

PRIVACY POLICY

- GREEN ACCESS -

This Policy regarding the processing of personal data (hereinafter referred to as "*the Policy*") details when and why we, **TIRIAC IMOBILIARE**, meaning

- **MASTERANGE ROMANIA S.R.L.** based in Bucharest, Nordului Road, no. 24-26, 2nd floor, room 25, 1st District, registered at the Trade Register under no. J40/3330/2003, CUI 15262492,
- **GERES REAL ESTATE S.R.L.**, headquartered in Bucharest, Nordului Road, no. 24-26, 2nd floor, room 16, 1st District, registered at the Trade Register under no. J40/20491/1994, CUI 6435888,
- **GLOBAL EAST EUROPEAN INVESTMENT S.R.L.** ., headquartered in Bucharest, Nordului Road, no. 24-26, 2nd floor, room 17, 1st District, registered at the Trade Register under no. J40/5836/2011, CUI 28472658

individually referred to as "*the Controller*", as independent Controller, process your personal data through the Green Access application (hereinafter referred to as "*Green Access*" or "*the Application*"), your data protection rights and how you can exercise these rights.

This Policy addresses to any user that installs and uses Green Access, hereinafter referred individually as the "*data subject*".

For any information or request regarding the processing of personal data covered by this Policy or for the exercise of your rights, you may contact us by using the following contact details:

Address: Nordului Road, no. 24-26, 1st District, Bucharest

Email Address: dataprotection@tiriacimobiliare.ro

I. HOW WE USE PERSONAL DATA. STORAGE PERIOD.

Green Access is an application that issues virtual access cards to facilitate and secure access to our buildings.

When you choose to use a virtual card, your data is processed as follows:

1. Download the Application from the online store (App Store or Google Store) and activate the Application in the presence of our representative.

After downloading and starting the app, Green Access will ask for your consent to query the Bluetooth / location. The query is required for Green Access to connect to the application available on our representative's device in order to activate your right of access. Activation of the access right is achieved by communicating unique identifiers between the two applications.

Unique identifiers will be stored until you deactivate the Application. New identifiers are assigned when you reinstall the Application. We will not store data about your location.

This data is processed exclusively for the operation of the Application, so that you can use it. Thus, the legal basis of the processing is represented by the provision of a service, according to art. 6 para. 1 lit. b) of the GDPR, respectively your agreement for accessing the Bluetooth / location, according to art. 6 para. 1 lit. a) of the GDPR.

2. Using the Application to access the building

When you use the virtual card to access a building, the access control equipment will query the unique identifiers assigned to grant access and record the date and time of entering the building.

The registration of access rights (name, surname, the company you represent, the unique identifier assigned by the system, access rights) and information regarding the access (date and time of entry into the building), is done through the systems / equipment managed by each Controller, individually.

The management of the access in the building is carried out in order to ensure the security of the objectives, goods, values and protection of the persons according to Law no. 333/2003. The data is kept according to the internal policies of each Controller, as well as in accordance with the applicable legal provisions. More information on these processing operations will be made available to you, separately, by each Controller.

In addition, we will process your personal data listed above to protect our systems and ensure their maintenance. In this case, the processing is performed in order to achieve our interest in ensuring the proper functioning of information systems.

In the event of a dispute, we will keep the data in accordance with the applicable limitation periods.

Subsequently, we will delete or erase the personal data from our systems and / or take steps to anonymize them so that you can no longer be identified.

II. RECIPIENTS OF PERSONAL DATA

Personal data may be disclosed, strictly to the extent necessary for the purposes detailed above or in cases where this is required by law or we have a duly justified legitimate interest, to the following categories of recipients who may have the status of independent controllers / joint controllers or processors, as follows:

- a.** Services providers, such as:
 - business administration and consultancy services,
 - personal data protection services,
 - system maintenance services,
 - security audit and IT infrastructure services.
- b.** External consultants we contact in specific situations (for example, lawyers, experts, other advisers).
- c.** Public authorities and bodies, respectively investigative bodies, and courts, insofar as the transmission of data to them is required by law and / or is necessary in case of litigation or settlement of a dispute, as well as in case of controls in which we have the obligation to make them available (for example, tax authorities, ANSPDCP).
- d.** Parties expressly indicated by you.
- e.** Third party acquirers, to the extent that our business would be transferred (in whole or in part) and the data of the data subjects would be inherently linked to the assets that are the subject of such a transaction.

III. TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

We will not transfer your personal data outside the European Economic Area. In exceptional cases and only if necessary, the transfer of your personal data outside the European Economic Area will only be done with the application of appropriate protection measures in accordance with the specific legal provisions on the protection of personal data and with your appropriate information.

IV. YOUR RIGHTS

Unless otherwise provided by law, you have the following rights with respect to your personal data:

a. Right to access data

By exercising this right, you can obtain confirmation from us that we are processing your personal data, as well as a copy of them and providing information about the processing conditions.

The answer to the request for access will be sent to you within a maximum period of one month from the date of the request. In special conditions this period may be extended up to two months, in which case we will inform you about the extension.

b. Right to rectification

By exercising this right, you can request the rectification / correction and / or completion without undue delay of inaccurate and / or incomplete personal data. Please note that any rectification will be made within a maximum period of one month from the date of the request. Under special conditions provided by the Regulation, this period may be extended to a maximum of two months, in which case we will inform you of the extension. In this regard, you may be required to provide the necessary documents for rectification or updating.

If you notice that some of your data are incorrect, please inform us as soon as possible using the contact details mentioned in the introductory part of this Policy.

c. Right to erasure / the right to be forgotten

You have the right to request us, and we have the obligation to delete personal data processed without undue delay in the following cases:

- your personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you have withdrawn your consent on the basis of which the processing takes place, in accordance with art. 6 of the GDPR and there is no other legal basis for processing;
- you object to the processing pursuant to Article 21 (1) of the GDPR and there are no overriding legitimate grounds for processing, or you object to the processing under Article 21 (2) of the GDPR;
- your personal data have been unlawfully processed by us;
- your personal data have to be deleted in order to comply with a legal obligation incumbent on us under Union or national law to which we are subject.

When we can deny the request to delete data:

- processing is necessary for the exercise of the right to freedom of expression and information;
- processing is necessary to comply with an applicable legal obligation;
- for reasons of public interest in the field of public health, in accordance with Article 9 (2) (h) and (i) and Article 9 (3);
- the processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, under the conditions of the GDPR, insofar as the exercise of the right may make it impossible or seriously affect the achievement of the processing objectives;
- processing is necessary to establish, exercise or defend a right in court.

d. Right to restriction

"Restriction" means that - except for storage - your personal data may be retained but may be processed only with your consent or for the establishment, exercise, or defence of a right in court or for the protection of the rights of another natural or legal person, public interest of the EU or of an EU Member State.

This right shall apply if:

- you dispute the accuracy of your personal data,
- the processing is unlawful, and you oppose the deletion of personal data, instead requesting the restriction of the processing,
- we no longer need your personal data, but you request that it be kept for you to establish, exercise, or defend a right in court,
- you have objected to the processing, for the time period in which it is verified that our legitimate interests in the processing of personal data prevail over your rights.

e. Right to object

You have, for reasons related to your particular situation, the right to object to processing carried out for the purpose of our legitimate interests, unless we demonstrate that we have legitimate reasons to process your data, which prevails over interests, rights, and freedoms. or to establish, exercise or defend a right in court.

Please also keep in mind that you can object at any time, free of charge and without any justification, to the processing of your data for direct marketing purposes, including the creation of profiles for this purpose.

f. Right to data portability

You have the right to receive the personal data, which you have provided to us for the purposes shown, in a structured, commonly used and automatically readable format, as well as the right to request that we send this data to another controller (only if this transmission is technically feasible), if the processing is based on consent or a contract and the processing is carried out by automatic means.

g. The right not to be subject to a decision based solely on automated processing, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which has legal effects on you or affects you in a similar manner, unless such processing is necessary for the performance of the contract, is permitted by law or is based on your explicit consent.

Without prejudice to your right to contact at any time the public authority for the processing of personal data, please contact us in advance regarding the exercise of your rights mentioned above by sending a written request to the contact details. indicated in the introductory part of this Policy.

h. Right to withdraw your consent

This right applies if your data is processed as a result of the consent expressed, in which case you have the possibility to withdraw your consent. Withdrawal of consent does not affect the lawfulness of the processing carried out on the basis of the consent before its withdrawal.

Without prejudice to your right to contact at any time the public authority supervising the processing of personal data, please contact us in advance in connection with the exercise of your rights mentioned above by sending a written request to the contact details. indicated in the introductory part of this Policy. If you consider that the processing of your data is carried out by the Controller in violation of the legislation in force, you also have the following rights:

- **the right to file a complaint with ANSPDCP** (National Authority for the Supervision of Personal Data Processing having the following contact details:
Headquarters: Bucharest, Bdul Gen. Gheorghe Magheru no. 28-30, sector 1, CP 010336
Phone: +40.318.05.92.11
Fax: +40.318.05.96.02
Email: anspdcpc@dataprotection.ro
Website: www.dataprotection.ro
- **the right to take legal action.**

Please note that if we have doubts about the applicant's identity as a data subject, we may request additional information to confirm the identity.

V. KEEPING YOUR PERSONAL INFORMATION SECURE

Masterange will make every reasonable effort to protect your personal data in its possession or control by establishing reasonable security measures to prevent unauthorized access, collection, use, disclosure, copying, modification or deletion of your data, and other similar risks.