

Data Management Information

In connection with the processing of personal data on the basis of an appointment to ensure compliance with Act CXII of 2001 on informational self-determination and freedom of information (Info tv.) and with the General Data Protection Regulation 2016/679/EU (GDPR)

Controller: FANOS Szolgáltató és Kereskedelmi Kft.

Registered office: 1015 Budapest, Csalogány u. 6-10.

Tax number: 11917261-2-41

Registration number: 01 09 725744

Our Data Management Information covers our following units:

- AQUA Hotel Termál - <https://aquahoteltermal.hu/>,
Address: 9200 Mosonmagyaróvár, Kígyó utca 1.
- AQUA Termál Kemping - <https://www.campingmovar.hu/>,
Address: 9200 Mosonmagyaróvár, Kígyó utca 1.
- AQUASOL Resort - <https://www.aquasolhotel.com/>,
Mosonmagyaróvár 9200 Lucsony utca 19.
E-mail: info@aquasolhotel.com

Contact details: Tel: 00 36 96 / 579 168, Fax: 00 36 96 / 579 169,

E-mail: aquahotel@t-online.hu

As a controller, we respect the privacy of all persons to whom personal data is provided. We make sure that all data management operations related to our activities comply with the expectations specified in this Information, the effective national laws and the legal acts of the European Union.

Data protection guidelines related to data management by Fanos Kft. are available on sites https://aquahoteltermal.hu/wp-content/uploads/2023/06/Adatkezelesi-tajekoztato_20230613.pdf, https://www.campingmovar.hu/wp-content/uploads/2023/06/Adatkezelesi-tajekoztato_20230613.pdf and https://www.aquasolhotel.com/wp-content/uploads/2023/06/Adatkezelesi-tajekoztato_20230613.pdf.

If you have any question in connection with this notification, please feel free to contact us. We state that Fanos Kft, as a controller, confidentially handles the personal data, and takes all safety, technical and organisational measures guaranteeing the safety of data.

This Information contains the followings:

- the types of identification data of those concerned, that has been collected by us;
- the list of data management purposes;
- the legal bases, according to which these are processed;
- the list of all persons to whom the data is forwarded; and
- the method of their storage.

Please carefully read this Information to understand the way in which we process your personal data.

Content

Interpretation of Key Concepts Used in the Information	3
Data provided during on-line contact	5
Mandatory registration and data supply in connection with checking in by those using accommodation services.....	5
Use of credit card data.....	7
Personal data managed for parking	8
Purchase of gift vouchers for the Beneficiary	8
Camera surveillance data.....	9
Data requested when a transfer service is demanded	10
Lost objects	10
Complaint management.....	11
Data related to the data management of employees	11
Job applications	12
Social media surfaces	12
Cookies.....	12
Technical data - What do we do for data security?	13
What are your rights and obligations in relation to your personal data?.....	14
Data protection Authority.....	17
Other Provisions.....	17

Our General Data Management Guidelines

Our data management principles comply with the data protection related effective legislation, including, in particular:

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Infotv.);
- 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, GDPR);
- Act V of 2013 on the Civil Code (Ptk.);
- Act C of 2000 on Accountancy (Számv. tv.);
- Act LIII of 2017 on the prevention and avoidance of money laundry and terrorism (Pmt.);
- Act CLVI of 2016 on state functions pertaining to the development of tourism regions
- Act CLV of 1997 on consumer protection
- Act CLXIV of 2005 on trade
- Act LXXVI of 2009 on the general rules of official public administration procedures and services
- Act C of 2003 on electronic communications (Ehtv.)
- Act XLVIII of 2008 on essential conditions of and certain limitations to business advertising (hereinafter: Grt.)
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (hereinafter: Eker tv.)

Interpretation of Key Concepts Used in the Information

Person concerned: A natural person identified or identifiable on the basis of any information.

Consent of person concerned: Definite statement of the will of the person concerned based on voluntary, clear and proper information, when the person concerned indicates with his/her statement or other behaviour unmistakably expressing his/her will, that he/she gives his consent to the processing of his/her personal data.

Personal data: Any information related to the person concerned.

A natural person is identifiable, when he/she can be identified either directly or indirectly, in particular on the basis of some identification data such as a name, number, location data, on-line ID or one or more factors related to the physical, physiological, genetic, intellectual, economic, cultural or social identity of the natural person.

Special data: all data belonging to the special category of personal data, i.e. personal data related to the racial or ethnic origin, political opinion, religious or philosophical conviction or union membership, as well as genetic data, biometric data intended to individually identify a natural person, the health data and personal data related to the sexual life or sexual orientation of the natural person.

Controller: A natural person or legal entity, or any association not having legal personality, who or which specifies the purpose of data processing, makes and implements decisions on data processing (including the devices used) or have the data processor implement them independently or together with others;

Joint controller: A controller, who or which specifies the purposes and devices of data processing – in the framework specified in a law or in a compulsory legal act of the European Union – jointly with one or more other controllers, makes and implements the decisions on data processing (including the devices used) jointly with one or more other controllers, or have the data processor implement them.

Data management: Any operation or a combination of operations performed on the data irrespective of the procedure followed, including, in particular, collection, recording, registration, systematisation, storage, change, use, consultation, forwarding, publication, harmonisation or connection, blocking, deletion and destruction of the data as well as prevention of additional use of the data, taking photos, sound or video recording, and registration of physical characteristics suitable for the identification of a person (i.g. finger or palm print, DNA sample, iris image);

Restriction of data management: Blocking of the stored data by using marks to restrict further processing of the data.

Data processing: All data management operations performed by the processor on behalf of the controller or at his/her instruction.

Processor: A natural person or legal entity, or any association not having legal personality, who or which processes the data under a contract signed with the controller, including also any contract signed on the basis of a provision of a law;

Data protection incident: Violation of data security, which results in accidental or unlawful destruction, loss, modification, unauthorised forwarding or publication of the personal data forwarded, stored or managed in any other way, or in unauthorised access to them.

Third party: A natural person or legal entity, or any association not having legal personality, who or which is not identical to the person concerned, the controller or processor;

Addressee: A natural person or legal entity, or any association not having legal personality, for whom or which the controller or the processor provides access to personal data.

How do we manage your data?

We receive the data directly from you. In these cases, the legal base for the data collection and processing is ensured either by your consent or by a contract made between us. Based on its sphere of activities, Fanos Kft. manages personal data in the following category:

Data provided during on-line contact

Purpose of data management	Inquiry, disclosure of information
Circle of persons concerned	All persons concerned inquiring about the services of Fanos Kft.
Managed data	<ul style="list-style-type: none"> • name • e-mail address • data send in mails
Use	Establishing and maintaining contacts, administration via e-mails
Legal base	definite and voluntary consent on the basis of preliminary information - Article 6 (1)(a) of General Data Protection Regulation 2016/679/EC
Storage time	until the achievement of the data management purpose
Data forwarding	not applicable

Mandatory registration and data supply in connection with checking in by those using accommodation services

On checking in at the accommodation, the Controller registers the data specified in the requirements in the IT system protected by means of multiple asymmetric encryption named VISA, i.e. in a storage space provided by the hosting service provider designated by the Government Decree. The purpose of the data registration is to make sure that the rights and security of the Person Concerned and of others are protected, and the control of adherence to regulations related to the staying of citizens from third countries and of persons having the right of free movement and residence is implemented. That is the primary purpose of the VIZA is to promote the protection of the public order, the public security, the rules of the state border, and the rights, security and properties of the Person Concerned and of others.

Purpose of data management	The support of purposes designated by the Government and execution of statutory obligation.
Circle of persons concerned	All persons concerned reserving accommodations at Fanos Kft.

Managed data	Data of the Person Concerned using the accommodation service <ul style="list-style-type: none"> • first name and surname • first name and surname at birth • place and date of birth • gender • citizenship • mother first name and surname at birth • identification data of the identification document or passport • the number of the visa or of the residence permit, the time and place of entry for citizens from third countries,
Use	Establishing and maintaining contacts, administration via e-mails
Legal base	performance of legal obligation (Article 6(1)(c) of the GDPR). The process of data supply is specified and regulated by Act CLVI of 2016 on state functions pertaining to the development of tourism regions.
Storage time	The data is erased by us after 5 years from termination of the connection with the Person Concerned on the basis of Paragraph 6:22 of the Ptk. It is kept for a longer period, if required by the law, for example, if the data must be kept on the basis of Paragraph 169 of Act C of 2000 on the accountancy (“Accountancy Act”), then the data is erased after 8 years from termination of the connection with the Person Concerned. Such cases include when the data is part of documents supporting accountancy, they are indicated for example in contract-related documents (or in the contract itself in relevant cases), and it must be kept for 6 years in the case of police reports.
Data forwarding	Please note that in the case of our accommodation services, data is forwarded and processed towards a third party (IFA - on the basis of a processor contract).
Source of managed data	person concerned, accommodation reservation portal, travel bureau

For persons who request an offer for accommodation services, but do not become guests, their personal data is managed in accordance with the content of Paragraph 6:64-65 of Act V of 2013 on the Civil Code.

Paragraph 6:64 [*Binding offer*]

(1) The person who makes a legal statement clearly expressing his/her intention to sign a contract and covering essential issues shall be bound by his/her statement. The bidder may specify the period in which his/her offer is binding.

(2) The period of the binding offer starts when the offer becomes effective.

Paragraph 6:65 [*The end of the binding offer*]

(1) If the bidder does not specify the period in which his/her offer is binding, the period of the binding offer ends

a) when an offer is made between the parties present, and the other party does not accept the offer immediately;

b) when an offer is made between the parties without their physical presence, after the expiry of the period in which the bidder would have expected the receipt of the answer under normal circumstances in view of the nature of the service indicated in the offer and of the method of making the offer;

c) when the other party rejects the offer.

(2) The binding offer ends, if the bidder withdraws his/her offer with his/her legal statement addressed to the other party before the other party sends his/her legal statement of acceptance.

(3) The written offer may be withdrawn in writing.

(4) An offer that has become effective may not be withdrawn, if the offer provides that it is irrevocable, or a date is specified in the offer for the acceptance.

If the inquirer sends his/her data to us, then he/she gives an official offer (legal statement) to our Company. For us to be able to follow up the acceptance of the offer, we continue to manage the personal data of the inquirer, and may call the inquirer via our communication channels (phone, e-mail) to ask him/her to make a statement on the offer during the period of the **binding offer**.

The binding offer shall be valid as long as the Company may expect the receipt of an answer under normal circumstances in view of the nature of the service indicated in the offer and the method of making the offer. Our Company shall manage the personal data in this period, however, for maximum six months from making the offer.

Use of credit card data

Purpose of data management	Room reservation for guests
Circle of persons concerned	All persons concerned reserving accommodations at Fanos Kft.
Managed data	<ul style="list-style-type: none">• Name indicated on the card• Card number,• CVC code,• Expiry date
Use	administration, payment of reservation of accommodation, request for advance
Legal base	performance of contract - Article 6 (1)(b) of General Data Protection Regulation 2016/679/EC

Storage time	The credit card data shall be used only for the transaction, and only by the authorised person. On departure from the hotel, the data shall not be disclosed any more, and any access to it shall not be allowed. The data shall be deleted after a successful transaction.
Data forwarding	not applicable

Personal data managed for parking

Purpose of data management	Provision of parking in the parking lot of the units of Fanos Kft.
Circle of persons concerned	All persons concerned parking their vehicles in the units of Fanos Kft.
Managed data	<ul style="list-style-type: none"> • name and address of person • date and time of arrival and departure • registration number of vehicle
Use	Establishment of contact, maintenance of contact, administration
Legal base	definite consent on the basis of preliminary information - Article 6 (1)(a) of General Data Protection Regulation 2016/679/EC
Storage time	until the achievement of the data management purpose
Data forwarding	not applicable

Purchase of gift vouchers for the Beneficiary

Purpose of data management	Purchase of gift vouchers
Circle of persons concerned	All persons purchasing gift vouchers for the services of Fanos Kft.
Managed data	<ul style="list-style-type: none"> • Customer's data: Name, e-mail address, phone, invoice address • Beneficiary's data: Name, voucher's content
Use	Establishment of contact, maintenance of contact, administration
Legal base	consent on the basis of preliminary information - Article 6 (1)(a) of General Data Protection Regulation 2016/679/EC

	We call the attention of those disclosing data to Fanos Kft. that if they provide not their own personal data, then the person disclosing the data shall acquire the consent of the person concerned.
Storage time	Until expiry of the voucher If an invoice is issued – legal obligation on the basis of the period specified in Article 6(1)(c) of Chapter II of General Data Protection Regulation 2016/679/EU - Accountancy Act: Relevant year + 8 years
Data forwarding	not applicable

Camera surveillance data

In connection with the operation of the camera system, we are obliged to give the following information:

- indication of signals (pictograms, labels)
- posting of information
- camera rules and annexes
- data protection rules and provisions made in the data management information in connection with camera surveillance
- information for the employees – certification confirmed in writing
- answer to questions received from employees

Purpose of data management	Property protection, i.e. the protection of precious assets and personal values of the guests is particularly important for us. Considering that the detection of violations of the laws, in flagrant delict and prevention of such violating acts cannot be achieved in other ways, and evidencing cannot be made with other methods, we have set up a security camera system.
Circle of persons concerned	All persons concerned staying at the accommodations and in areas under camera surveillance of Fanos Kft.
Managed data	image recorded by camera
Use	camera footage
Legal base	on the basis of a legitimate interest Article 6(f) of General Data Protection Regulation 2016/679/EU
Storage time	72 hours, in accordance with the requirements of the law if there is a data protection incident

Data forwarding	not applicable
------------------------	----------------

For further information on data management related to the camera system, contact our colleagues.

Data requested when a transfer service is demanded

Purpose of data management	Performance of transfer service on the basis of the request of the person concerned
Circle of persons concerned	All persons concerned requesting transfer services via the colleagues of Fanos Kft.
Managed data	name and phone number of the person concerned
Legal base	voluntary consent Article 6(1)(a) of General Data Protection Regulation 2016/679/EU
Storage time	until the achievement of the data management purpose
Data forwarding	Please note that in the case of our transfer services, data is forwarded and processed towards a third party (passenger transport company).

Lost objects

Purpose of data management	Handling and storage of objects found in the area of the accommodations of Fanos Kft., their identification by the person concerned
Circle of persons concerned	All persons concerned reserving accommodations at Fanos Kft. and leaving some value or object there.
Managed data	name of the finder, place and time of finding, room number, designation of the found object, its identification details
Legal base	Performance of contract signed on the room reservation as a service - Article 6(1)(b) of General Data Protection Regulation 2016/679/EC
Storage time	until the civil legal rights deriving from the use of the accommodation service expire, but for maximum 6 months
Data forwarding	not applicable

Complaint management

Purpose of data management	consumer protection, complaint management Please raise your complaints arising within the guarantee period via e-mail address aquahotel@t-online.hu or info@aquasolhotel.com . The data is recorded based on this.
Circle of persons concerned	All persons concerned who raise a complaint to Fanos Kft.
Managed data	<ul style="list-style-type: none">• name• contact details• designation of complaint
Legal base	Paragraph 17/A(7) of Act CLV of 1997 on consumer protection , which requires the above data management.
Storage time	5 years from making a report.
Data forwarding	To the Consumer Protection Authority

Data related to the data management of employees

We state that the data of the employees contracted by our Company is managed on the basis of Act CXII of 2011 (Info tv.), General Data Protection Regulation 2016/679/EC and Act I of 2012 (Labour Code).

Your data is managed, recorded and forwarded by our colleagues at the reception desk. Our employees are trained in GDPR, protection of personal data.

The GDPR applies also to the data and data management of our employees. Act I of 2012 on the Labour Code provides for this. Based on this, we manage and forward compulsory data to the authorities. The relevant detailed data management requirements is available in the controller's Data Protection Rules.

- Labour, personnel records
- Data management in relation to medical examinations for fitness
- Data management in relation to the control of use of an e-mail account
- Data management in relation to the control of a computer, laptop or tablet
- Data management in relation to the control of use of internet at work
- Data management in relation to the control of use of a company mobile phone
- Data management in relation to the use of GPS navigation system
- Data management in relation to entry and exit to and from the workplace
- Data management in relation to camera surveillance at work

Job applications

Purpose of data management	Advertised position, filling an empty post
Circle of persons concerned	All persons concerned who file a CV to Fanos Kft.
Managed data	data provided in the CV
Legal base	consent on the basis of preliminary information - Article 6(1)(a) of General Data Protection Regulation 2016/679/EC
Storage time	until the empty post is filled
Data forwarding	not applicable

Social media surfaces

Purpose of data management	Marketing based advertisements, information on our services, novelties and discounts Contact details: https://www.instagram.com/aqua.hotel.termal/ https://www.instagram.com/aquasol.resort/ https://hu-hu.facebook.com/aquahoteltermal/ https://www.facebook.com/aquasolhotel/
Circle of persons concerned	Any user who likes and follows our social media sites
Managed data	data published by you in the social media.
Use	on-line, on the admin surfaces of the social media
Legal base	voluntary consent on the basis of preliminary information - Article 6 (1)(a) of General Data Protection Regulation 2016/679/EC
Time of use	until withdrawal of the consent
Data forwarding	To the controllers of social media

Cookies

Purpose of cookies They collect data on the visitors of our websites and their devices;

- the special settings of the visitors are recorded, and will (may) be used e.g when on-line transactions are carried out, and therefore it is not necessary to enter them again;
- the facilitate the use of websites;
- they offer excellent user experiences.
- For customized service provision, a data package, a so-called cookie is installed on the user's computer, which is read during subsequent visits.
- If the browser returns a previously saved cookie, the service provider controlling the cookie is allowed to connect the actual visit of the user to previous ones, but only in relation to his/her own content.

Further information: a

- https://aquahoteltermal.hu/wp-content/uploads/2023/06/Adatkezelesi-tajekoztato_20230613.pdf **separate link** and
- https://www.aquasolhotel.com/wp-content/uploads/2023/06/Adatkezelesi-tajekoztato_20230613.pdf
- https://www.campingmovar.hu/wp-content/uploads/2023/06/Adatkezelesi-tajekoztato_20230613.pdf címen.

Technical data - What do we do for data security?

Fanos Kft. selects and operates the IT tools used during the service provision for the management of the personal data to make sure that the managed data:

- is available for the authorised persons (availability);
- its authenticity and verification are ensured (authenticity of data management);
- its unchanged condition can be confirmed (data integrity);
- is protected against unlawful access (data confidentiality).

In addition, the controller states that the data

- is protected with proper measures
- against unauthorised access, modification, forwarding, publication, deletion or destruction as well as accidental destruction – e.g. limited authorities.

The controller provides for the protection of the security of data management with technical and organisational measures, which offer a protection level in accordance with the risks to which the data management is exposed – e.g. introduction of high security levels.

Information Security

The technical measures include the use of *encryption, protection of passwords and antivirus* software related to access to our systems.

As part of the process, during which you provide your personal data for us, this data may be forwarded also via the internet. Though we take all necessary measures to protect the personal data provided by you for us, data forwarding via the internet cannot be considered fully safe.

Therefore you have to acknowledge and accept, that we cannot take full responsibility for the security of data forwarding via our website, and if you forward the data in this way, then you shall be liable for it. As soon as your personal data is received in our systems, we follow stringent procedures to ensure security, and to prevent any unauthorised access.

What are your rights and obligations in relation to your personal data?

The person concerned may request information on the management of his/her personal data or correction and – except for compulsory data management – deletion, cancellation of his/her personal data, he/she may exercise his/her right to data portability and to object in the way indicated during data recording and via the above contact details of the controller.

Right to information

Fanos Kft. shall take proper measures to offer the persons concerned all information related to the management of personal data and mentioned in Articles 13 and 14 of the GDPR as well as all details included in Articles 15 to 22 and 34 in a brief, transparent, clear and plain way, and shall ensure easy access to them.

Right of the person concerned to access

The person concerned is entitled to receive feedback from the controller as to whether his or her personal data is being managed, and if such data management is in process, he or she is entitled to have an access to the personal data collected and the following information:

Purposes of data management;

- categories of personal data in question;
- addressees or categories of addressees to whom or which personal data has been or will be disclosed, including in particular addressees in third countries and international organisations;
- planned period of storage of personal data;
- right to correct, delete or restrict data management or to object;
- right to submit a complaint addressed to the supervisory authority;
- information on data sources;
- fact of automated decision-making, including profile creation, as well as information on the applied logics and on the significance of such data management and its potential consequences affecting the person concerned.

The controller shall give the information within maximum one month from submission of the request.

Right to correct

The person concerned may request the correction of inaccurate personal data managed by the controller and related to him/her as well as addition of missing data.

Right to delete

If any of the following reasons exists, the person concerned shall be entitled to request the controller to delete personal data related to him/her without any unreasonable delay:

- the personal data is not necessary any more for the purpose for which it was collected, or if it was managed in a different way;
- the person concerned withdraws his/her consent on which data management is based, and there is no other legal base for data management;
- the person concerned objects the data management, and there is no priority lawful reason for data management;
- the personal data has been unlawfully managed;
- the personal data must be deleted to meet a legal obligation specified in a legal act of the EU or in a law of a member state, which is applicable to the controller;
- the personal data was collected in connection with services offered in relation to information society.

Deletion of the data may not be initiated, if data management is necessary:

- to exercise the right of freedom of expression and information;
- to meet an obligation pursuant to a legal act of the EU or to a law of a member state specifying the management of personal data and applicable to the controller, and to perform a task required for any public interest or in the framework of exercising a public authority assigned to the controller;
- for any purpose concerning public health or for archiving, scientific and historical research purposes or statistic purpose based on public interest; or for submission, enforcement or protection of legal claims.

Right of limitation of data control

The person concerned is entitled to ask the controller to limit the data control, if any of the following terms is met:

- the person concerned argues the accuracy of the personal data, in which case the limitation applies to the period allowing the controller to check the accuracy of the personal data;
- the data control is unlawful, and the person concerned opposes the deletion of the data, and he or she requests the limitation of its use instead;

- the data controller does not need the personal data for data management purposes any more, but the person concerned needs it for submission, validation or protection of legal claims; or
- the person concerned objects the data management;
- in that case the limitation applies unless it is established that the legal reasons of the controller has a priority over the legal reasons of the person concerned.

If data management is subject to restriction, the personal data may be managed – except for storage – only with the consent of the person concerned, or for the submission, enforcement or protection of legal claims, or for the protection of the rights of other natural or legal entities, or in an important public interest of the EU or a member state.

Data portability right

The person concerned is entitled to receive the personal data related to him/her and provided by him/her for the controller in an articulated, widely used format which can be read on a machine, and to forward this data to another controller.

Right to object

The person concerned is entitled to object data management necessary for the performance of a task required in a public interest or in the framework of the exercise of a public authority assigned to the controller, or the enforcement of the legal interests of the controller or a third party, including profile creation based on the above provisions, any time, for reasons related to his/her own situation. In case of objection, the controller shall not continue to manage the personal data, unless it is justified by compelling legal reasons, which have priority over the interests, rights and freedom of the person concerned, or which connect to the submission, enforcement or protection of legal claims.

In automated decision-making in special cases, including profiling, the person concerned is entitled to be exempted from the effect of a decision based on only automated data control - including profiling -, which would have a legal effect on him or her, or would significantly affect him or her in a similar way.

Right to withdraw

The person concerned shall be entitled to withdraw his/her consent at any time.

Right to appeal to a court

If his/her rights are injured, the person concerned shall be entitled to initiate a legal procedure against the controller. The court will proceed with urgency.

Data protection Authority

The controller shall be liable for damages caused by the processor against the person concerned, and the controller shall pay also any injury fee due to violation of personality rights caused by the data processor. The controller shall be exempted from liability for damages and from the payment of injury fees, if it proves that the damages or the violation of the personality rights of the person concerned were caused by an unavoidable reason beyond the sphere of data management. No damages or injury fees may be claimed if the damages or the violation of the personality rights derived from the intentional or gross negligence of the person concerned. In addition to the above remedies, the person concerned may turn also to the National Authority for Data Protection and Freedom of Information

Name: National Authority for Data Protection and Freedom of Information

Registered office: 1055 Budapest, Falk Miksa utca 9-11

Postal address: 1363 Budapest, P.O.B.: 9.

Phone: 0613911400 Fax: 0613911410

E-mail: ugyfelszolgalat@naih.hu

Website: <https://www.naih.hu>

Other Provisions

We provide details on data management issues not included in this information when the data is recorded. We inform our clients that the court, the prosecutor, the investigation authority, the law enforcement authority, the administration authority, the National Authority for Data Protection and Freedom of Information and other bodies authorised by the law may request the controller to provide information, to disclose data and to supply documents.

Fanos Kft. shall be allowed to disclose personal data to the authorities – if the authority has indicated the purpose and the sphere of data accurately – to the extent which is essential for the purpose of the request.

Based on the provisions of the GDPR, if the Controller does not take measures without any delay, but within one month from the receipt of the request based on Articles 15 to 22 at the latest, the Controller informs the person concerned on the reasons of the failure to take the measure, and that the person concerned may submit a complaint to any supervision authority, and initiate a legal procedure.

Validity: 31 July 2023