
PRIVACY POLICY

Pursuant to 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 referred to as "GDPR") and to Hungarian Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, Földgázszállító Zrt. (hereinafter referred to as „**FGSZ**” or „**Data controller**”) provides you – as the data subject with regard to the processing carried out by MOL in connection with its whistleblowing system – with the following information.

Purposes of the data processing and principles of the ethics procedure:

The primary purpose this Privacy Notice is to provide a description of the data processing activities carried out in connection with the procedures aimed to ensure that people adopt the particular courses of conduct as defined in FGSZ’s Code of Ethics, and a description of the data processing carried out when responding to ethical questions and investigating possible violations of the rules of conduct as well as during proceedings of the Ethics Committee and the Ethics Officer. In ethics procedures, each participant is required to act in compliance with the criteria of objectivity and impartiality, in accordance with the rules laid down in the Code of Ethics and adopt a course of conduct that is in line with the principles of good faith and fairness. In order to protect the personal data of people involved in ethical issues, any document prepared or made available in the course of ethical procedures shall be treated confidentially, unless otherwise provided for in this Notice.

The Rules of Procedure of FGSZ’s Ethics Committee lay down the roles and responsibilities of people involved in procedures aimed to ensure that people adopt the particular courses of conduct as defined in FGSZ’s Code of Ethics – including those involved in whistleblowing management and whistleblower protection as defined in Hungarian Act CLXV of 2013 on Complaints and Public Interest Disclosures, in the section on whistleblowing systems operated by employers –, and also set out rules for responding to ethical issues, for investigating possible violations of the rules of conduct, and for the proceedings of the Ethics Committee and Ethics Officer.

In order to protect the personal data of people involved in ethical issues, any document prepared or made available in the course of ethical procedures shall be treated confidentially, unless otherwise provided for in this Notice.

Any people involved in ethical issues (Members of the Ethics Committee, Ethics Officer, other investigators, whistleblower, person who is the subject of a whistleblowing allegation, witness, experts, etc.) are required to treat all pertinent information confidentially. This shall not cover the right of defence and the right to clarification of the facts of the person who is the subject of a whistleblowing allegation; however, in exercising his or her rights, the person who is the subject of a whistleblowing allegation shall act in compliance with the laws, and among other things, respect personality rights and the right to informational self-determination.

Description of the data processing activity:

Whistleblowers can report regulatory non-compliance, raise ethical concerns or submit ethics related questions in following ways: by completing a form on the FGSZ website (www.fgsz.hu), by telephone ((+36 84) 505-560) or by post (address: Siófok, Tanácsház u. 5, 8600). When the form is submitted, an automatic e-mail is generated about the report and is sent to etikaibizottsag@fgsz.hu. Whistleblowers have the option to submit their

report anonymously. Where the non-anonymous option is chosen, after reviewing the whistleblowing report, FGSZ will notify the whistleblower of the decision and the outcome of the investigation. The Ethics Officer of the Ethics Committee transcribes and keeps records of whistleblowing reports recorded as voicemail. FGSZ's ethical organisational unit decides on ethical issues or complaints, where necessary, after investigating the matter or complaint and gathering evidence from persons and/or entities inside or outside of FGSZ. Throughout the process, the contact details of the whistleblower and the entire content of the report are only accessible to the organisational unit responsible for conducting investigations, and accordingly, the records of whistleblowing reports are protected by access control and stored separately from other systems of FGSZ.

Whistleblowing report and documents generated during the related investigations may include personal and special personal data relating to natural persons.

"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Sensitive personal data" means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Legal basis of the data processing: The legal basis of the data processing is that it is necessary for the fulfilment of legal obligation, the prevention and investigation of misconducts that endanger the assets, trade secrets, intellectual property and business reputation of the data controller, or the proper, respect based, fear and retaliation free working environment and the impeachment of the responsible persons (based on GDPR Article 6 (1) c) and Article 9. paragraph (2) point b) and g)).

Duration of the data processing: Where, based on the investigation, a report is unfounded or no further action is required, any data relating to the report should be erased within 60 days of the completion of the investigation. Where action is taken based on the investigation, including action related to the initiation of legal proceedings or of a disciplinary measure against the whistleblower, any data relating to the whistleblowing may be processed in the employer's whistleblowing system at the latest until the definitive conclusion of the proceedings initiated based on a specific whistleblowing report.

Data security measures:

In order to guarantee the confidentiality, integrity and availability of your personal data, FGSZ stores your data in a password-protected database created exclusively for the Ethics Committee and the Ethics Officer, in accordance with IT security rules and standards.

The Data Controller shall protect the data in the framework of risk-proportionate protection, including network, infrastructure and application level protection (firewalls, antivirus programs, storage and communication encryption mechanisms according to the classification of personal and business data). Data stream cannot be decrypted by content filtering and other technical and process solutions. It constantly monitors and manages privacy incidents.

Your data management rights:

Your data protection rights and remedies, and their limitations are set out in detail in the GDPR (in particular the GDPR 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79 and 82). You may request information about your data at any time, request the correction, deletion or

restriction of your data at any time, or object to the processing of data based on a legitimate interest. The most important provisions are summarized below.

Right to be informed:

If the Data Controller handles personal data concerning you, the Data Controller is obliged to provide you with information on the most important features of data processing, such as the purpose, legal basis, duration, the identity and contact details of the Data Controller and his representative. In the case of data processing based on a legitimate interest, the Data Controller is obliged to inform you of the data controller's and / or third party's legitimate interest, including your rights and remedies (among others the right to complain to the supervisory authority if you do not already have this information).

Access right:

You have the right to receive feedback from the Data Controller as to whether the processing of your personal data is in progress, and if such data processing is in progress, you have the right to access personal data and certain information related to data processing, including the purposes of the processing, the categories of personal data concerned, the recipients of the personal data, the (intended) duration of the processing, the data subject's rights and remedies (including the right to lodge a complaint with the supervisory authority) and, if collected, the source of the data.

Upon your request, the Data Controller will provide you with a copy of the personal data that is the subject of the data processing. The Data Controller may charge a reasonable fee based on administrative costs for any additional copies you request. The right to request a copy must not adversely affect the rights and freedoms of others. Upon request, the Data Controller will provide information on the possibility of issuing a copy, its method, possible costs and other details.

Right to correction:

You have the right to request from the Data Controller, to correct inaccurate personal data concerning you without undue delay. Taking into account the purpose of the data processing, you have the right to request incomplete personal data to be supplemented, also with a supplementary statement.

Right to deletion:

You have the right to request the Data Controller to delete your personal data without undue delay, and the Data Controller is obliged to delete your personal data without undue delay, if certain conditions are met. Among others, the Data Controller is obliged to delete your personal data at your request, if the personal data are no longer needed for the purpose for which they were collected or processed for; if you withdraw your consent on the data processing and there is no other legal basis for the data processing; or personal data was processed unlawfully; or you object to the processing and there is no other prioritized legitimate reason for the processing; personal data must be deleted in order to fulfil the legal obligation the European Union or Member State law; personal data was collected in connection with the provision of information society services.

Right to restrict data processing:

You have the right to request the Data Controller to restrict the data processing if one of the following is met:

- a) You dispute the accuracy of the personal data. In this case, the restriction applies to the period of time that allows the Data Controller to verify the accuracy of the personal data;
- b) The processing is unlawful and you object to the deletion of the data and instead request a restriction on their use;

c) The Data controller no longer needs the personal data for the purpose of data processing, but you request the data in order to make, enforce or protect legal claims;

d) You have objected to the data processing; in this case, the restriction applies for the period until it is determined whether the legitimate reasons of the Data Controller has legal priority over your legitimate reasons.

If the processing is subject to restrictions as per above, personal data may only be obtained with your consent, with the purpose to enforce or protect legal claims, to protect the rights of another natural or legal person or in the important public interest of the Union. (Exception from this is data storage).

If the data management restriction is lifted, the Data controller will inform you in advance.

Right to object:

You have the right to object against the processing of your personal data, which is in the legitimate interest of the Data controller for reasons related to your situation.

In this case, the Data Controller may not further process the personal data, unless the Data controller can prove that the data processing justified by compelling legitimate reasons, which take precedence over your interests, rights and freedom, or which are required to enforce or protect legal claims. If you exercise your right to object, the Data controller will examine whether the objection is well-founded.

The rights of the data subjects related to data management can be found in the general Privacy Policy on the website www.fgsz.hu.