SECURITY POLICY

OF PERSONAL DATA PROCESSING

1. Identify and authenticate the user

Authorized users' access to the personal database is accessed by typing the username and password for each user. Passwords are confidential and are regularly exchanged every 6 months by our Company's IT Department. If the password was entered incorrectly 5 times in a row, the system will automatically lock the user account.

If a user's work contract ceases in any way (including as a result of dismissal or resignation) or the user will be absent from work for a long period of time, his account will be deactivated by our Company's IT Department, which is authorized to do so.

2. Type of access

Users only have access to the personal data needed to fulfill their service duties. The type of access is set for each user depending on the functionality (administration, input, processing, saving, etc.) and the actions applied to personal data (write, read, delete).

Our IT Department has access to personal data to solve exceptional cases (for example, recovering erroneous data by mistake, solving technical problems in the system, etc.).

3. Data collection

Our company designates authorized persons to collect personal data and enter them into the Company's information system. Our Company's information system records the identification data of people who have made changes to the database and the date and time at which these operations were performed. Deleted and modified data is also retained.

4. Making safety copies

The backup of the personal database is performed daily by our Company's IT Department. They are kept in rooms separated from spaces where personal data is stored or operated and access to them is restricted.

5. Computers and access terminals

Computers are installed in restricted rooms. If personal data is displayed on the monitor that does not work for 20 minutes, the session is automatically closed. Our company recommends that users use the "log off" option before leaving the computers they use for more than 10 minutes. Computers used in the relationship with the public, on which personal data are displayed, are positioned so that the displayed information can not be seen by the public.

6. Access files

Any access to the personal database is recorded in the applications used. The information recorded is the following: - the identification code of the person who has accessed the personal database; - the type of operation performed; - date of access (year, month, day); - time of access (hour, minute, second).

Records of the history of database access are kept for at least 2 years to be used as evidence in case of investigations. If investigations are prolonged, this information will be retained as long as it is deemed necessary.

7. Telecommunication systems

Verification of the functionality of programs processing personal data as well as the type of user access is made regularly by the IT Department of our Company. Access to personal data outside the Company's headquarters is through a secure VPN channel that uses encryption of transmitted data.

8. Staff training

Users who have access to personal data are trained on the provisions of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, the minimum security requirements for the processing of personal data, the risks to personal data processing, as well as the confidentiality On them. The information system displays a warning message on the monitor when the personal data section is accessed. At the end of the work program, each user is required to close his work session.

9. Using computers

In order to maintain the security of personal data, the following measures are adopted: - the preparation of the computers for use only by the IT department of our company; - Users do not have the right to install software on their computers; - each computer has an antivirus program installed; - The PrintScreen key is automatically disabled when personal data is displayed on the monitor, and the printer is forbidden to print.

10. Printing the data

The removal of the personal data from the printer is done only by the authorized users in this respect and only if it is strictly necessary, the printed documents being classified as confidential documents for internal use. If the use of printed documents containing personal data is no longer required, the persons who used them will proceed to their destruction, according to the Database Access Rules prepared at our Company level.