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

DATA PROCESSING NOTICE

Customer data management

Table of contents

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

DATA PROCESSING NOTICE

Customer data management
General contact

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	https://victofon.hu/hu
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 Personal data provided by the data subject Special personal health data - may also be processed under Article 9 of the GDPR.	Handling inquiries received by telephone, e-mail, in person or otherwise from persons interested in the services, other interested parties or contact persons: responding, keeping contact, providing information, scheduling appointments. Forwarding the inquiry to the competent area or person.	Consent of the data subject - Article 6(1)(a) GDPR	10 years from the inquiry, but no later than until the consent is withdrawn, unless there is another legal basis supporting the data processing. You can withdraw your consent by writing to the following e-mail address: ugyfelszolgalat@victofon.hu Consequences of refusing consent: without consent, contact will be difficult or impossible. If the document cannot be disposed of according to the archiving and disposal regulations, the personal data contained therein will not be deleted. 3

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)	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), Opennetworks Kft. 1125 Budapest, Kiss Áron utca 9. Telephone center operator, 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, Meta Platforms Ireland Limited 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland Facebook, Instagram social media, 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
Recipients	

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Meta Platforms Ireland Limited,USA,Privacy Policy Data Privacy Framework,https://hu-hu.facebook.com/privacy/policy https://www.dataprivacyframework.gov/list,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

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 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:

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

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 contacting us, the data subject declares that he or she has read the Data Processing Notice for General Contact, and consents to the processing and storage of his or her data as set out in the notice.

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

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	https://victofon.hu/hu
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:

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

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.

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

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	https://victofon.hu/hu
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
Processors (performing technical tasks related to data processing operations)	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
Recipients	

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

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 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:

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

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 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.

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

DATA PROCESSING NOTICE

Customer data management
Processing hearing test data

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	https://victofon.hu/hu
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 Social security number Address Place and date of birth Email address Telephone number Audiograms Content of the prescription All health data related to the examination, data included in the outpatient form, final report, data regarding the patient's current and historical health status, additional data provided by the patient, data included in the hearing aid booklet Public medical assistance certificate number - if applicable Special personal health data is also processed under Article 9 of the GDPR.	Provision of healthcare services, verification of eligibility, outpatient specialist consulting, specialist examinations, conducting hearing tests, needs assessment, storing, transferring or sending healthcare documentation by email Storage of declarations	Necessary for the performance of a contract or fulfilment of a legal obligation - GDPR Article 6(1) paragraph (b) and (c)	The controller retains the health documentation for 30 years from the date of data collection. 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
Act CLIV of 1997 on Healthcare Act XLVII of 1997 on the Processing and Protecting of Medical and other Related Personal Data;

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)	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, Cloudent Kft. 1027 Budapest, Tölgyfa u. 28 Cloudent medical software
Recipients	

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically healthcare workers, audiology department staff, CRM admin staff, and Call Center staff. 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 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:

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

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.

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

Customer data management
Data processing relating to trial period

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	https://victofon.hu/hu
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 Social security number Certificate no. Data concerning hearing aids and accessories Duration of trial period Fees Reason for rejection - if applicable Special personal health data is also processed under Article 9 of the GDPR.	Trial administration, conclusion of trial agreement, keeping contact	Necessary for the performance of a contract - GDPR Article 6(1) paragraph (b)	The controller retains the health documentation for 30 years from the date of data collection.

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)	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, Cloudent Kft. 1027 Budapest, Tölgyfa u. 28 Cloudent medical software
Recipients	

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically healthcare workers, audiology department staff, CRM admin staff, and Call Center staff. 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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Hearing Aids

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	https://victofon.hu/hu
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 Social security number Address Place and date of birth Email address Telephone number Content of the prescription Special personal health data is also processed under Article 9 of the GDPR.	Management of the distribution of medical aids, sales of hearing aids and accessories - provision of the appropriate hearing aid, sales, adjustment and maintenance of the device Keeping contact, scheduling appointments, sending notifications for check-ups, sending device-related information and notifications	Necessary for the performance of a contract - GDPR Article 6(1) paragraph (b)	The controller retains the health documentation for 30 years from the date of data collection. 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
Processors (performing technical tasks related to data processing operations)	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, Operators of hearing aid adjustment programs, hearing aid fitting software, and other software, Cyfex AG Schwamendingenstrasse 10 8050 Zurich Switzerland Cyfex modeling software, Autodesk Netfabb 111 McInnis Pkwy, San Rafael, California 94903, US. 3 D scanning software, 3 D printing software, Cloudent Kft. 1027 Budapest, Tölgyfa u. 28 Cloudent medical software Audiosoft IT-Consulting Kft. 1013 Budapest, Pauler u. 15. AVOIR software medical aids, MED-EL Elektromedizinische Geräte Gesellschaft m.b.H. Fürstenweg 77a, 6020 Innsbruck, Austria Otoplan healthcare software
Recipients	

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,possible access by parent company, data storage, Cyfex AG, Switzerland, Swiss Conformity Decision - 2000/518/EC Privacy Policy, https://Www.cyfex.com/en/privacy,data storage, Autodesk Netfabb,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://www.autodesk.com/company/legal-notices-trademarks/privacy-statement#storage,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, healthcare workers, audiology department staff, sales staff, CRM admin staff, Call Center staff, and management can 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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Hearing implants

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	https://victofon.hu/hu
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 Social security number Telephone number Email address Address Place and date of birth Mother's name Date of surgery Hearing test results Specialist's medical report Diagnosis, CT, MRI scan results All health data related to the examination, data included in the outpatient form, final report, data regarding the patient's current and historical health status, additional data provided by the patient, additional personal data provided by partners, if any. Special personal health data is also processed under Article 9 of the GDPR.	Carrying out activities related to the distribution of hearing aids, visiting the person concerned, managing and forwarding health documentation, keeping contact, forwarding data to partners, purchasing and selling implants Keeping contact, scheduling appointments	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. The controller retains the health documentation for 30 years from the date of data collection. 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 Collaborating healthcare institution - Partner hospitals Manufacturing partner - MED-EL

The data will be transmitted:

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	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, Cloudent Kft. 1027 Budapest, Tölgyfa u. 28 Cloudent medical software Audiosoft IT-Consulting Kft. 1013 Budapest, Pauler u. 15. AVOIR software medical aids, MED-EL Elektromedizinische Geräte Gesellschaft m.b.H. Fürstenweg 77a, 6020 Innsbruck, Austria Otoplan healthcare software
Recipients	Semmelweis University, Department of Otorhinolaryngology and Head and Neck Surgery, 1083 Budapest, Szigony u. 36. Cooperating healthcare institution - for implant surgeries and procedures, Heim Pál Children's Hospital, Otorhinolaryngology Department, 1089 Budapest, Delej utca 13-15. Cooperating healthcare institution - for implant surgeries and procedures, University of Pécs Clinical Center, Department of Otorhinolaryngology and Head and Neck Surgery, 7621 Pécs, Munkácsy M. u. 2. Cooperating healthcare institution - for implant surgeries and procedures, University of Szeged, Faculty of General Medicine, Department of Otolaryngology and Head and Neck Surgery, 6725 Szeged, Tisza Lajos krt. 111. Cooperating healthcare institution - for implant surgeries and procedures

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, healthcare workers, audiology department staff, sales staff, implant staff, CRM admin staff, Call Center staff, and management can 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 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:

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

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 contacting us, the data subject declares that he/she has read the Data Processing Notice related to Hearing Implants, and consents to the processing and storage of his/her data as set out in the notice.

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

DATA PROCESSING NOTICE

Customer data management
EESZT mandatory data disclosure

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	https://victofon.hu/hu
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 Social security number Outpatient form content Content of the E-prescription	Completing mandatory data transmission to the EESZT, redeeming/issuing prescriptions in the EESZT, uploading paper prescriptions to the EESZT	Necessary for the fulfilment of a legal obligation - GDPR Article 6(1) paragraph (c)	In the EESZT system, data is stored for 10 years after the death of the person concerned. - detailed storage periods are available in the EESZT data processing notice, see. https://www.eeszt.gov.hu/documents/20182/36430/EESZT_Lakossagi_adatkezelesi_tajekoztato_07.01_.pdf/9fc81355-d9d0-5f88-8746-10df9d2fd10d

Related legislation
Decree 39/2016.(XII. 21.) of the Ministry of Human Resources on detailed rules related to the Electronic Health Service System Act XLVII of 1997 on the Processing and Protecting of Medical and other Related Personal Data;

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)	Cloudent Kft. 1027 Budapest, Tölgyfa u. 28 Cloudent medical software Audiosoft IT-Consulting Kft. 1013 Budapest, Pauler u. 15. AVOIR software medical aids, MED-EL Elektromedizinische Geräte Gesellschaft m.b.H. Fürstenweg 77a, 6020 Innsbruck, Austria Otoplan healthcare software
Recipients	Ministry of the Interior, 1014 Budapest, Szentháromság tér 6. Unified Electronic Health Service System (EESZT)

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, healthcare workers, audiology department staff - doctors and assistants.
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 Access to the EESZT is limited - e-Személyi, mobile token

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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Preparation of financial documents, payment, invoicing

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	https://victofon.hu/hu
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, billing address, address Method of payment In case of transfer, the bank account number Last 4 digits of the credit card number in case of card payment Email address if sent by email Amount Health fund membership details, identifier - if applicable Coupon code - if applicable Designation of product, date	Data processing related to payments Preparation of financial documents, conclusion and administration of installment agreements, issuance of warranty certificates Debt management - if applicable	Necessary for the performance of a contract or fulfilment of a legal obligation - GDPR Article 6(1) paragraph (b) and (c)	8+1 years pursuant to Section 169(2) of the Accounting Act.

Related legislation
Act CXXVII of 2007 on Value Added Tax Act C of 2000 on Accounting

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)	Kiss-Tóth Könyvelő Kft. 1149 Budapest, Nagy Lajos király útja 108. Accountant, Magyar Telekom Nyrt. 1097 Budapest Könyves Kálmán krt. 34-36 Telecommunications service provider(s), MBH Bank Nyrt. 1056 Budapest, Váci utca 38., Bank(s), Raiffeisen Bank Zrt. 1133 Budapest, Váci út 116-118. financial institution(s), POS terminals Bizworks Kft. (Worldline business partner) 1024 Budapest, Margit krt.15-17. Payment service provider - in the case of online payments, a web store, VPOS terminal provider, etc. 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, AXEL Professional Softwares Kft. 6000 Kecskemét, Dobó I. krt. 13. III/11. Axel Pro invoicing software 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
Recipients	Health Fund service providers Flex Audit Kft. 1223 Budapest, Kápolna utca 25/A I.em.4. Auditor - if applicable

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, audiology department, finance, CRM admin, Call Center staff, and management can access the data.
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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Subsidy settlements

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	https://victofon.hu/hu
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
Content of the prescription Data included in the prescription settlement, personal data - in particular: Social security number Patient ID Date of birth Public medical assistance certificate number Data pertaining to the device	Processing of subsidy settlement, prescription settlements, fulfilment of legal obligations	Necessary for the fulfilment of a legal obligation - GDPR Article 6(1) paragraph (c)	8+1 years pursuant to Section 169(2) of the Accounting Act.

Related legislation
Govt. Decree 134/1999 (VIII. 31.) on the accounting and disbursement of subsidies for the price of medicines, medical aids and spa services prescribed within the framework of outpatient care Decree 14/2007 (III. 14.) of the Minister of Health on the inclusion of medical aids in social security support, subsidized prescription, distribution, repair and rental Govt. Decree 43/1999 (III. 3.) on the detailed rules for financing healthcare services from the Health Insurance Fund

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 will be transmitted:

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	Kiss-Tóth Könyvelő Kft. 1149 Budapest, Nagy Lajos király útja 108. Accountant, MBH Bank Nyrt. 1056 Budapest, Váci utca 38., Bank(s), Raiffeisen Bank Zrt. 1133 Budapest, Váci út 116-118. financial institution(s), POS terminals Cloudent Kft. 1027 Budapest, Tölgyfa u. 28 Cloudent medical software Audiosoft IT-Consulting Kft. 1013 Budapest, Pauler u. 15. AVOIR software medical aids
Recipients	National Health Insurance Fund Management (NEAK) BÉVER system 1140 Budapest, Váci út 73/A, operation of the Békéscsaba Prescription Settlement System (BÉVER)

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, finance, CRM admin, Call Center staff, and management can access the data.
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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Data processing of relatives and legal representatives

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	https://victofon.hu/hu
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 Place and date of birth Other identifying information - mother's maiden name, address - if applicable Email Phone Type and number of personal identification document	In the case of minor or incapacitated patients, related administration, patient identification, data collection, data verification, provision of healthcare services, preparation and retention of patient documents, keeping contact, providing information, provision of information to relatives, issuance of medical aids to the authorized person/recipient	Necessary for the performance of a contract or fulfilment of a legal obligation - GDPR Article 6(1) paragraph (b) and (c)	For 10 years after the contact is established, unless there is another legal basis to support the processing. As part of the health documentation, the data controller retains the data for 30 years from the date of data collection.

Related legislation
Act V of 2013 on the Civil Code

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 relative of the data subject

The data will be transmitted:

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	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
Recipients	

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, healthcare workers, audiology department staff, sales staff, CRM admin staff, Call Center staff, and management can 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 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:

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

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.

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

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	https://victofon.hu/hu
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
Processors (performing technical tasks related to data processing operations)	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,
Recipients	

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Google Inc,USA,Privacy Policy Data Privacy Framework,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	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.
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 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:

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

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 providing his or her data, the data subject declares that he or she has read the Data Processing Notice related to Sending Marketing Inquiries and Offers, and consents to the processing and storage of his or her data as set out in the notice.

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

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	https://victofon.hu/hu
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

The data will be transmitted:

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	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,
Recipients	

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Google Inc,USA,Privacy Policy Data Privacy Framework,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	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.
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 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:

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

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 providing their data, the data subject declares that they have read the Data Processing Notice related to the Satisfaction Survey, Questionnaires, and Customer Reviews, and consents to the processing and storage of their data as set out in the notice.

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

DATA PROCESSING NOTICE

Customer data management
Publishing 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	https://victofon.hu/hu
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
Personal data provided in the review or story Photo, name, signature - optional	Recording and publishing customer reviews for marketing purposes on the website, social media, and in printed marketing materials	Consent of the data subject - Article 6(1)(a) GDPR	10 years, but no later than until the consent is withdrawn. You can withdraw your consent by writing to ugyfelszolgalat@victofon.hu Consequences of refusing consent: the review will not be published, the reference will not be published, but no other adverse consequences will affect the data subject.

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, Meta Platforms Ireland Limited 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland Facebook, Instagram social media, X International Unlimited Company 1 Cumberland Place, Fenian Street, Dublin 2, Dublin, D2, Dublin, Ireland Twitter social media, Google LLC 1000 Cherry Avenue, San Bruno, CA 94066, United States Youtube social media,
Recipients	

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Meta Platforms Ireland Limited,USA,Privacy Policy Data Privacy Framework,https://hu-hu.facebook.com/privacy/policy https://www.dataprivacyframework.gov/list,possible access by parent company, data storage, X International Unlimited Company,USA,Privacy Policy Data Privacy Framework,https://x.com/en/privacy,possible access by parent company, data storage, Google LLC,USA,Privacy Policy Data Privacy Framework,https://policies.google.com/privacy?hl=hu&fg=2,data storage,

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, 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.
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 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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Prize draws, promotion campaigns

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	https://victofon.hu/hu
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 Date of birth Telephone number, email address Address Photo, video - if applicable	Ensuring participation in prize draws, ensuring online or offline registration, conducting the competition, drawing, preparing a report, notifying the winner, contacting, publishing the winner's details if applicable, delivering the prize to the winner Taking pictures and making a video of the prize presentation - if applicable	Consent of the data subject - Article 6(1)(a) GDPR	5 years after the end of the contest, 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

The data will be transmitted:

Category	Company name, registered seat, activity
Processors (performing technical tasks related to data processing operations)	Kiss-Tóth Könyvelő Kft. 1149 Budapest, Nagy Lajos király útja 108. Accountant, Magyar Telekom Nyrt. 1097 Budapest Könyves Kálmán krt. 34-36 Telecommunications service provider(s), Total Studio Kft. 2096 Üröm, Asztalos utca 14/B. Website development, website support, operation, Meta Platforms Ireland Limited 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland Facebook, Instagram social media, X International Unlimited Company 1 Cumberland Place, Fenian Street, Dublin 2, Dublin, D2, Dublin, Ireland Twitter social media, Google LLC 1000 Cherry Avenue, San Bruno, CA 94066, United States Youtube social media, MiniCRM Zrt. 1075 Budapest, Madách Imre út 13-14. MiniCRM - CRM system operator, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Office 365 software (word, excel, etc.)
Recipients	Notary Public certification of the prize draw

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Meta Platforms Ireland Limited,USA,Privacy Policy Data Privacy Framework,https://hu-hu.facebook.com/privacy/policy https://www.dataprivacyframework.gov/list,possible access by parent company, data storage, X International Unlimited Company,USA,Privacy Policy Data Privacy Framework,https://x.com/en/privacy,possible access by parent company, data storage, Google LLC,USA,Privacy Policy Data Privacy Framework,https://policies.google.com/privacy?hl=hu&fg=2,data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, marketing, sales, CRM admin, and Call Center staff can 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 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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Customer referrals, Ambassador program

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	https://victofon.hu/hu
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
For both the referrer and the referee: Surname, first name Date of birth Address Telephone number Email address	Finding and registering potential customers, operating a referral program, and delivering gifts to participants	Consent of the data subject - Article 6(1)(a) GDPR	For 5 years after the referral, unless there is another legal basis to support the 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 Person referring 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), 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, 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, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Office 365 software (word, excel, etc.)
Recipients	

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties. Typically, marketing and sales staff, CRM admin staff, Call Center staff, and audiology department staff can 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 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 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:

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

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 providing his or her data and participating in the program, the data subject declares that he or she has read the related data processing notice, and consents to the processing and storage of his or her data as set out in the notice.

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

DATA PROCESSING NOTICE

Customer data management
Service activities, warranty administration

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	https://victofon.hu/hu
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 Social security number Address Telephone number Email address Product information, date, name of the audiology department and purchase-related data, information that may contain personal data	Servicing, repair, maintenance, and replacement of products Investigating and fulfilling warranty and guarantee claims Contacts	Necessary for the performance of a contract - GDPR Article 6(1) paragraph (b)	For 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), Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Office 365 software (word, excel, etc.)
Recipients	MED-EL Elektromedizinische Geräte Gesellschaft m.b.H. Fürstenweg 77a, 6020 Innsbruck, Austria Implant Manufacturing Partner, healthcare service provider, WS Audiology-H Kft. 1196 Budapest, district 19, Petőfi utca 75 Hearing aid service activity GN Hearing A/S DK-2750 Ballerup Lautrupbjerg 7 Hearing aid service activity

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,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:

Restricting access	Only those employees have access to personal data who are in absolute need of this information to perform their duties, e.g. CRM admin staff, Call Center staff.
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 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:

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

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.

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

DATA PROCESSING NOTICE

Customer data management
Photos, videos

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	https://victofon.hu/hu
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
Photo, video	Taking and publishing photos and videos of customers, their relatives, and persons participating in the controller's events on the website and social media for marketing purposes	Consent of the data subject - Article 6(1)(a) GDPR	for 10 years, but no later than until the consent is withdrawn. You can withdraw your consent by writing to ugyfelszolgalat@victofon.hu, or via any of the other known contact details. Consequences of refusing consent: no recording will be made, no publication will take place.

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, Meta Platforms Ireland Limited 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland Facebook, Instagram social media, X International Unlimited Company 1 Cumberland Place, Fenian Street, Dublin 2, Dublin, D2, Dublin, Ireland Twitter social media, Google LLC 1000 Cherry Avenue, San Bruno, CA 94066, United States Youtube social media,
Recipients	

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

Name of data processor, place of transfer, guarantees of transfer, reason for transfer
Meta Platforms Ireland Limited,USA,Privacy Policy Data Privacy Framework,https://hu-hu.facebook.com/privacy/policy https://www.dataprivacyframework.gov/list,possible access by parent company, data storage, X International Unlimited Company,USA,Privacy Policy Data Privacy Framework,https://x.com/en/privacy,possible access by parent company, data storage, Google LLC,USA,Privacy Policy Data Privacy Framework,https://policies.google.com/privacy?hl=hu&fg=2,data storage,

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. This typically includes marketing and sales staff, CRM admin staff, Call Center staff. The enterprise ensures this through authorization management. Data disclosed on online or offline platforms is public data, accessible to anyone."
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 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 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:

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

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 participating in the event, the data subject declares that he or she consents to the processing and storage of his or her related data as set out in the Data Processing Notice for Photos and Videos.
The data subject may withdraw his or her consent at any time or indicate during the recording that he or she does not wish to appear in the recordings.

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

DATA PROCESSING NOTICE

Complaints handling
Complaints handling

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	https://victofon.hu/hu
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 Address Email address Telephone number Place and date of birth, social security number - if applicable Content of complaint or report - any personal data contained therein	Investigation of complaints, reports, abuse reports, giving response, case management, administration Retention of documents and related personal data for the purpose of protecting and enforcing legal claims	Necessary for the fulfilment of a legal obligation - GDPR Article 6(1) paragraph (c)	The storage period is 5 years for complaints related to healthcare, 3 years for consumer protection complaints, and 5 years for other reports.

Related legislation
Act CLV of 1997 on Consumer Protection Act CLIV of 1997 on Healthcare Act XXV of 2023 on Complaints, Notifications of Public Interest and the Rules for Reporting Abuses Act V of 2013 on the Civil Code

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.

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

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), 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, Microsoft Corporation One Microsoft Way Redmond, Washington 98052 Office 365 software (word, excel, etc.)
Recipients	Lászka Ügyvédi Iroda 1111 Budapest, Irinyi József u. 23. II/3 Attorney-at-law, legal advisor - if necessary, if applicable

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,https://policies.google.com/privacy?hl=hu&fg=2,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,possible access by parent company, data storage, Microsoft Corporation,USA,Terms of Service and Privacy Policy Data Privacy Framework,https://privacy.microsoft.com/hu-hu/privacystatement, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA https://www.dataprivacyframework.gov/list,possible access by parent company, data storage,

Joint processing takes place:

Answer	Name and registered seat of the joint controller

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 customer service, legal department, complaint handling staff and management. The company 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 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:

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

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.