VIDEOTON HOLDING ZRT.
PRIVACY NOTICE

VIDEOTON HOLDING ZRt. (8000 Székesfehérvár, Berényi út 72-100., company registration number: 07-10-001107)
as the data controller aims to ensure the enforcement of the protection of personal data and the right of informational self-determination; that is why it has prepared its policies that ensure that the Company's activities comply with the provisions of applicable data protection laws. This Notice provides information on the scope of personal data processed by the Company, their use, as well as the rights of the data subjects.

I. APPLICABLE LAWS

The Company's data processing principles are in harmony with the applicable laws, in particular the following:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: GDPR)
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: Privacy Act)
- Act V of 2013 on the Civil Code of Hungary (hereinafter: Civil Code)
- Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter: Security Services Act)

II. DATA PROCESSING PRINCPLES FOLLOWED BY THE COMPANY

a) The Company processes the data **lawfully, fairly** and in a **transparent manner** in relation to the data subject.
b) The Company collects personal data **for specified, explicit and legitimate purposes** and not in a manner that is incompatible with those purposes.
c) The personal data processed by the Company are adequate, relevant and **limited to what is necessary** in relation to the purpose(s) for which they are processed. Accordingly, the Company does not collect or store more data than what is strictly necessary for the purposes of data processing.
d) The personal data processed by the Company are **accurate** and **kept up to date**. The Company takes every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
e) Personal data are kept by the Company in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the personal data are processed, having regard to any storage obligation stipulated by the applicable laws.
f) The Company ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using **appropriate technical or organisational measures**.
g) The **Company** shall be **responsible** for, and can **demonstrate** compliance with, the principles detailed above. Accordingly, the Company ensures the continuous enforcement of those set out in its privacy

policies, the continuous revision of its data processing operations and, as necessary, the modification or supplementation of its relevant procedures.

III. INDIVIDUAL INSTANCES OF DATA PROCESSING BY THE COMPANY

1. Processing the data of employees applying for work or to the database, or those applying for dual education; applications, curricula vitae

***Scope of** personal **data** that may be processed:* the natural person's name, date and place of birth, mother's name, address, address for notices, ID card number, qualification data, language skills, requested wage in the case of job applications, photo, phone number, email address, other data provided by the applicant in CVs and cover letters, any note taken by the employer about the applicant and, in the case of non-Hungarian citizens, passport number, data of the residence and work permit. Further data processed in the case of dual education: data of secondary school (name and city), name of the selected university and the major, data of school certificates.

***Purpose** of personal data processing:* application, assessment of the application, entering the jobseeker in the database, conclusion of a (student) work contract with the selected applicant.

***Legal basis** for data processing:*
- the data subject's consent
- the Company's legitimate interest

*The **controllers and/or the recipients** or categories of recipients of the personal data:*
Data at the Company are processed by the manager authorised to exercise employer's rights and the employees performing tasks related to HR administration.

Under a specific declaration of consent to that effect, if the given applicant so requests, their personal data may be transmitted to the employees of companies within the VIDEOTON Group performing tasks of HR administration so as to increase the chances of employment.

In the case of those applying for dual education, recipients of the personal data may also include those employees of the member companies of the VIDEOTON Group participating in dual education who perform HR administration tasks, as application is to the VIDEOTON Group. The member companies affected by data processing shall qualify as joint controllers with the Company.

***Duration of processing and storage** of personal data:*

The Company processes the applicant's personal data until the closure of the announcement or the application period, for the purpose of contacting the applicant in connection with the job or the dual education, and to assess the application.

In the case of job applications, following the application procedure, under a specific declaration of consent and provided that the unsuccessful applicant so requests, their personal data may continue to be processed also in the jobseeker database after the closure of the application procedure so that the Company can contact them with and notify them of any further vacancies, until the date stipulated in their consent.

Otherwise the data of the applicants will be stored for 4 years following the assessment of the application, on the basis of the Company's legitimate interest: with respect to possible legal claims, authority or court procedures, or inspections by the authorities.
Following the expiry of the above periods, the personal data of any applicants not selected shall be deleted; along with the data of anyone who has withdrawn their application.
If the applicant seeking a job has submitted their application other than for a job announcement, the above deadlines shall be calculated from the submission of their application or CV.

2. Data processing in connection with CCTV surveillance

*Processed data and the **legal basis** for processing:*
At its registered office and site, our Company uses electronic surveillance and video camera system enabling the recording of images, which shall qualify as personal data pursuant to the applicable legal regulations.
The legal basis for data processing is the Company's legitimate interest.

***Purpose** of data processing:*
The primary purpose of installing the CCTV system is **property protection** i.e. guarding the products and movables stored, warehoused or under processing by the Company, preventing and investigating any entry by unauthorised persons, preventing thefts, and protecting business secrets.
Furthermore, at places where the machines, the work equipment, the materials or the activity may pose danger, data processing also aims to protect the **life and bodily integrity of visitors and anyone at the premises.**

***Location** of the video cameras:*
Video cameras are located in line with the specified purposes, primarily in storage rooms, at exits and entrances, on corridors, specific parts of the plant that are important in terms of property protection, and in offices. No video camera may be installed at places where it would violate personality rights (e.g. bathrooms).
The fact of applying an electronic surveillance system at the given premises shall be indicated with a sign or notification that is placed at a location where it is easily visible, clearly legible and provides information to any third person wishing to attend the premises.
The exact location of the installed video cameras and the areas under surveillance shall also be made available by the Company at the given location and shall be amended accordingly if there are any changes in the cameras.

***Means and duration** of data processing:*
Data processing is limited to its purpose and shall comply with this purpose in each phase. The recordings made by the video cameras shall be saved, and the Company is entitled to store them for a period corresponding to the purpose. If no circumstance justifying storage for a longer period occurs, and the data were not used, they will be deleted after **15 days.**

***Persons authorised** to process and access the data:*
Data may be processed at the Company by the employees performing security services at the entrances, the manager in charge of property protection and the relating technical, IT tasks and control, and the employees tasked with such responsibilities. The scope of such employees may be defined by the management.
In addition to the employees specified above, data may be accessed by the CEOs and their deputies. In specific cases, the employee appointed by the CEO or their deputy on a case by case basis may also be authorised to access the data, to the extent necessary. This shall be subject to a managerial decision in each case, and the principle of purpose limitation and other provisions of privacy laws shall also be taken into consideration even in these cases in connection with data processing.

In connection with the data processing associated with such control, the data subject shall be entitled to exercise the rights set out in the paragraph of this Notice on data subject rights.

Anyone whose right or legitimate interest is affected by data in the image, audio or image and audio recording, may request – within 15 days from the date of recording such image, voice or image and voice, by demonstrating their right or legitimate interest – the controller not to destruct and/or delete the data.

3. Data processing during the use of the Company's website

*Types of data processing, **the personal data processed***
The persons visiting our website (www.videoton.hu) are not required to provide any personal data or information on the public parts of the website, or to register, in order to access the various parts of the website.
If the user does not specifically provide any data or information concerning themselves on the website, our Company shall not collect or process any personal data concerning the user in a way allowing for the user's personal identification.
On the basis of their own decision, the visitor may provide information in order to, for example, contact us for further information (in such a case, the processed data include: name, email, phone number) or to send a CV

or information regarding their work experience (see section III.1). In accordance with our data protection principles, we only collect the minimum of information required for the fulfilment of the visitor's request.
The Company assumes no liability for the content and data or information protection practices of any third-party websites/links available through hyperlinks from the Company's website.

In such a case, the legal basis of data processing is the data subject's consent; whereas regarding the legal basis for processing the data and CVs of job applicants, further specific rules can be found in section III.1 of this Notice.

*The **purpose** of data processing*
Any personal data provided by the visitor will only be used for the purpose for which the visitor has provided it at the time of collection (or which was obvious based on the circumstances of data collection). Personal data are typically collected for the following purposes: registration for specific parts of the website; application for a job or dual education, submission of professional CV; contact or communication for other purposes.
Our website does not collect or aggregate personal data for the purpose of transferring or selling such data to third parties so that they can use such data for consumer marketing purposes or for sending messages on behalf of third parties.

Data retention
Personal data collected on our website will be retained as long as they are necessary for the purpose for which they have been collected (as detailed in this Notice) or as long as required by law.
The contact data of visitors are retained as long as the information is necessary for fulfilling the request or until the user requests the deletion of the information.
Otherwise the provisions of section III.1 shall mutatis mutandis apply to the retention period of the data in CVs and job applications submitted through the website and to the relating legal bases.

4. Use of cookies on the website

On the Company's website, www.videoton.hu, data can also be collected automatically, by means of cookies, to a limited extent, as follows.

Cookies are small files, consisting of letters and numbers, which are downloaded to online devices (e.g. computer hard drive or telephone) when the visitor enters specific websites. The cookie enables the given website to recognise the visitor's online device, and so individual information concerning the visitor is stored for the website (e.g. the selected language). This way, the visitor need not select this data or information again when visiting the website later. Most major websites use such cookies.

On the Company's website, two types of cookies are used:

Session cookie: These are temporary cookies that only operate when the visitor enters the given website and only until they close the browser. Session cookies help the VIDEOTON website "remember" what the visitor selected on the previous site, so that they need not provide the same information again.

Persistent Cookies: These are the cookies that remain on the online device even after the visitor has left the given website, and store a randomly generated number in relation to the website visitor. The period of such cookie remaining on the visitor's online device depends on the type of the cookie. The stored (tracking) cookies applied on the website provide important traffic data regarding the use of the website.

Tracking and reporting to us is performed by our following partners:

- Google Analytics (further information:https://www.google.dk/intl/hu/analytics/)
- The third-party cookies of our advertising partners, measuring our campaign results:
    - Google Adwords (further information: adwords.google.hu)
    - Yahoo! Bing Network (further information: http://advertising.microsoft.com/international/advertise/bing?s_int=intl_prem_msahp_mid_1_bing/)

The above **cookies are not linked to any other user data, and so the user is not personally identifiable i.e. the data controller does not process personal data in connection with the cookies.**

The primary purpose of cookies is to aggregate data for website analytics and developments.

Means of disabling and/or removing cookies:
If visitors would like to disable, block the cookies associated with the Company's website or delete the ones already placed, they can do so among the settings of their browser. They will be assisted by their browser's Help function or the user guide of their mobile phone.
The detailed information on the www.aboutcookies.org website can also help with the settings in the various browsers. To see the content of the cookie, click on the cookie itself; then it opens and reveals a short line of text and numbers.
The disabling of cookies may affect certain functions on the website, resulting in their limited use.

For further information on those regulated in this section, see the Company's IT Security Policy.

5. Data processing on the Company's Facebook page

General rules *applicable to the Company's Facebook page*
The Company maintains a Facebook page for the purposes of providing information on and promoting its products, services and activities, and to publish job offers.

The Company shall not process the personal data published by visitors on the Company's Facebook page.
Any questions asked or comments posted on the Company's Facebook page shall not qualify as an official enquiry sent to the Company. Incoming messages will be answered by the Company's PR and Marketing staff, and the Company performs no data processing in this connection.

Facebook's Terms and Conditions of Data Protection and Service shall apply to the visitors.
If unlawful or illegal content is published on the page, the Company may without prior notice delete the data subject as a member or remove the comment.
The Company shall not be liable for any infringing content and comment published by Facebook users.
The Company shall not be liable for any defect, breakdown caused by the operation of Facebook or problems arising from a change in the operation of the system.

Applying for a job on the Company's Facebook page
The Company's Facebook page enables for direct application to the Company's job advertisements, by clicking on the Apply button and providing personal data.
The Company ***processes the personal data*** provided by the user, namely: name, telephone number, city/town, email, work experience, studies.
Legal basis *for data processing:* the Company processes these voluntarily provided data on the basis of the data subject's consent.
The ***purpose*** *of data processing* is to contact the applicants in order to fill the position.
Duration *of data processing:* until the closure of the application process.
Recipient *of the data:* the Company's PR and HR staff who, as the case may be, contact the applicant for further consultations. If this entails the submission of a CV or further data processing, this shall be governed by section III.1 of the Notice.

Otherwise the Privacy Policy and Notice of Facebook can serve with detailed information regarding the processing of these data by Facebook.

6. Data processing in connection with organising prize games

Categories of data *processed*
If the Company organises any promotion or prize game – either on the Company's Facebook page or other forum –, it may process the personal data provided by the data subject (such as the name, address, phone

number, email address, online ID and Facebook username of the natural person) on the basis of the data subject's consent. Participation in the game is voluntary.

The **purpose of processing** the personal **data:** identifying and notifying the winner of the prize game, sending them the prize, ensuring the verifiability of the draw.

Legal basis *for data processing:* the data subject's consent until the draw, and then the Company's legitimate interest.

Duration of storage of the personal ***data:*** the Company stores the personal data for 12 months after the draw on the basis of its legitimate interest, consisting in the verifiability of the result of the draw and the conduction of the game.

The ***recipients*** or categories of recipients of the personal data: the Company's marketing and PR staff and, if gift is dispatched, the postal service or courier staff in respect of the name and delivery address.
Publication: the name of the winners will be published on the Company's Facebook page on the basis of the data subject's consent.

Possible consequences of failure to provide the data: the data subject will not be able to participate in the prize game.

The detailed rules, conditions and data processing principles of the individual prize games and draws will be made available by the Company in the appropriate manner concurrently with announcing the prize game in question.

7. Processing of the data of partners and contact persons

If the Company concludes a contract or enters into negotiations in order to conclude a contract with a *natural person* external to its organisation, then the ***scope of*** *personal* ***data*** *processed* may include: the natural person's name, name at birth, place and date of birth, mother's name, address, mailing address, email address, phone number, ID card number, tax number, nationality.
If the Company concludes a contract or enters into negotiations in order to conclude a contract with a *legal person*, then the ***scope of*** *personal* ***data*** *processed* may include: the name, phone number and email address of the natural person acting as the contact person or representative.

The ***purpose*** *of processing the personal data:* the conclusion and performance of contract and ensuring communication and effective cooperation between the parties.

Legal basis *for data processing:*

- performance of the contract, taking steps prior to entering into a contract,
- the Company's legitimate interest

The ***controllers and/or the recipients*** *or categories of recipients of the personal data:*
The data will be processed by the employees of the Company's units in charge of preparing and implementing contract conclusions (e.g. Procurement Directorate, Business Development Directorate, Legal Directorate).
The recipients of personal data may also include the member companies within the VIDEOTON Group, cooperating with the Company's given organisational units with regard to the contracts, and that shall qualify as joint controllers with the Company. The list of VIDEOTON Group companies is available at the Company's website in the "Our Company"/"Member Companies" menu; the data subject will receive sufficient information about the recipient member company at the time of contact.

Duration of storage *of personal data:*
The personal data will be stored during the preparation and the term of the contract in order to take the steps prior to entering into the contract and then to perform it.
If, for any reason, the contract is eventually not concluded, the data used for the preparation of the contract will be stored for 6 years following the conclusion of the negotiations on the basis of the Company's legitimate

interest, which in this case consists in making it possible to enter into contact in connection with further or modified business opportunities.
If the concluded contract terminates or ceases to have effect, the personal data will be stored for further 8 years on the basis of the Company's legitimate interest that consists in the exercise of or substantial defence against legal claims.

The Company will inform the data subject about the processing of their personal data and their rights relating to personality. If a contract is concluded, such contract shall set out the provisions on data processing.

8. **Data processing in connection with the whistleblowing system**

Scope of personal data *that may be processed*:
In a case when a report is submitted to the Company through the legally required whistleblowing system, the personal data processed related to the reporting are those which are essential for the investigation of the notification in connection with the persons concerned i.e.:

- the whistleblower
- the person whose conduct or omission gave rise to the report
- the person who may have substantial information about the subject matter of the report.

The scope of these data may vary depending on the nature of the report; tipically it covers basic data necessary to the identification of the concerned persons (e.g. name, e-mail address, telephone number, the content of the report, date of the reporting, etc.)

Purpose *of personal data processing:*
The purpose of processing personal data is to investigate the report, to remedy or terminate the conduct subject to the report, to keep contact, and to fulfil legal obligations.

Legal basis *for data processing*
The operation of the whistleblowing system is a legal obligation of the Company under the provisions of Act XXV of 2023, therefore the legal basis for data processing is the fulfilment of the Company's legal obligation.

The controllers and/or the recipients *or categories of recipients of the personal data*:
The personnel receiving the report, designated employees, the investigators, the body competent to conduct investigation proceedings including the members of the ethical committee designated for investigation as determined in the whistleblowing regulation.
The processed data may be transferred to the whistleblower protection attorney or external entities involved in the investigation.
Until the investigation is concluded or formal disciplinary actions are initiated based on the results of the investigation, the content of the report and information about the individuals involved in the report – beyond informing the involved person – can be shared with other departments or employees of the employer to the extent necessary for conducting the investigation. This also applies to individuals who may possess substantial information about the report.

The personal data of the whistleblower shall not be disclosed without his/her consent.

In accordance with legal provisions, if it becomes evident that the whistleblower, acting in bad faith, provided false or misleading data or information and:
a) it implies the commission of a crime or an offense, their personal data shall be handed over to the competent authority or person conducting the proceedings,
b) it is reasonably probable that it caused unlawful harm or other violations to others, their personal data shall be handed over to the authority or person authorized to initiate or conduct proceedings, upon request.

Duration of storage*, aspects of determination*
If no investigation is initiated based on the report, the data shall be deleted after 6 years following the communication of written notification about the dismissal of the investigation to the whistleblower. If an investigation is conducted, the data shall be deleted after 6 years following the communication of written notification about the results of the investigation to the whistleblower.

If the possible legal proceedings, legal claims, or other reasons require longer data retention period, the specific circumstances of such cases shall determine the applicable storage period, which may deviate from the aforementioned rules.

The above storage periods have been determined considering possible legal claims and enforcement of rights, taking into account the period of limitation of 5 years according to civil law.

Other rules
If the report concerns a natural person, during the exercise of his/her right to information and access, in accordance with the provisions of personal data protection, the personal data of the whistleblower shall not be disclosed to the requesting person.

IV. DATA SECURITY MEASURES

Whatever the purpose and legal basis of data processing, the Company shall take all necessary technical and organisational measures and shall have in place the appropriate procedural rules with a view to the security of personal data. In the course of this, it shall take into account the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and the costs of implementation.

The Company uses appropriate measures to protect personal data against accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure or access.

The Company qualifies and handles personal data as confidential information. Employees are bound by the obligation of confidentiality in connection with the processing of personal data. Authorisations to access the personal data are set out by the Company in the Record of Data Processing Activities.

The Company applies firewalls and antivirus protection to protect IT systems. Otherwise IT protection shall be governed by the provisions of the IT Security Policy.

The proper physical protection of personal data and the devices and documents serving as data carriers must be ensured; including the processing of data in a properly organised manner, locking them up if so required, and restricting entry into the storage rooms – in line with property protection and other relevant regulations.

Documents necessary for work in progress may only be accessed by the competent administrators; documents containing personnel, wage, employment and other relating personal data shall be kept safely locked up.

V. RIGHTS OF DATA SUBJECTS, HANDLING OF DATA SUBJECTS' REQUESTS

1. In harmony with the provisions of the GDPR, data subjects shall be entitled to the following rights, under the following terms and conditions.

Right of information

The data subject shall be entitled to the right of information regarding all legal bases for processing.

The data subject shall be entitled to be notified of the facts and information relating to data processing prior to the start of data processing, regarding all legal bases for processing.

The Company provides information to the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

a) Where personal data relating to a data subject are collected by the Company from the data subject, it shall, at the time when personal data are obtained, provide the data subject with the following information: the identity and the contact details of the data controller and the data controller's representative; the purposes of processing; the legal basis for the processing; if the legal basis is "legitimate interest", the legitimate interests pursued; the recipients or categories of recipients; *the period for which the personal data will be stored, or the criteria used to determine that period; the rights of data subjects; the right to lodge a complaint with a supervisory authority; whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.*

   If further data processing for a different purpose is planned, the data subject shall be previously notified of this different purpose and the information in italics in the above paragraph.

   The provisions in this point a) shall not apply where and insofar as the data subject already has the information.

b) Where the Company obtained the personal data other than from the data subject, the data subject shall be notified of the information listed in point a) above, plus the categories of personal data concerned; and the source of the personal data.

   The deadline for providing the information: as a main rule, within a reasonable period after obtaining the personal data, but at the latest within one month. However, if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

   If further data processing for a different purpose is planned, the data subject shall be previously notified of this different purpose and the information in italics in points a) and b) above.

   The provisions in this point b) shall not apply where and insofar as the data subject already has the information, and in the cases mentioned in Article 14(5) of the GDPR.

Right of access by the data subject

The data subject shall be entitled to the right of access regarding all legal bases for processing.

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

a) purposes of data processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed by the Company
d) where possible, the envisaged period for which the personal data will be stored
e) the existence of the right to request from the Company rectification of personal data or, in the case of processing on certain legal bases, deletion or restriction of processing of personal data or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling and the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Company shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Company may charge a reasonable fee based on administrative costs.

Right to rectification

The data subject shall be entitled to the right to rectification regarding all legal bases for processing.

At the data subject's relevant request, the Company shall, without undue delay, rectify any inaccurate personal data processed concerning the data subject. The data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten')

The data subject is not automatically entitled to the right of erasure in the case of all legal bases of processing.

The Company shall erase the personal data concerning the data subject without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed by the Company;
b) if processing is based on consent, the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
c) in the case of data processing carried out in the public interest, in the exercise of official authority or based on legitimate interest, the data subject objects to the processing and there are no overriding legitimate grounds for the processing or they do not apply;
d) the personal data have been unlawfully processed by the Company;
e) the personal data have to be erased for compliance with a legal obligation in Union or Hungarian law to which the Company is subject;
f) the personal data have been collected in relation to the offer of information society services (any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services).

The Company shall not be obliged to fulfil the data subject's request for erasure to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by law to which the Company is subject;
c) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company;
d) for reasons of public interest in the area of public health;
e) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
f) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

The data subject shall be entitled to the right to restriction regarding all legal bases for processing.

The Company shall restrict data processing at the data subject's request where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the Company to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
d) the data subject has objected to processing carried out in the public interest, in the exercise of official authority or based on legitimate interest, pending the verification whether the legitimate grounds of the Company override those of the data subject.

Where processing has been restricted according to the list above, such personal data shall, with the exception of storage, only be processed on the following bases:

a) with the data subject's consent, or
b) for the establishment, exercise or defence of legal claims, or
c) for the protection of the rights of another natural or legal person, or
d) for reasons of important public interest of the Union or of a Member State.

The Company shall notify this obligation to each recipient to whom the personal data have been transferred and shall inform the data subject before the restriction of processing is lifted.

Right to notification regarding rectification or erasure of personal data or restriction of processing

The Company shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been transferred, unless this proves impossible or involves disproportionate effort. The Company shall inform the data subject about those recipients if the data subject requests it.

Right to data portability

The data subject shall have the right to data portability if the processing is based on consent or on a contract and provided that processing is carried out by automated means.

The Company ensures the possibility to the data subject to receive the personal data concerning them, which they have provided to the Company, in a structured, commonly used and machine-readable format and to transmit those data to another data controller.

Right to object

The data subject shall have the right to object if processing is carried out in the public interest, in the exercise of official authority or based on legitimate interest.

If the data subject has objected to processing, the Company shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. In such a case the personal data shall no longer be processed for such purposes.

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

Automated individual decision-making

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

a) is necessary for entering into, or performance of, a contract between the data subject and the Company;
b) is authorised by Union or Hungarian law to which the Company is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.

The safeguards applicable to the cases in points a) to c) above shall be governed by Article 22(3)-(4) of the GDPR.

Right to be notified of a personal data breach

If the conditions laid down in this Notice are met and none of the exemptions apply, the Company shall be obliged to notify the data subject of the personal data breach as described herein.

Right to lodge a complaint with a supervisory authority, legal remedies

Every data subject shall have the right to lodge a complaint with the supervisory authority (Hungarian National Authority for Data Protection and Freedom of Information, H-1125 Budapest, Szilágyi Erzsébet fasor 22/c, mailing address: 1530 Budapest, Pf.: 5., e-mail: ugyfelszolgalat@naih.hu) if the data subject considers that the processing of personal data relating to them infringes the legal regulations.
The judicial review of the decision made by the Authority may be requested from the court, of which the supervisory authority itself shall also notify the data subject. For further detailed information please consult Articles 77-79 of the GDPR.

2. Actions to be taken upon the data subject's request

The Company shall **provide information** on action taken on a request – for exercising the data subject's rights – to the data subject without undue delay and in any event **within one month** of receipt of the request.

That period **may be extended by two further months** where necessary, taking into account the complexity and number of the requests. The Data Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the Company does not take action on the request of the data subject, it shall inform the data subject at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The Company **will provide** the details as prescribed by the GDPR and the **information** relating to data processing **free of charge.** Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
b) refuse to act on the request.

The Company shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Where the Company has reasonable doubts concerning the identity of the natural person making the request, the Company may request the provision of additional information necessary to confirm the identity of the data subject.

The Company shall keep records of the requests received from data subjects.

3. Special provisions applicable to erasure requests

If the Company receives an erasure request, as a first step it shall examine whether it is actually from a person entitled to submit such a request. To that end the Company may request the provision of details to identify the contract between the data subject and the Company (such as contract ID, date of the contract), the identification number of any other document issued to the data subject by the Company, and the personal identification data

on record at the Company concerning the data subject. However, the Company may not request for identification purposes any excess data which it does not keep on record concerning the data subject.

If the Company is obliged to fulfil the erasure request, it shall make every effort to ensure that the personal data is erased from all databases.

The Company shall keep records of the erasures performed.

The Company shall notify the erasure obligation to each recipient to whom the personal data have been transferred.

VI. THE DATA CONTROLLER, ITS REPRESENTATIVE, CONTACT INFORMATION

The Data Controller: VIDEOTON HOLDING ZRt., 8000 Székesfehérvár, Berényi út 72-100.
It is not mandatory for the Company to appoint a data protection officer pursuant to Articles 37-39 of the GDPR, and so the Company has no data protection officer.
In relation to data protection issues, the employees of the Human Resources Directorate of VIDEOTON HOLDING ZRt. tasked with data protection matters shall act on behalf of the Company, namely: Viktória Csóri and Gabriella Tamanné Bogárdi, both working in HR.
Data subjects can submit their requests to the following email address: adatvedelem@videoton.hu.
Further contact information: 8000 Székesfehérvár, Berényi út 72-100., phone number: 06-22 / 533 – 332.

The above text of the Notice – in a consolidated structure with the amendments to the version in effect from 25 May 2018 – shall be effective as of 24 July 2023.