In order to ensure customised service, the website operator installs and reads a small data package, a so-called cookie, on the user’s computer. If the browser returns a cookie saved earlier, the service providers managing that cookie have an opportunity to link the user’s current visit to their earlier visits, but only in respect of their own content. Users may delete the cookie from their own computers, or may block the use of cookies in the browser. In general, cookies can be managed in the Tools/Settings menu of the browser under Privacy settings, under the label Cookies.

The controller as seller does not use cookies to transmit personal data.

Scope of data controlled:

1. identification number;
2. date;
3. time;
4. address of the page visited;
5. IP address of the user's computer;
6. properties of the user's platform (e.g. type of browser, operating system, etc.)

The purpose of data control: Identification and distinction of users, identification of the user's current session, storage of the data provided during the session, prevention of data loss.

Legal grounds for data control: Data subject's consent according to **Article 6(1)a) of the GDPR, Section 5(1)a) of the Info Act.**

The **consent** granted to data controlling on the basis of **Article 6(1)a) of the GDPR may be withdrawn at any time**. The withdrawal will not affect the lawfulness of data control carried out on the basis of consent before the withdrawal.

Duration of data control: duration of the session launched by the visitor on the website, 1 year for registered users.

2.6. Registrations on websites

Purpose of data control: to improve and accelerate user experience, facilitate information related to orders, display order history.

In the course of online registration, only personal data absolutely necessary for registration may be controlled.

You have the option to register in the webstore using your Facebook or Google account. In the event you decide to make use of either of these options, the link selected will redirect you to the Facebook Admin/Google LLC page, where the service provider concerned will inform you about the manner in which your data provided to us by them are handled. You may learn about the data privacy guidelines of Facebook or Google by clicking the following link: https://www.facebook.com/about/privacy, https://policies.google.com/privacy

Scope of data controlled: Details listed in the "Scope of data controlled" table set out in section 2.1.

Legal grounds for data control: Data subject’s consent according to **Article 6(1)a) of the GDPR, Section 5(1)a) of the Info Act.**

The **consent** granted to data controlling on the basis of **Article 6(1)a) of the GDPR may be withdrawn at any time**. The withdrawal will not affect the lawfulness of data control carried out on the basis of consent before the withdrawal.

2.7. Building data bases for marketing and commercial purposes

The website operated by the controller offers an opportunity for data subjects to consent to being recorded in the controller's commercial data base, and to be contacted with relevant offers at the contact details provided by the data subject.

Scope of data controlled:

1. name (family name, given name)
2. invoicing address (country, county, postal code, city, district, street name, street type, house number/topographic lot number, building, stairwell, floor, door number);
3. phone number;
4. e-mail address.

The purpose of data control: Building a data base, contacting data subjects with the controller's offers using the contact details provided by the data subject.

Legal grounds for data control: Data subject's consent according to **Article 6(1)a) of the GDPR, Section 5(1)a) of the Info Act.**

The **consent** granted to data controlling on the basis of **Article 6(1)a) of the GDPR may be withdrawn at any time**. The withdrawal will not affect the lawfulness of data control carried out on the basis of consent before the withdrawal.

Duration of data control: Until the purpose of data control is achieved, for 24 months after the last contact.

Withdrawal of the consent given to registration in the data base and the **deletion or modification of personal data** may be requested at:

Name	**Shiver Kft.**
Address:	**3508 Miskolc, Csaba vezér út 129.**
E-mail	hello@oem-bike-parts.com

2.8. Data control for newsletter subscription

According to Section 6 of the Advertising Act, the subscriber may clearly and expressly consent in advance to be contacted by the service provider on contact details provided at the time of registration with advertising offers and other correspondence, and to the controlling of subscriber's personal data required for sending commercial offers by the service provider. Subscribers may unsubscribe from receiving offers without restriction and without having to give reasons, free of charge, by clicking on the link included in the e-mail message or in an e-mail sent to hello@oem-bike-parts.com. In case of unsubscribing, the service provider will not contact the subscriber with any more advertising offers and will delete the subscriber's personal data from the register.

Scope of data controlled:

1. name (family name, given name);
2. e-mail address;
3. mailing address;
4. phone number;
5. IP address of the data subject's computer;
6. statement of consent;

The purpose of data control: Despatch of electronic messages containing advertising, on a custom basis, and information on current promotions, information, products, new products and

new functions.

Legal grounds for data control: Data subject's consent according to **Section 6 of the Advertising Act, Section 13/A(4) of the Eker tv., Article 6(1)a) of the GDPR, Section 5(1)a) of the Info Act.**

The **consent** granted to data controlling on the basis of **Article 6(1)a) of the GDPR may be withdrawn at any time**. The withdrawal will not affect the lawfulness of data control carried out on the basis of consent before the withdrawal.

Duration of data control: Until withdrawal of consent, i.e. unsubscribing from the newsletter.

Withdrawal of the consent given to newsletter subscription and the **deletion of personal data** may be requested by clicking on the link in the message, and **modification of personal data** may be requested at the following address:

Name	**Shiver Kft.**
Address:	**3508 Miskolc, Csaba vezér út 129.**
E-mail	hello@oem-bike-parts.com

Processor:

Company name	**Registered office, website**	**Data processing activity**	**Scope of data processed**

SendGrid, Inc.	1801 California Street, Suite 500, Denver, Colorado 80202 USA https://sendgrid.com/	Newsletter mailing service provider.	name (family name, given name); e-mail address; mailing address; phone number; IP address of the data subject's computer;

2.9. Mandatory data control

2.9.1. Provisions of accounting and tax legislation

Purpose and legal grounds of data control: The data controller controls the accounting documents containing the name and address of the data subject/payer and the data to be indicated mandatorily based on law as **mandatory data control** based on **Article 6(1)c) of the GDPR, Section 5(1)b) of the Info Act,** on the basis of **Section 169 of the Accounting Act.**

Source of data: the data provided by the data subjects.

Scope of data required for achieving the purpose of data control:

1. name of payer;
2. amount paid;
3. date of payment.

Duration of data control: The controller shall control data for **8 years** from the date when the data were generated according to **Section 169(2) of the Accounting Act**.

Data transmission: Hungarian Tax and Customs Authority

Data processing technology: manual and automated data processing.

2.9.2. Complaint management

Purpose and legal grounds of data control: The data controller manages consumer complaints regulated in **Section 17/A of the Fgy tv.** as **mandatory data control** based on **Article 6(1)c) of the GDPR** and **Section 5(1)b) of the Info Act.**

Source of data: the data provided by the data subjects.

Scope of data required for achieving the purpose of data control:

1. name (family name, given name);
2. e-mail;
3. phone number;
4. invoicing address (country, county, postal code, city, district, street name, street type, house number/topographic lot number, building, stairwell, floor, door number);
5. bank account number;
6. The minutes taken about the complaint shall include the following:
    1. name and address of the consumer,
    2. the place, time and method of submitting the complaint,
    3. detailed description of the consumer complaint, the list of papers, documents and other evidence presented by the consumer,
    4. a statement from the undertaking on its position concerning the consumer's complaint, if the complaint can be investigated immediately,

5. the signatures of the person recording the minutes and of the consumer, except for complaints communicated by phone or using electronic communications services,
6. the place and time of recording the minutes,
7. for complaints communicated by phone or using electronic communications services, the unique identification number of the complaint.

Duration of data control: The controller shall retain the minutes recorded about the complaint and a copy of the reply for **5 years** and present it if requested by auditing authorities, based on **Section 17/A(7) of the Fgy tv.**.

Data transmission: The controller shall retain the minutes recorded about the complaint and a copy of the reply for **5 years** and present it if requested by auditing authorities, based on **Section 17/A(7) of the Fgy tv.**.

Data processing technology: manual and automated data processing.

2.10. Other data control

Unless otherwise provided by law, the Hungarian Central Statistical Office (KSH) may receive personal data controlled in the framework of mandatory data control in a manner suitable for individual identification, and may control it in the manner defined by law. Unless otherwise provided by law, personal data recorded, received or processed for statistical purposes may only be controlled for statistical purposes. The detailed rules on control of personal data for statistical purposes are set out in separate law.

The controller will release personal data to authorities only to the extent absolutely necessary for realising the purpose of the inquiry, provided that the authority has indicated the exact purpose and the scope of data.

3. RIGHTS OF DATA SUBJECTS

3.1. Right of access by the data subject

3.1.1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1. the purpose of the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
6. the right to lodge a complaint with a supervisory authority;
7. where the personal data are not collected from the data subject, any available information as to their source;
8. the existence of automated decision-making, including profiling, referred to in **Article 22(1) and (4) of the GDPR** and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to **Article 46 of the GDPR** relating to the transfer.

3.1.2 The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

3.2. Right to rectification

3.2.1. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3.2.2. If the personal data is incorrect and the correct personal data is available to the controller, the controller will rectify the personal data.

3.3. Right to erasure ("right to be forgotten")

3.3.1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2. the data subject withdraws consent on which the processing is based according to **Article 6(1)a)**, or **Article 9(2)a) of the GDPR**, and where there is no other legal ground for the processing;
3. c) the data subject objects to the processing pursuant to **Article 21(1) of the GDPR** and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to **Article 21(2)**;
4. the personal data have been unlawfully processed;
5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
6. the personal data have been collected in relation to the offer of information society services referred to in **Article 8(1) of the GDPR**.

3.3.2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology

and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3.3.3. Sections 3.3.1 and 3.3.2 of the policy shall not apply to the extent that processing is necessary:

1. for exercising the right of freedom of expression and information;
2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
3. for reasons of public interest in the area of public health in accordance with **points (h) and (i) of Article 9(2)** as well as **Article 9(3) of the GDPR**;
4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with **Article 89(1) of the GDPR** in so far as the right referred to in **paragraph 1** is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
5. for the establishment, exercise or defence of legal claims.

3.4. Right to restriction of processing

3.4.1. The data subject shall have the **right to obtain** from the controller **restriction of processing** where one of the following applies:

1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
4. the data subject has objected to processing pursuant to **Article 21(1) of the GDPR** pending the verification whether the legitimate grounds of the controller override those of the data subject

3.4.2. Where processing has been restricted under section 3.4.1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3.4.3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

3.5. Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with **Article 16, Article 17(1)** and **Article 18 of the GDPR** to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

3.6. Right to data portability

3.6.1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

1. the processing is based on consent pursuant to **point (a) of Article 6(1)** or **point (a) of Article 9(2)** or on a contract pursuant to **point (b) of Article 6(1) of the GDPR**; and
2. the processing is carried out by automated means.

3.6.2. In exercising his or her right to data portability pursuant to section 3.6.1, the data subject

shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. The exercise of the right shall be without prejudice **Article 17 of the GDPR**. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right referred to shall not adversely affect the rights and freedoms of others.

3.7. Right to object

3.7.1. The data subject shall have the right **to object**, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on **point (e) or (f) of Article 6(1) of the GDPR**, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

3.7.2. Where personal data are processed for direct marketing purposes, the data subject shall have the right **to object at any time** to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3.7.3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right referred to in sections 3.7.1 and 3.7.2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

3.7.4. In the context of the use of information society services, and notwithstanding **Directive 2002/58/EC**, the data subject may exercise his or her right to object by automated means using technical specifications.

3.7.5. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to **Article 89(1) of the GDPR**, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

3.7.6. The controller will investigate the complaint within the shortest time from the date of submitting the complaint but in no more than 15 days, decide whether it is well-founded, and inform the complainant about its decision in writing.

3.7.7. If the controller finds that the data subject's complaint is well-founded, it will terminate data control - including additional collection and transmission of data - and lock the data, and will notify all parties to whom it has transmitted the personal data affected by the complaint earlier about the complaint and the measures taken on the basis of the complaint, and such parties must take measures to enforce the right to object.

3.7.9. If the data recipient fails to receive the data required for enforcing its rights due to the data subject's objection, it may resort to **court** against the controller within **15 days** of the communication of the notification based on section 3.7.7 - in the manner defined in **Section 22 of the Info Act** -in order to obtain the data. The controller may interplead the data subject as well in the lawsuit.

3.7.10. If the controller fails to give notification according to section 3.7.7, the data recipient may request information from the controller about the circumstances related to the failure of data transmission, and the controller must provide this information **within 8 days** following the receipt of the data recipient's request. In case information is requested, the data recipient may resort to the **court**, contesting the controller, within **15 days** of receiving the information but of the deadline for providing the information at latest. The controller may interplead the data subject as

well in the lawsuit.

3.7.11. The controller may not delete the data subject’s data if data control was ordered by law. However, the data may not be transmitted to the data recipient if the controller agreed with the objection or a court has found that the objection was justified.

3.8. Automated individual decision-making, including profiling

3.8.1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

3.8.2.shall not apply if the decision:

1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;
2. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
3. is based on the data subject's explicit consent.

3.8.3. In the cases referred to in points a) and c) of section 3.8.2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

3.8.4. Decisions referred to in section 3.8.2 shall not be based on special categories of personal data referred to in **Article 9(1) of the GDPR**, unless **point (a) or (g) of Article 9(2)** applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3.9. Communication of a personal data breach to the data subject

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

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

1. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
3. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. REMEDIES

4.1. Right to lodge a complaint with a supervisory authority

4.1.1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

Contact details of the Authority:
National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c, phone: 1/391-1400, e-mail: ugyfelszolgalat@naih.hu)

4.1.2. No person may suffer any detriment on account of having lodged a complaint with the Authority. The Authority may disclose the identity of the complainant only if the investigation could not be conducted without it. If requested by the complainant, the Authority may not disclose the identity of the complainant even if the investigation could not be conducted without it. The Authority must inform the complainant about this consequence.

4.1.3. The Authority's investigation is free of charge, the Authority shall advance and bear the costs of the investigation.

4.1.4. The Authority must inform the client about the developments of the procedure related to the complaint and the result of that procedure, including the fact that based on **Article 78 of the GDPR**, the client may seek legal remedy before the court.

4.2. Right to an effective judicial remedy against a controller or processor

The data subject may resort to the court contesting the controller where the data subject's rights are infringed. The court will proceed in the case on an expedient basis. The data subject may initiate the lawsuit - at his or her discretion - before the court having competence at either the data subject's permanent or temporary place of residence.

4.3. Representation of data subjects

The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights on his or her behalf, and to exercise the right to receive compensation on his or her behalf where provided for by Member State law.

4.4. Right to compensation and liability

4.4.1. Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered.

4.4.2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

4.4.3. Where the controller violates the data subject's personality rights by unlawfully controlling the data subject's data or breaching the requirements of data security, the data subject may claim compensation.

4.4.4. The controller shall be liable for damage caused by the processor vis-a-vis the data subject, and the controller shall pay the compensation due to the data subject in the event of a violation of personality rights caused by the processor as well. The controller shall be released from liability for damage caused and payment of compensation if it proves that the damage or the infringement of the data subject's personality rights was caused by an inevitable reason outside the scope of data control.

4.4.5. No damages shall be paid and no compensation may be claimed to the extent that the damage was caused by the aggrieved party, or the aggrievement caused by infringement of personality rights arose out of the wilful or seriously negligent conduct of the data subject.

4.4.6. The court procedure for enforcing damages or compensation shall be instituted before the court having competence according to the right of the Member State where the controller or processor pursues its activities.

Effective from 2026-06-01