

## DATA PROCESSING NOTICE

---

### Table of contents

Online hearing test .....	2
Customer service, customer support .....	5
Call Center call recording .....	9
Sending marketing inquiries and offers .....	12
Satisfaction survey, questionnaires, customer reviews .....	15

## DATA PROCESSING NOTICE

### Website Online hearing test

**Effective date: 15/10/2025**

In accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and Regulation (**Info Act**) (EU) 2016/679 of the European Parliament and of the Council 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 - General Data Protection Regulation**), we hereby inform you about the processing of the personal data you have provided:

### 1. Controller

Name of the Controller		Victofon Hallásjavító Kft.
Address of the Controller		1068 Budapest, Szondi u. 98/a. fszt. 2.
Contact details of the Controller	email	ugyfelszolgalat@victofon.hu
	telephone	+ 06 30 311 4123
	website	<a href="https://victofon.hu/hu">https://victofon.hu/hu</a>
Name of data protection officer (if any)		-
Contact details of the Data Protection Officer		-

### 2. The data processed

#### Scope of the data processed, purpose and legal basis for processing

Personal data	Purpose of data processing	Legal ground of processing	Data processing (storage) duration
Surname, first name Email address Telephone number Zip code Date of birth Hearing test, results of the assessment The results of the hearing test is special, health-related data, pursuant to Article 9 of the GDPR. By submitting the form, the data subject expressly consents to the processing and storage of this data.  You can find more information in the data processing notice for Customers.	Providing, evaluating, sending an online hearing test, and contacting the interested party	Consent of the data subject - Article 6(1)(a) GDPR	Until the consent is withdrawn, but for a maximum of 7 years, unless there is another legal basis supporting the data processing. You can withdraw your consent by writing to the following e-mail address: <a href="mailto:ugyfelszolgalat@victofon.hu">ugyfelszolgalat@victofon.hu</a> or via the other known contact details.  If consent is refused, the data subject will not be able to submit the online hearing test.

#### Related legislation

-

#### Does the processing involve profiling?

Answer	Short, clear description of profiling
No	---

#### Does the processing involve automated decision-making?

Answer	Short, clear description of the automatism
No	---

If so, the Data Subject has the right to request manual, human intervention.

**The source of the personal data processed:**

The data subject
------------------

**The data will be transmitted:**

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	Total Studio Kft. 2096 Üröm, Asztalos utca 14/B. Website development, website support, operation, MiniCRM Zrt. 1075 Budapest, Madách Imre út 13-14. MiniCRM - CRM system operator,
Recipients	

**Data is transferred to a third country (outside the EU):**

Name of data processor, place of transfer, guarantees of transfer, reason for transfer

**Joint processing takes place:**

Answer	Name and registered seat of the joint controller
No	

**Access to data and data security measures:**

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their work duties, typically the sales, customer service and audiology staff. The company ensures this through authorization management.
Data security measure	HTTP security protocol on the website Antivirus software on computers, regular backups of data stored on the server Computers are password protected Password protected Wi-Fi network The network is protected by a firewall Changing passwords at regular intervals is mandatory Uninterruptible power supply is provided for the company's servers and critical workstations Authorization management and its regular review Password protection of applications and software Two-factor authentication for logging into certain software

**3. Rights of the Data Subject:**

Rights of data subjects relating to the legal basis and an explanation of these rights
Right to information: The Data Subject has the right to be informed about the way in which personal data are processed before the processing starts Right of rectification: The Data Subject has the right to request the rectification of his or her personal data if the personal data held by the Controller are inaccurate and he or she can prove this Right of access: The Data Subject has the right to obtain from the Controller the personal data held about him or her Right to erasure, right to be forgotten: The Data Subject has the right to obtain the permanent erasure of his or her data, unless the processing is based on the performance of a contract, the fulfilment of a legal obligation or the exercise of official authority Withdrawal of consent: Where processing is based on consent, the Data Subject may withdraw his or her previously given consent at any time. Acceptance of a withdrawal request may also imply erasure of the data, but where there is another legal basis supporting the processing, the processing will cease only in relation to the specific purpose of the processing Right to restriction: If the Data Subject does not consider the Controller to be entitled to process his or her personal data, he or she may request the suspension of the processing during the investigation The right to data portability: The Data Subject has the right to request the personal data stored about him or her in digital, tabular form

Right to review of automated decision-making: The Data Subject has the right to request a manual review of any processing operation where the controller has used automated decision-making with legal effect on the Data Subject

#### 4. Exercise of data subject rights

Where the data subject has made a request to the controller in relation to the exercise of his or her rights as described in point 3, the controller shall respond without undue delay, but no later than one month from the receipt of the request, and inform the data subject of the action taken on the request. If necessary, this period may be extended by a further two months.

If the Controller fails to act on the data subject's request, the Controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the supervisory authority and to seek judicial redress.

#### 5. Lodging a complaint

The data subject has the right to lodge a complaint with the data protection authority:

<b>Name</b>	National Authority for Data Protection and Freedom of Information (NAIH)
<b>Seat</b>	H-1055 Budapest, Falk Miksa utca 9-11.
<b>Postal address</b>	1363 Budapest, Pf.9.
<b>Email</b>	<a href="mailto:ugyfelszolgalat@naih.hu">ugyfelszolgalat@naih.hu</a>
<b>Phone</b>	+36 (1) 391-1400
<b>Fax</b>	+36 (1) 391-1410
<b>Website</b>	<a href="http://naih.hu">http://naih.hu</a>

#### 6. Judicial redress

The provisions on judicial redress are in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

The data subject may go to court against the controller in order to protect his or her data if he or she considers that the controller has infringed the provisions on the processing of personal data. The data subject may choose to bring the action before the tribunal having jurisdiction over the place where he or she lives or resides. A person who does not otherwise have legal ability in the lawsuit may also be a party to the lawsuit. The data protection authority may intervene in the lawsuit in order to ensure that the data subject is successful.

Any person who has suffered pecuniary or non-pecuniary damage as a result of a breach of the General Data Protection Regulation shall be entitled to receive compensation from the controller or processor for the damage suffered. The 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.

## DATA PROCESSING NOTICE

### Customer data management Customer service, customer support

**Effective date: 15/10/2025**

In accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and Regulation (Info Act) (EU) 2016/679 of the European Parliament and of the Council 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 - General Data Protection Regulation), we hereby inform you about the processing of the personal data you have provided:

#### 1. Controller

Name of the Controller		Victofon Hallásjavító Kft.
Address of the Controller		1068 Budapest, Szondi u. 98/a. fszt. 2.
Contact details of the Controller	email	ugyfelszolgalat@victofon.hu
	telephone	+ 06 30 311 4123
	website	<a href="https://victofon.hu/hu">https://victofon.hu/hu</a>
Name of data protection officer (if any)		-
Contact details of the Data Protection Officer		-

#### 2. The data processed

##### Scope of the data processed, purpose and legal basis for processing

Personal data	Purpose of data processing	Legal ground of processing	Data processing (storage) duration
Name Email address Telephone number Zip code Social security number Place and date of birth Answers to questions about hearing quality, hearing aid data  Personal data provided by the data subject - all personal data provided by the data subject, personal data included in any attached documents Personal data recorded in a note or free-text description Special personal health data is also processed under Article 9 of the GDPR.	Visiting people applying for hearing tests and those interested in the service, sending thank-you letters, managing forms, making contact, status assessment, assessing needs, pre-screening, collecting and recording personal data necessary for the service Providing services, keeping contact, scheduling appointments, sending reminder emails, text messages, making calls Storage of declarations Visiting the patient before the end of the support period and service life, contacting the patient for annual hearing tests and control examinations	Necessary for the performance of a contract - GDPR Article 6(1) paragraph (b)	The data is retained for 10 years after inquiry, unless there is another legal basis to support the processing. If the data are part of a medical record, the relevant retention period will apply. If the document cannot be disposed of according to the archiving and disposal regulations, the personal data contained therein will not be deleted.

##### Related legislation

**Does the processing involve profiling?**

Answer	Short, clear description of profiling
No	---

**Does the processing involve automated decision-making?**

Answer	Short, clear description of the automatism
No	---

*If so, the Data Subject has the right to request manual, human intervention.*

**The source of the personal data processed:**

The data subject
------------------

**The data will be transmitted:**

Category	Company name, registered seat, activity
<i>Processors (performing technical tasks related to data processing operations)</i>	Dunaelektronika Kft. 1183 Budapest Gyömrői út 99. External system administrator, IT service provider, Magyar Telekom Nyrt. 1097 Budapest Könyves Kálmán krt. 34-36 Telecommunications service provider(s), Google Inc 3rd Floor Gordon House, D04 E5W5 Barrow Street, Dublin, Ireland Mail system, Google workspace, Google services, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Mailing system, MiniCRM Zrt. 1075 Budapest, Madách Imre út 13-14. MiniCRM - CRM system operator, HRP Europe Kft. 1033 Budapest, Huszti út 34. ERP system operator, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Microsoft Dynamics NAV (formerly Navision) ERP system
<i>Recipients</i>	

**Data is transferred to a third country (outside the EU):**

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Google Inc,USA,Privacy Policy Data Privacy Framework, <a href="https://policies.google.com/privacy?hl=hu&amp;fg=2">https://policies.google.com/privacy?hl=hu&amp;fg=2</a> ,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework, <a href="https://privacy.microsoft.com/hu-hu/privacystatement">https://privacy.microsoft.com/hu-hu/privacystatement</a> ,  <a href="https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA">https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA</a> <a href="https://www.dataprivacyframework.gov/list">https://www.dataprivacyframework.gov/list</a> ,possible access by parent company, data storage,

**Joint processing takes place:**

Answer	Name and registered seat of the joint controller
No	

**Access to data and data security measures:**

<b>Restricting access</b>	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, customer service, customer management staff, managers, CRM admin staff, Call Center staff, and, where applicable, management may access the data. The enterprise ensures this through authorization management.
<b>Data security measure</b>	Alarm, Unauthorized person cannot enter the office Key management - rights management Closed document storage, closed archive Security camera system Safe deposit box Antivirus software on computers, regular backups of data stored on the server Computers are password protected Password protected Wi-Fi network The network is protected by a firewall Changing passwords at regular intervals is mandatory

	Uninterruptible power supply is provided for the company's servers and critical workstations Authorization management and its regular review Private use of IT equipment is prohibited Employee confidentiality agreement signed or confidentiality is secured by relevant legislation. It is mandatory to turn off the screen when the employee leaves their workstation Employees must immediately report the loss or damage of IT devices and data carriers to their superior or a designated person It is mandatory to keep documents that are not in use during work in a locked place. Password protection of applications and software Two-factor authentication for logging into certain software
--	---

### 3. Rights of the Data Subject:

Rights of data subjects relating to the legal basis and an explanation of these rights	
Right to information:	The Data Subject has the right to be informed about the way in which personal data are processed before the processing starts
Right of rectification:	The Data Subject has the right to request the rectification of his or her personal data if the personal data held by the Controller are inaccurate and he or she can prove this
Right of access:	The Data Subject has the right to obtain from the Controller the personal data held about him or her
The right to data portability:	The Data Subject has the right to request the personal data stored about him or her in digital, tabular form
Right to review of automated decision-making:	The Data Subject has the right to request a manual review of any processing operation where the controller has used automated decision-making with legal implication on the Data Subject.

### 4. Exercise of data subject rights

Where the data subject has made a request to the controller in relation to the exercise of his or her rights as described in point 3, the controller shall respond without undue delay, but no later than one month from the receipt of the request, and inform the data subject of the action taken on the request. If necessary, this period may be extended by a further two months.

If the Controller fails to act on the data subject's request, the Controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the supervisory authority and to seek judicial redress.

### 5. Lodging a complaint

The data subject has the right to lodge a complaint with the data protection authority:

<b>Name</b>	National Authority for Data Protection and Freedom of Information (NAIH)
<b>Seat</b>	H-1055 Budapest, Falk Miksa utca 9-11.
<b>Postal address</b>	1363 Budapest, Pf.9.
<b>Email</b>	<a href="mailto:ugyfelszolgalat@naih.hu">ugyfelszolgalat@naih.hu</a>
<b>Phone</b>	+36 (1) 391-1400
<b>Fax</b>	+36 (1) 391-1410
<b>Website</b>	<a href="http://naih.hu">http://naih.hu</a>

### 6. Judicial redress

The provisions on judicial redress are in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

Victofon Hallásjavító Kft. 1068 Budapest, Szondi u. 98/a. fszt.2.  
e-mail: [ugyfelszolgalat@victofon.hu](mailto:ugyfelszolgalat@victofon.hu)  
website: <https://victofon.hu/hu>  
telephone: +36 30 311 4123



The data subject may go to court against the controller in order to protect his or her data if he or she considers that the controller has infringed the provisions on the processing of personal data. The data subject may choose to bring the action before the tribunal having jurisdiction over the place where he or she lives or resides. A person who does not otherwise have legal ability in the lawsuit may also be a party to the lawsuit. The data protection authority may intervene in the lawsuit in order to ensure that the data subject is successful.

Any person who has suffered pecuniary or non-pecuniary damage as a result of a breach of the General Data Protection Regulation shall be entitled to receive compensation from the controller or processor for the damage suffered. The 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.

**By contacting us, the data subject declares that he/she has read the Data Processing Notice related to Customer Service and Customer Support, and consents to the processing and storage of his/her provided data in accordance with the information contained in the notice.**



## DATA PROCESSING NOTICE

### Customer data management Call Center call recording

**Effective date: 15/10/2025**

In accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and Regulation (Info Act) (EU) 2016/679 of the European Parliament and of the Council 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 - General Data Protection Regulation), we hereby inform you about the processing of the personal data you have provided:

#### 1. Controller

Name of the Controller		Victofon Hallásjavító Kft.
Address of the Controller		1068 Budapest, Szondi u. 98/a. fszt. 2.
Contact details of the Controller	email	ugyfelszolgalat@victofon.hu
	telephone	+ 06 30 311 4123
	website	<a href="https://victofon.hu/hu">https://victofon.hu/hu</a>
Name of data protection officer (if any)		-
Contact details of the Data Protection Officer		-

#### 2. The data processed

##### Scope of the data processed, purpose and legal basis for processing

Personal data	Purpose of data processing	Legal ground of processing	Data processing (storage) duration
Name Telephone number The recording of the telephone call and the personal data provided by the data subject during the telephone call Special personal health data is also processed under Article 9 of the GDPR.	Recording and storing incoming and outgoing calls for patient rights and consumer protection purposes, complaint handling and for quality assurance.	Legitimate interest - Article 6(1)(f) GDPR	5 years

##### Related legislation

--

##### Does the processing involve profiling?

Answer	Short, clear description of profiling
No	---

##### Does the processing involve automated decision-making?

Answer	Short, clear description of the automatism
No	---

*If so, the Data Subject has the right to request manual, human intervention.*

##### The source of the personal data processed:

The data subject

**The data will be transmitted:**

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	Magyar Telekom Nyrt. 1097 Budapest Könyves Kálmán krt. 34-36 Telecommunications service provider(s), Opennetworks Kft. 1125 Budapest, Kiss Áron utca 9. Telephone center operator
Recipients	

**Data is transferred to a third country (outside the EU):**

Name of data processor, place of transfer, guarantees of transfer, reason for transfer

**Joint processing takes place:**

Answer	Name and registered seat of the joint controller
No	

**Access to data and data security measures:**

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, customer service, customer management staff, managers, CRM admin staff, Call Center staff, and, where applicable, management may access the data. The enterprise ensures this through authorization management.
Data security measure	Alarm, Unauthorized person cannot enter the office Key management - rights management Closed document storage, closed archive Security camera system Safe deposit box Antivirus software on computers, regular backups of data stored on the server Computers are password protected Password protected Wi-Fi network The network is protected by a firewall Changing passwords at regular intervals is mandatory Uninterruptible power supply is provided for the company's servers and critical workstations Authorization management and its regular review Private use of IT equipment is prohibited Employee confidentiality agreement signed or confidentiality is secured by relevant legislation. It is mandatory to turn off the screen when the employee leaves their workstation Employees must immediately report the loss or damage of IT devices and data carriers to their superior or a designated person It is mandatory to keep documents that are not in use during work in a locked place. Password protection of applications and software Two-factor authentication for logging into certain software

**3. Rights of the Data Subject:**

Rights of data subjects relating to the legal basis and an explanation of these rights
Right to information: The Data Subject has the right to be informed about the way in which personal data are processed before the processing starts Right of rectification: The Data Subject has the right to request the rectification of his or her personal data if the personal data held by the Controller are inaccurate and he or she can prove this Right of access: The Data Subject has the right to obtain from the Controller the personal data held about him or her

Right to object: If the legal basis is on the grounds of legitimate interest or public authority, the data subject may object to the processing of his or her personal data, but the objection does not imply the immediate erasure of his or her data  
Right to restriction: If the Data Subject does not consider the Controller to be entitled to process his or her personal data, he or she may request the suspension of the processing during the investigation  
The right to data portability: The Data Subject has the right to request the personal data stored about him or her in digital, tabular form  
Right to review of automated decision-making: The Data Subject has the right to request a manual review of any processing operation where the controller has used automated decision-making with legal implication on the Data Subject.

#### 4. Exercise of data subject rights

Where the data subject has made a request to the controller in relation to the exercise of his or her rights as described in point 3, the controller shall respond without undue delay, but no later than one month from the receipt of the request, and inform the data subject of the action taken on the request. If necessary, this period may be extended by a further two months.

If the Controller fails to act on the data subject's request, the Controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the supervisory authority and to seek judicial redress.

#### 5. Lodging a complaint

The data subject has the right to lodge a complaint with the data protection authority:

<b>Name</b>	National Authority for Data Protection and Freedom of Information (NAIH)
<b>Seat</b>	H-1055 Budapest, Falk Miksa utca 9-11.
<b>Postal address</b>	1363 Budapest, Pf.9.
<b>Email</b>	<a href="mailto:ugyfelszolgalat@naih.hu">ugyfelszolgalat@naih.hu</a>
<b>Phone</b>	+36 (1) 391-1400
<b>Fax</b>	+36 (1) 391-1410
<b>Website</b>	<a href="http://naih.hu">http://naih.hu</a>

#### 6. Judicial redress

The provisions on judicial redress are in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

The data subject may go to court against the controller in order to protect his or her data if he or she considers that the controller has infringed the provisions on the processing of personal data. The data subject may choose to bring the action before the tribunal having jurisdiction over the place where he or she lives or resides. A person who does not otherwise have legal ability in the lawsuit may also be a party to the lawsuit. The data protection authority may intervene in the lawsuit in order to ensure that the data subject is successful.

Any person who has suffered pecuniary or non-pecuniary damage as a result of a breach of the General Data Protection Regulation shall be entitled to receive compensation from the controller or processor for the damage suffered. The 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.

**By making the phone call, the data subject declares that he or she has read the Data Processing Notice related to Call Center call recording, and consents to the processing and storage of his or her data as set out in the notice.**

## DATA PROCESSING NOTICE

### Customer data management Sending marketing inquiries and offers

**Effective date: 15/10/2025**

In accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and Regulation (Info Act) (EU) 2016/679 of the European Parliament and of the Council 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 - General Data Protection Regulation), we hereby inform you about the processing of the personal data you have provided:

#### 1. Controller

Name of the Controller		Victofon Hallásjavító Kft.
Address of the Controller		1068 Budapest, Szondi u. 98/a. fszt. 2.
Contact details of the Controller	email	ugyfelszolgalat@victofon.hu
	telephone	+ 06 30 311 4123
	website	<a href="https://victofon.hu/hu">https://victofon.hu/hu</a>
Name of data protection officer (if any)		-
Contact details of the Data Protection Officer		-

#### 2. The data processed

##### Scope of the data processed, purpose and legal basis for processing

Personal data	Purpose of data processing	Legal ground of processing	Data processing (storage) duration
Name Email address Telephone number Address Information related to the inquiry, the first contact, previous examinations, services used, orders, which may contain personal data, additional personal data provided by the inquiring party/customer	Direct marketing-type inquiries not considered newsletters for the purpose of direct business acquisition to those interested in the service, sending offers - by phone, e-mail, or by post	Legitimate interest - Article 6(1)(f) GDPR	7 years after establishing contact. In the event of an objection, the data will be deleted unless there is another legal basis supporting the data processing.

##### Related legislation

--

##### Does the processing involve profiling?

Answer	Short, clear description of profiling
No	---

##### Does the processing involve automated decision-making?

Answer	Short, clear description of the automatism
No	---

*If so, the Data Subject has the right to request manual, human intervention.*

#### The source of the personal data processed:

The data subject  
Marketing VF Ltd (MVF)  
Bloom Media Group

#### The data will be transmitted:

Category	Company name, registered seat, activity
<i>Processors (performing technical tasks related to data processing operations)</i>	Dunaelektronika Kft. 1183 Budapest Gyömrői út 99. External system administrator, IT service provider, Magyar Telekom Nyrt. 1097 Budapest Könyves Kálmán krt. 34-36 Telecommunications service provider(s), Google Inc 3rd Floor Gordon House, D04 E5W5 Barrow Street, Dublin, Ireland Mail system, Google workspace, Google services, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Mailing system, Google Inc 3rd Floor Gordon House, D04 E5W5 Barrow Street, Dublin, Ireland Other Google products for marketing purposes, MiniCRM Zrt. 1075 Budapest, Madách Imre út 13-14. MiniCRM - CRM system operator,
<i>Recipients</i>	

#### Data is transferred to a third country (outside the EU):

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Google Inc,USA,Privacy Policy Data Privacy Framework, <a href="https://policies.google.com/privacy?hl=hu&amp;fg=2">https://policies.google.com/privacy?hl=hu&amp;fg=2</a> ,possible access by parent company, data storage, Google Inc,USA,Privacy Policy Data Privacy Framework, <a href="https://policies.google.com/privacy?hl=hu&amp;fg=2">https://policies.google.com/privacy?hl=hu&amp;fg=2</a> ,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework, <a href="https://privacy.microsoft.com/hu-hu/privacystatement">https://privacy.microsoft.com/hu-hu/privacystatement</a> , <a href="https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA">https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA</a> <a href="https://www.dataprivacyframework.gov/list">https://www.dataprivacyframework.gov/list</a> ,possible access by parent company, data storage,

#### Joint processing takes place:

Answer	Name and registered seat of the joint controller
No	

#### Access to data and data security measures:

<b>Restricting access</b>	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, marketing staff, sales staff, CRM admin staff, and Call Center staff can access the data. The enterprise ensures this through authorization management.
<b>Data security measure</b>	Alarm, Unauthorized person cannot enter the office Key management - rights management Closed document storage, closed archive Security camera system Safe deposit box Antivirus software on computers, regular backups of data stored on the server Computers are password protected Password protected Wi-Fi network The network is protected by a firewall Changing passwords at regular intervals is mandatory Uninterruptible power supply is provided for the company's servers and critical workstations Authorization management and its regular review Private use of IT equipment is prohibited Employee confidentiality agreement signed It is mandatory to turn off the screen when the employee leaves their workstation Employees must immediately report the loss or damage of IT devices and data carriers to their superior or a designated person

	It is mandatory to keep documents that are not in use during work in a locked place. Password protection of applications and software Two-factor authentication for logging into certain software
--	---

### 3. Rights of the Data Subject:

<b>Rights of data subjects relating to the legal basis and an explanation of these rights</b>
Right to information: The Data Subject has the right to be informed about the way in which personal data are processed before the processing starts
Right of rectification: The Data Subject has the right to request the rectification of his or her personal data if the personal data held by the Controller are inaccurate and he or she can prove this
Right of access: The Data Subject has the right to obtain from the Controller the personal data held about him or her
Right to object: If the legal basis is on the grounds of legitimate interest or public authority, the data subject may object to the processing of his or her personal data, but the objection does not imply the immediate erasure of his or her data
Right to restriction: If the Data Subject does not consider the Controller to be entitled to process his or her personal data, he or she may request the suspension of the processing during the investigation
The right to data portability: The Data Subject has the right to request the personal data stored about him or her in digital, tabular form
Right to review of automated decision-making: The Data Subject has the right to request a manual review of any processing operation where the controller has used automated decision-making with legal implication on the Data Subject.

### 4. Exercise of data subject rights

Where the data subject has made a request to the controller in relation to the exercise of his or her rights as described in point 3, the controller shall respond without undue delay, but no later than one month from the receipt of the request, and inform the data subject of the action taken on the request. If necessary, this period may be extended by a further two months.

If the Controller fails to act on the data subject's request, the Controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the supervisory authority and to seek judicial redress.

### 5. Lodging a complaint

The data subject has the right to lodge a complaint with the data protection authority:

<b>Name</b>	National Authority for Data Protection and Freedom of Information (NAIH)
<b>Seat</b>	H-1055 Budapest, Falk Miksa utca 9-11.
<b>Postal address</b>	1363 Budapest, Pf.9.
<b>Email</b>	<a href="mailto:ugyfelszolgalat@naih.hu">ugyfelszolgalat@naih.hu</a>
<b>Phone</b>	+36 (1) 391-1400
<b>Fax</b>	+36 (1) 391-1410
<b>Website</b>	<a href="http://naih.hu">http://naih.hu</a>

### 6. Judicial redress

The provisions on judicial redress are in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

The data subject may go to court against the controller in order to protect his or her data if he or she considers that the controller has infringed the provisions on the processing of personal data. The data subject may choose to bring the action before the tribunal having jurisdiction over the place where he or she lives or resides. A person who does not otherwise have legal ability in the lawsuit may also be a party to the lawsuit. The data protection authority may intervene in the lawsuit in order to ensure that the data subject is successful.

## DATA PROCESSING NOTICE

### Customer data management Satisfaction survey, questionnaires, customer reviews

**Effective date: 15/10/2025**

In accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and Regulation (Info Act) (EU) 2016/679 of the European Parliament and of the Council 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 - General Data Protection Regulation), we hereby inform you about the processing of the personal data you have provided:

#### 1. Controller

Name of the Controller		Victofon Hallásjavító Kft.
Address of the Controller		1068 Budapest, Szondi u. 98/a. fszt. 2.
Contact details of the Controller	email	ugyfelszolgalat@victofon.hu
	telephone	+ 06 30 311 4123
	website	<a href="https://victofon.hu/hu">https://victofon.hu/hu</a>
Name of data protection officer (if any)		-
Contact details of the Data Protection Officer		-

#### 2. The data processed

##### Scope of the data processed, purpose and legal basis for processing

Personal data	Purpose of data processing	Legal ground of processing	Data processing (storage) duration
Name Email address - to send the survey The answers given in the questionnaire and the conclusions that can be drawn from them The questionnaire is anonymous in some cases, but the data provided may indirectly identify the data subject.	Customer satisfaction survey on paper, via form, by email and, if applicable, by phone, contacting the data subject after both successful and unsuccessful sales, asking questions for the purpose of improving services, improving customer service, quality assurance goals	Legitimate interest - Article 6(1)(f) GDPR	For 10 years

##### Related legislation

--

##### Does the processing involve profiling?

Answer	Short, clear description of profiling
No	---

##### Does the processing involve automated decision-making?

Answer	Short, clear description of the automatism
No	---

*If so, the Data Subject has the right to request manual, human intervention.*

##### The source of the personal data processed:

The data subject



Victofon Hallásjavító Kft. 1068 Budapest, Szondi u. 98/a. fszt.2.  
e-mail: [ugyfelszolgalat@victofon.hu](mailto:ugyfelszolgalat@victofon.hu)  
website: <https://victofon.hu/hu>  
telephone: +36 30 311 4123



**The data will be transmitted:**

Category	Company name, registered seat, activity
<i>Processors (performing technical tasks related to data processing operations)</i>	Dunaelektronika Kft. 1183 Budapest Gyömrői út 99. External system administrator, IT service provider, Magyar Telekom Nyrt. 1097 Budapest Könyves Kálmán krt. 34-36 Telecommunications service provider(s), Google Inc 3rd Floor Gordon House, D04 E5W5 Barrow Street, Dublin, Ireland Google Forms - satisfaction survey Google Inc 3rd Floor Gordon House, D04 E5W5 Barrow Street, Dublin, Ireland Mail system, Google workspace, Google services, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Mailing system, MiniCRM Zrt. 1075 Budapest, Madách Imre út 13-14. MiniCRM - CRM system operator,
<i>Recipients</i>	

**Data is transferred to a third country (outside the EU):**

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Google Inc,USA,Privacy Policy Data Privacy Framework, <a href="https://policies.google.com/privacy?hl=hu&amp;fg=2">https://policies.google.com/privacy?hl=hu&amp;fg=2</a> ,possible access by parent company, data storage, Google Inc,USA,Privacy Policy Data Privacy Framework, <a href="https://policies.google.com/privacy?hl=hu&amp;fg=2">https://policies.google.com/privacy?hl=hu&amp;fg=2</a> ,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework, <a href="https://privacy.microsoft.com/hu-hu/privacystatement">https://privacy.microsoft.com/hu-hu/privacystatement</a> , <a href="https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA">https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA</a> <a href="https://www.dataprivacyframework.gov/list">https://www.dataprivacyframework.gov/list</a> ,possible access by parent company, data storage,

**Joint processing takes place:**

Answer	Name and registered seat of the joint controller
No	

**Access to data and data security measures:**

<b>Restricting access</b>	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, marketing staff, sales staff, quality assurance staff, CRM admin staff, and Call Center staff can access the data. The enterprise ensures this through authorization management.
<b>Data security measure</b>	Alarm, Unauthorized person cannot enter the office Key management - rights management Closed document storage, closed archive Security camera system Safe deposit box Antivirus software on computers, regular backups of data stored on the server Computers are password protected Password protected Wi-Fi network The network is protected by a firewall Changing passwords at regular intervals is mandatory Uninterruptible power supply is provided for the company's servers and critical workstations Authorization management and its regular review Private use of IT equipment is prohibited Employee confidentiality agreement signed It is mandatory to turn off the screen when the employee leaves their workstation Employees must immediately report the loss or damage of IT devices and data carriers to their superior or a designated person It is mandatory to keep documents that are not in use during work in a locked place. Password protection of applications and software Two-factor authentication for logging into certain software



### 3. Rights of the Data Subject:

Rights of data subjects relating to the legal basis and an explanation of these rights	
Right to information:	The Data Subject has the right to be informed about the way in which personal data are processed before the processing starts
Right of rectification:	The Data Subject has the right to request the rectification of his or her personal data if the personal data held by the Controller are inaccurate and he or she can prove this
Right of access:	The Data Subject has the right to obtain from the Controller the personal data held about him or her
Right to object:	If the legal basis is on the grounds of legitimate interest or public authority, the data subject may object to the processing of his or her personal data, but the objection does not imply the immediate erasure of his or her data
Right to restriction:	If the Data Subject does not consider the Controller to be entitled to process his or her personal data, he or she may request the suspension of the processing during the investigation
The right to data portability:	The Data Subject has the right to request the personal data stored about him or her in digital, tabular form
Right to review of automated decision-making:	The Data Subject has the right to request a manual review of any processing operation where the controller has used automated decision-making with legal implication on the Data Subject.

### 4. Exercise of data subject rights

Where the data subject has made a request to the controller in relation to the exercise of his or her rights as described in point 3, the controller shall respond without undue delay, but no later than one month from the receipt of the request, and inform the data subject of the action taken on the request. If necessary, this period may be extended by a further two months.

If the Controller fails to act on the data subject's request, the Controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the supervisory authority and to seek judicial redress.

### 5. Lodging a complaint

The data subject has the right to lodge a complaint with the data protection authority:

<b>Name</b>	National Authority for Data Protection and Freedom of Information (NAIH)
<b>Seat</b>	H-1055 Budapest, Falk Miksa utca 9-11.
<b>Postal address</b>	1363 Budapest, Pf.9.
<b>Email</b>	<a href="mailto:ugyfelszolgalat@naih.hu">ugyfelszolgalat@naih.hu</a>
<b>Phone</b>	+36 (1) 391-1400
<b>Fax</b>	+36 (1) 391-1410
<b>Website</b>	<a href="http://naih.hu">http://naih.hu</a>

### 6. Judicial redress

The provisions on judicial redress are in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

The data subject may go to court against the controller in order to protect his or her data if he or she considers that the controller has infringed the provisions on the processing of personal data. The data subject may choose to bring the action before the tribunal having jurisdiction over the place where he or she lives or resides. A person who does not otherwise have legal ability in the lawsuit may also be a party to the lawsuit. The data protection authority may intervene in the lawsuit in order to ensure that the data subject is successful.