

PRIVACY POLICY

1. INTRODUCTION

This Personal Data Protection Policy (**Policy**) provides information on the processing and protection of personal data by the company GAURUS d.o.o., with headquarters in Zagreb, VAT ID: 87359785969 (**Company**) as a data controller, which data are processed as part of the Company's operations.

The personal data to which this Policy applies are all information relating to an individual - an identified or identifiable natural person (the **data subject**), either directly from individual personal data or indirectly, or through a combination of several personal data items (e.g. first and last name, PIN, residential addresses or e-mail addresses, etc.). The processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated (computer) means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

The processing and protection of personal data processed by our Company is carried out in accordance with the applicable General Data Protection Regulation (GDPR), the applicable and other regulations for the protection of personal data, as well as this Policy.

In connection with the application of the aforementioned regulations, as well as for provision of detailed information on the method of processing and protection of personal data that we process, below we provide information on the type of personal data that we process, the purposes of their processing, the legal basis for their processing, the recipients with whom we share them or could share them, the method of processing and the time of their storage and protection, the rights of data subjects in relation to the processing of personal data, and information about the Company's actions in the event of breach of the personal data it processes.

2. ABOUT US

GAURUS d.o.o., VAT ID: 87359785969, is a limited liability company registered in the Court Register of the Commercial Court in Zagreb under company registration number (MBS): 081062229. Company headquarters are located in Zagreb, the Company business address is Jablanovac 27, and the Company office is located at Koturaška 69. The Company develops specific software solutions for the public and private sector with a focus on real-time data processing and modern machine learning technologies applicable to fintech and transaction data processing.

The Company holds all necessary certificates issued by the Croatian National Bank, based on which it is authorized to develop software solutions and provide services related to the processing of financial data.

In relation to personal data processing to which this Policy applies, the Company acts as the controller, which means that it independently determines the purposes and means of personal data processing.

3. PERSONAL DATA WHICH WE PROCESS

When providing services, as well as in business operations in general, and in situations where applicable regulations require us to do so, the Company collects and processes certain personal data that we need to fulfill legal obligations. We also process the personal data of our potential clients and persons with whom we cooperate when fulfilling our contractual obligations, as well as the personal data of our employees and

persons applying for work at our Company. To the extent which is necessary to achieve a specific purpose, for example viewing the content of our services, the Company also collects personal data of visitors to Company websites (www.gaurus.hr, www.f-iq.app) and Company pages on social networks.

As part of Company operations, special attention is paid to the fact that all personal data that we need are collected to the minimum extent necessary to achieve the purpose, always in accordance with the purpose for which they were collected, as well as that these data are kept only for the time allowed or necessary, and that they are always adequately protected during processing and storage.

We especially note that the collection of certain personal data is essential for the execution of the services we provide to our clients, as well as for the compliance of our Company's actions with applicable regulations. Preventing the collection of these personal data may therefore prevent us from providing the aforementioned services, or may lead to our Company having to refuse to perform some of the services. In any such situation, we will warn the data subject of this possibility.

In certain situations when, in connection with the provision of services, we will have to contact or engage certain third parties according to the order and in agreement with the client (e.g. insurance companies, accountants, auditors, consultants, banks, lawyers, notaries public, tax advisors), such third parties could, due to the legal provisions that apply to their business operations, request from our Company the delivery of personal data that we have collected from our clients. We will, at our own discretion, provide the requested personal data to such third parties, taking into account all the requirements for the protection of such data, unless the client has expressly prohibited us from doing so in advance. Considering the above, if there are any third parties to whom our clients do not want us to provide personal data, it is necessary to inform us in advance.

As a rule, we collect all personal data directly from the data subject, but sometimes we also collect certain personal data from third parties, such as the bank where the data subject has an account or from the so-called data brokers such as Google and similar operators who arrange personal data processing themselves, whom the client addresses directly and independently of the business relationship with the Company.

We process and protect personal data that we collect from a person who is not a data subject to whom the personal data refers in the same way as those data which are collected directly from the data subject.

For the personal data of data subjects that we collect from third parties, whom the client addresses directly and independently of the business relationship with us, we will consider them accurate and lawfully processed by that person. We will not specifically check the above assumption, unless it is stated otherwise in this Policy for certain personal data or if there is a justified reason for this.

We specify the personal data that our Company collects and processes below.

A. PERSONAL DATA WE PROCESS AS PART OF SERVICE PROVISION AND BUSINESS OPERATIONS

In order to provide services, improve our services and carry out the education of our employees, and in order to ensure the general operations of the Company, we primarily process personal data of our business partners (users of our services, suppliers), but also of third parties such as bookkeepers, accountants, auditors, tax advisors, authorized translators, experts, lawyers, IT service providers, visitors to our premises, namely natural persons and directors, representatives, employees, associates and other persons who act on behalf of our partners who are legal entities (e.g. their shareholders, members, or persons associated with those persons).

The personal data that we process for these purposes refer to: name and last name, personal identification, registration or other appropriate number under which they are entered in official registers, telephone, mobile or fax numbers, e-mail addresses, IBAN and other bank account and transaction information, IP address as well as all other data that are relevant for the specific service we provide, the business

relationship and/or payment for services performed. At the explicit request of the data subject, we can also process other data that we do not need to provide services, such as images or photographs.

The Company will process the IBAN and other data from the data subject's bank accounts and transactions only and exclusively if and when it receives such a request from the data subject and if the data subject has previously instructed their bank to provide this information to the Company.

Given that the provision of our services requires the processing of specific data concerning bank accounts and transactions, i.e. the management of financial assets, and given that certain parts of the analysis of these data are carried out through automated data processing, we use the mentioned personal data in order to create a client profile, without which we cannot ensure the provision of our service. For the above reasons, the Company regularly assesses the efficiency of personal data protection measures and tests the vulnerability of the entire system, in order to ensure complete protection of all personal data.

It is especially noted that the Company, within the framework of its services, which includes profiling, does not make any decisions that would produce legal effects for the data subject or similarly affect them to a significant extent. The results of the services provided by the Company are always used exclusively by the data subject themselves, who decides on all further actions with these results, for example whether they will be submitted to a bank or other financial institution for further action. The company will deliver said data to banks or other financial institutions only and exclusively based on the express written instructions of the data subjects.

Bearing in mind that our services serve data subjects to increase personal responsibility in the management of personal finances and further communication with financial institutions, it is necessary that the Company provide its services at the highest level, which requires continuous training of the Company's employees. Such training is conducted exclusively on the Company's internal systems, and personal data are not shared, forwarded or disclosed to other persons outside the Company. Therefore, with the consent of the data subject, we use personal data even after the service has been performed for the purpose of training employees and improving our service in general.

As part of our business, we participate in numerous professional and business conferences, seminars and similar gatherings in order to continuously improve our professional knowledge and expand contacts in the business community. Also, due to the nature of our work, we communicate face-to-face and in writing with the members of the business community in order to establish, maintain and improve business contacts and relationships. During the aforementioned communication with the mentioned persons, we exchange business cards, e-mails, as well as written correspondence, which leads to the processing of certain personal data mentioned above.

We will ask every client or business partner to whom we want to send our promotional material or contact them as part of a marketing campaign of our Company for their consent to use their personal data for the stated purposes, or we will base the processing of personal data for the stated purpose on the legitimate interest of the Company.

All our services are intended exclusively for adults, i.e. people who are able to open bank accounts and manage their finances independently. For this reason, we can ask potential clients who use our services to declare or confirm that they are of legal age and that they are authorized to request the aforementioned services.

The company has also developed games that are intended for children or persons under the age of 16, which can be downloaded exclusively through Google Play and App Store platforms, in accordance with conditions set by said platforms. The company does not and will not offer games and/or other services directly to children or persons under the age of 16 on its websites.

B. PERSONAL DATA OF EMPLOYMENT CANDIDATES, WORKERS AND MEMBERS OF THE MANAGEMENT BOARD AND RELATED PERSONS

In order to fulfill its obligations arising from employment relationships, the Company, as an employer, processes the following personal data of employees: name and last name, address of permanent (or temporary) residence, personal identification number, place and date of birth, user names on internal servers, professional education and special exams and/or courses which are the prerequisite for performing the job (including certificates, licenses, etc.), jobs/functions they perform, telephone, mobile or fax numbers, e-mail addresses, information on identity documents (identity card, passport, etc.), information on marital status, information on the number and age of children and other persons supported by the worker (including first and last name, address of permanent (or temporary) residence, personal identification numbers and dates of birth of these persons), information on bank accounts, public and private documents issued by competent authorities relating to workers (certificates of health and pension insurance, etc.), salary data, salary supplements and all other data on workers the employer must keep. The Company will also collect the aforementioned data from the members of its management board with whom it has concluded employment contracts, while from those members of the management board with whom it has concluded service contracts (management contracts), it will collect only those of the aforementioned data that are necessary for the fulfillment of the Company's obligations arising from those contracts.

The Company also processes personal data of employees and members of the management board regarding their health status. These data are processed only and exclusively for the purpose of fulfilling the Company's legal obligations related to the determination of temporary or other incapacity for work and the payment of appropriate salary compensation or checking whether the health status of the specified persons meets the needs of the workplace/function they perform, and they will not be used for any other purpose.

Furthermore, if necessary, the Company processes the personal data of employees and members of the management board related to misdemeanor and/or criminal proceedings against the aforementioned persons, when these acts were committed in the performance of work/function in the Company or in connection with that work/function. These data are processed only and exclusively for the purpose of exercising and fulfilling the Company's rights and obligations arising from employment contracts/management contracts and possible recourse claims of the Company towards these persons, and they will not be used for any other purpose.

We process the personal data of the employee's dependents and other related persons exclusively for the purpose of fulfilling our legal obligations in the field of labor law and for the purpose of calculating and paying benefits in addition to the salary that the employee receives according to special regulations or internal acts of the Company (gifts for children, Christmas bonus, etc.) and will not be used for any other purpose.

During the recruitment process in our Company, we collect CVs and other appropriate documentation (applications, registrations, references, diplomas, certificates, decisions, etc.) from candidates, which usually contain their personal data. We receive the aforementioned documentation from candidates on the basis of tenders/calls that we have advertised or through open applications, and we check the information contained in them in publicly available sources. Also, in order to help in the recruitment process (sorting and evaluation of candidates), the Company may, if necessary, hire third parties (employment agencies, external consultants) who will process the personal data of the candidates according to the Company's instructions.

The personal data of employment candidates that we process are the following: name and last name, address of permanent (or temporary) residence, photo, personal identification number, place and date of birth, information about current and previous employment, information about education, telephone, mobile or fax numbers, e-mail addresses, as well as all other data that are relevant for employment at a

certain position, where we especially emphasize data on the candidate's health status in order to check whether the candidate's health status meets the needs of the position/function.

Any candidate who is not selected for the specific position for which they applied, but we consider them a candidate for employment in the Company in the future, will be asked to give consent to the processing of personal data for the purpose of future job vacancies, i.e. employment at another position in the Company.

4. PURPOSE OF PERSONAL DATA PROCESSING

The company processes the aforementioned personal data for the following purposes:

- provision of services;
- fulfillment of the Company's legal obligations;
- facilitating the Company's regular operations;
- service improvements and employee training;
- maintaining business contacts;
- fulfilling Company obligations towards employees and members of the Company's management board;
- employment of new workers and other persons in the Company;
- Company advertising and providing related information to our business partners;
- contacting data subjects when necessary and appropriate (e.g. when data subjects send inquiries about our services);
- collection of Company claims;
- protection of persons and Company assets;
- marketing and promotion of certain products.

After the personal data are no longer needed to fulfill the purpose for which they were collected or for other purposes for which the Company processes them, we will destroy or anonymize them so that the identification of a data subject is no longer possible.

5. LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

The legal basis for the processing of personal data, in order to fulfill the aforementioned purposes, includes:

- processing of personal data necessary for the performance of the Company's contractual obligations towards data subjects, or for carrying out certain actions at the request of data subjects before concluding a contract (e.g. in case of providing services, in case of executing other contracts to which the Company is a party, including negotiations for the conclusion of these contracts);
- processing of personal data for the purpose of fulfilling legal obligations that the Company is obliged to comply with (e.g. keeping accounting data, keeping data necessary for the exercise of employee rights in connection with the employment relationship (records on employees, records on working hours, etc., which also applies to management board members correspondingly);
- the consent of data subjects (e.g. for conducting trainings, for sending Company promotional materials or conducting other marketing actions of the Company, as well as in case of employment candidates who give their consent to the storage of their personal data for future job vacancies)
- legitimate Company interest (e.g. contacting persons with whom the Company should cooperate in connection with the provision of services, maintaining business contacts, sending promotional material of the Company or conducting other marketing actions of the Company).

6. PERSONAL DATA PROCESSING THROUGH VIDEO SURVEILLANCE

In order to protect people and the Company's property, certain premises of the Company may be recorded by surveillance cameras, and by conducting such video surveillance, the personal data (physical appearance

recorded on the video) of all data subjects who enter the recording (surveillance) area are processed. These personal data are used only and exclusively for the purpose specified under this item.

In the event that video surveillance is carried out, before entering the surveillance camera recording area a sign will be placed showing that a certain area is under video surveillance, and this sign will contain all other information prescribed by positive regulations.

The right to access personal data collected through video surveillance is exclusively available to responsible persons of the Company and/or persons authorized by said persons, as well as to competent state authorities as part of the performance of tasks within their scope of activities established by law.

The Company will not keep recordings obtained through video surveillance for longer than six months, unless these recordings serve as evidence in court, administrative, arbitration or other equivalent proceedings, or unless longer storage is prescribed by a special law.

7. RECIPIENTS OF PERSONAL DATA

The company will not pass on, provide access to, or otherwise make available the data subjects' personal data to third parties, with the exception of the persons specified in this Policy and in the event that it is mandatory to do so in accordance with binding regulations.

The company can provide personal data or provide access to:

- banks with which the data subject has an open account according to the instructions of the data subject;
- providers of financial security assessment services, in order to prevent fraud;
- public authorities (courts and administrative bodies), authorized translators, experts, lawyers, tax advisors, counterparties in court or other proceedings or the representative/proxy of the counterparty in the proceedings, companies dealing with the purchase of claims, all for the purpose of providing services and exercise of property and other rights of the Company;
- IT service providers hired by the Company for maintenance and protection of information technology and the Company's information systems;
- persons hired by the Company to perform accounting, bookkeeping and/or auditing services;
- other persons specified under item 3 of this Policy.

The Company cooperates with appropriate service providers in order to carry out advertising activities, to analyze the use of our websites and applications, and to monitor the efficiency of campaigns. In doing so, we share personal data only to the extent necessary to perform the service on our behalf. Providers of the aforementioned services required for cooperation:

- Google – Google Analytics and Firebase are used to track web statistics, demographics and web user behavior. We use it to monitor the efficiency of our marketing campaigns. You can find more information under item 14 of this Policy.

8. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

The Company will not transfer personal data to third countries (non-EU countries) or international organizations.

In the event that there is a need to transfer personal data to third countries or international organizations, the Company will ensure an adequate level of protection of the data subjects' personal data by applying permitted measures, for example approved standard clauses on the protection of personal data in the contract concluded between the Company and the third-country data controller or data processor.

9. PERSONAL DATA STORAGE PERIOD

We store personal data only for the period necessary to achieve the purpose for which these personal data are collected or for the period prescribed by positive regulations.

We store the data collected within the scope of the Company's operations for as long as the corresponding contractual relationship with the Company lasts, and after that for as long as prescribed by the statute of limitations for claims under certain types of contracts or for claims for indemnification.

We store certain data in accordance with special regulations governing the mandatory storage period. We are obliged to store accounting documentation and all personal data contained in it for a period of 11 years.

We are obliged to permanently store the employee data that we process in accordance with paragraph B of item 3 of this Policy, of which we keep employee records. Furthermore, according to applicable law, we are obliged to store the data from the records of workers who are temporarily hired-out, persons undergoing professional training, full-time students employed through the student service, full-time students who perform their work through authorized high school institutions or institutions for vocational education, persons performing community service work, if they are employed in any of the above ways, for at least 6 years after their work was discontinued, while we are obliged to store the data on the working hours of the workers for at least 6 years, and in the event of learning about a labor dispute in which the working hours records could contribute to the exercise of employee's rights arising from the employment relationship or in connection with it, we are obliged to store data for a longer period, i.e. until the final conclusion of such a dispute.

After the personal data are no longer needed to fulfill the purpose for which they were collected, we will destroy or anonymize them so that the identification of a data subject is no longer possible.

10. RIGHTS OF DATA SUBJECTS

Data subjects whose personal data we process, with the exceptions determined by regulations on personal data protection specified below, have the following rights in relation to the processing of personal data:

- the right to request confirmation as to whether we are processing personal data, and if we are processing them, the right to access this personal data and other information about the processing, with the possibility of submitting a written notification about this (**right of access to personal data by data subjects**) - Annex 1;
- the right to request the rectification of incorrect personal data and/or to have incomplete personal data completed (**right to rectification**) - Annex 2. We ask data subjects to notify us in a timely manner of any change in the personal data that we process using the specified form or through the contact information specified under item 13 of this Policy;
- the right to request the erasure of personal data without undue delay (**right to be forgotten**) - Annex 3, if:
 - the personal data are no longer necessary in relation to the purposes for which they were collected,
 - the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing,
 - the data subject objects to the processing of data based on legitimate interest or for the purposes of direct marketing, which includes profiling,
 - it has been determined that personal data have been unlawfully processed,
 - the personal data have to be erased for compliance with the Company's legal obligations prescribed by applicable law,
 - personal data have been collected in connection with the information society offer to a child.

Notwithstanding the aforementioned provisions, it is not possible to request the erasure of personal data if the data are necessary:

- for exercising the right of freedom of expression and information

- for compliance with a legal obligation in accordance with the applicable law and for the needs of public interest, especially in the area of public health,
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, with the mandatory application of personal data protection measures,
- for the establishment, exercise or defense of legal claims;
- The **right to withdraw consent** to personal data processing, if consent is the legal basis for personal data processing, provided that the withdrawal of consent does not affect the lawfulness of processing that was based on consent before its withdrawal;
- the right to request restriction of data processing, specifically in the event that (i) 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, (ii) the processing is unlawful without a request for the erasure of the personal data, (iii) the processing on the grounds of our legitimate interests was objected to, until verification that our legitimate processing interests override the interests, rights and freedoms of the data subject, and in the event that (iv) if the personal data are no longer needed for processing, but they are required by the data subject for exercise/defense of legal claims (**right to restriction of processing**) - Annex 4;
- the right to transmit the personal data to another controller if the processing is based on consent or a contract to which the data subject is a party, by direct transmission between the Company and another controller if this is technically feasible (**right to data portability**) - Annex 5;
- the right to object to personal data processing if the processing is based on our legitimate interest or is carried out for direct marketing purposes, which includes profiling (**right to object**), and the objection can be submitted to the Company at any time and free of charge;
- the **right to lodge a complaint** with a supervisory authority responsible for the application and compliance with regulations on the protection of personal data, namely the Croatian Personal Data Protection Agency, (hereinafter: AZOP);
- The **right of the data subject 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, unless the decision: (i) is necessary for entering into, or performance of, a contract between the data subject and the Company, (ii) is authorized by Union law or the law of the Republic of Croatia and which also lays down suitable measures to safeguard the data subjects' rights and freedoms and legitimate interests of the data subject, (iii) is based on explicit consent. In the cases referred to in this item under (i) and (iii), the Company shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests by ensuring in any event the **right to obtain human intervention** by the Company's employees, the **right to express his or her point of view** and the **right to challenge the Company's decision**.

In order to facilitate and accelerate the exercise of the above-mentioned rights of the data subjects, the Company has prepared forms for individual rights that are attached to this Policy. The Company will process any request for the exercise of any right of the data subject, regardless of whether it was submitted to the Company on the specified form or in any other way.

If the data subject decides to exercise one of the above-mentioned rights, the Company will, at the request of the data subject, provide the requested information 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 Company shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the Company has reasonable doubts concerning the identity of the natural person making the request, it may request the provision of additional information necessary to confirm the identity of the data subject.

Any data subject can submit a request to exercise all of their rights at any time and free of charge. However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may:

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

11. SECURITY OF PERSONAL DATA

In order to fulfill our obligations in accordance with the applicable regulations on the protection of personal data, we implement technical and organizational measures to protect personal data against accidental loss, destruction, unauthorized access, unauthorized alteration, unauthorized publication and any other misuse.

We protect our computer system at all times with appropriate antivirus, antispyware and antimalware software, as well as a suitable firewall and regular operating system updates. In addition, whenever possible due to business processes, we use pseudonymization for additional protection of personal data.

We have also organized the protection of the computer system by using passwords on official computers that are used in business operations, and said passwords are themselves protected by a special system. Access to data is limited only to persons who are authorized to process certain data and only to IP addresses or devices that have been verified as part of the Company's internal network, and we regularly backup computer data systems that are encrypted.

In particular, it should be noted that the Company regularly assesses the efficiency of technical measures to protect personal data, as well as system vulnerability testing, which checks the resistance of protective measures, and all protective measures are adjusted, if necessary, based on the results of this testing.

We also implement physical measures to protect personal data, which include: protected rooms with limited access, use of security alarms and locks, availability of fire extinguishers with instructions for use in the immediate vicinity of the mentioned rooms.

All employees of the Company have been informed and educated about the provisions of applicable regulations on the protection of personal data and about the obligation to comply with them and the manner of their implementation. All employees of the Company have assumed the obligation to preserve the confidentiality of all the data they process.

12. FURTHER PROCESSING OF PERSONAL DATA FOR OTHER PURPOSES

In the event that there is a need to process personal data for another purpose, different from one of the purposes stated in this Policy, before the start of such processing, the Company will provide the data subjects with information about the other purpose and all other necessary information, and if this is required in accordance with the relevant legal regulations, the Company will request consent for the processing of personal data for another purpose.

Please note that it is possible to differentiate the content of such a new notification in relation to this Policy, taking into account possible changes in legal regulations and business practices over time.

13. BREACHES, COMPLAINTS AND INQUIRIES

Personal data breach means a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access TO personal data that has been transmitted, stored or otherwise processed.

In the event of a personal data breach, the Company will assess the risk to personal data that has arisen as a result of the breach without undue delay, and if this is feasible no later than 72 hours after becoming aware of the breach, and notify AZOP of the personal data breach, unless the risk assessment has

determined that it is unlikely that the personal data breach will cause a risk to the rights and freedoms of the data subject. If the AZOP reporting is not done within 72 hours, the reasons for the delay will be explained.

When assessing the existence and level of risk, the Company will take into account the type of breach (loss or unauthorized access and/or copying of data), the type, sensitivity and amount of data affected by the breach, especially whether the breach may lead to identity theft, how easy it is to identify the subject through the data included in the breach, how severe the consequences of the breach are for the data subject, especially depending on whether it is sensitive data and the manner of the breach which may be accidental by the controller/processor of the processing or intentional by a third party, as well as the characteristics of the data subjects and the number affected by the breach, as well as on the characteristics of the Company, as the controller. When assessing the risk, the Company will be guided by the rules of the European Union Agency for Cybersecurity (ENISA) on assessments of the severity of personal data breaches.

In the event of a personal data breach which, according to the conducted risk analysis, is likely to cause a high risk to the rights and freedoms of the data subject, the Company will also notify the data subject of the personal data breach, unless:

- appropriate technical and organizational protection measures have been implemented, and these measures have been applied to personal data affected by the breach, especially those that render the personal data unintelligible to any person not authorized to access them, such as encryption,
- subsequent measures have been taken to ensure that it is no longer likely that a high risk to the rights and freedoms of data subjects is no longer likely to materialize (the Company managed to take actions that prevented the use and further sharing of personal data),
- notifying the data subject would involve disproportionate effort (e.g. the data subject's contacts were lost due to the breach, and this was made public or communicated to the data subject). In this case, public notification or a similar measure will be necessary to inform the data subjects in an equally effective way.

When necessary, the notification of the breach will be delivered to the data subjects by direct communication (e-mail, letter), separated from other notifications, or if this is not possible due to the breach, a public notification or a similar measure will be carried out, thereby informing the data subjects in an equally effective way.

The Company will document all personal data breaches, including the facts related to the personal data breach, its consequences and measures taken to remedy the damage.

In case of any inquiries, requests and complaints, feel free to contact our Company via the following contact details:

- address **GAURUS d.o.o.**
Jablanovac 27
10 000 Zagreb
Croatia
- e-mail info@gaurus.hr
- mobile **+385 (0)98 456 543**

Also, for additional questions, we refer to the contact information of the Croatian Personal Data Protection Agency (AZOP):

- address **Agencija za zaštitu osobnih podataka**
Selska cesta 136
10000 Zagreb
Croatia
- e-mail azop@azop.hr
- telephone **+385 1 4609 000**
- fax **+385 1 4609 099**

14. COOKIE POLICY AND COMPANY WEBSITE VISITS MEASUREMENT

In order to ensure the correct operation of the Company's websites, to enable the use of the pages and to improve content browsing, we save a small amount of information on the visitor's computer, the so-called cookies. They serve to make the website work optimally and to improve the browsing and use experience, as well as to understand how our websites are used.

What is the purpose of cookies?

The purpose of a cookie that is allowed to be stored on the data subject's computer is to save the user's settings, website settings, preferred language or user's IP address. When the data subject visits the same page again after some time, the Internet browser they use sends information tailored to the user's needs.

Depending on the defined task, cookies store a wide range of information, which includes personal data, among others. However, only the data subject decides which information the cookies will save. In the settings of the Internet browser, the data subject can choose for himself whether to approve or reject requests to save cookies. By disabling cookies, it may not be possible to use some of the functionalities on the Company's websites.

Types of cookies

Permanent cookies remain on the data subject's computer after closing the Internet browser program. Permanent cookies have no duration limit and, in principle, remain in the browser until the data subject manually deletes them. They have the purpose of storing permanent data such as username and password so that you don't have to log in again every time.

Temporary cookies disappear from your computer after you close your internet browser. With their help, temporary data such as the data you provide when shopping online is stored.

First-party cookies can be permanent or temporary, and they store data that will be used again during the next visit to the pages from which they were stored on the data subject's computer.

Third-party cookies or so-called advertising cookies are stored on the user's computer if the user uses commercials and advertisements on the page he is visiting, and it redirects the user to a third party. This method is used to monitor Internet usage for marketing purposes.

The company uses cookies related to:

- website functionality – the task of these cookies is to recognize you on our website and remember your previously selected settings. These may include your preferred language and location, and a combination of first and third party cookies are used,
- advertising - the task of these cookies is to collect information about your visit to our website, the content you have viewed, the links you have followed and information about your browser, device and your IP address. The Company sometimes shares some limited aspects of these data with third parties for advertising purposes. This means that when you visit another website, you may be shown an advertisement based on your browsing patterns on our website.

Our website uses the Google Analytics traffic measurement service, a web analytics service provided by Google, Inc. (Google). The information generated by the cookie about the use of our website (including the visitor's IP address) will be transmitted to Google and stored on their server(s). Google will use this information for the purpose of evaluating the use of our website, compiling reports on website activity for website operators and providing other services related to website activity and internet usage. Google may also transfer these data to third parties, if required by law, or if such third parties process the data on behalf of Google. Google will not associate the IP address of the data subject with other data in Google's possession. More information about Google's privacy policy is available at:

<http://www.google.com/privacy.html>.

The data collected in this way cannot identify a site visitor, and all data is used exclusively for statistical purposes. If you want to prohibit the aforementioned services from saving cookies, you can do so at the following link:

Google Analytics:

<https://tools.google.com/dlpage/gaoptout>

You can visit the following links for more information about cookies:

- <http://www.allaboutcookies.org/>
- <http://www.youronlinechoices.eu/>
- <http://www.youronlinechoices.com/hr/>
- <http://www.aboutads.info/choices/>

Detailed descriptions of cookie control and how to disable them for individual browsers:

Chrome:

<https://support.google.com/chrome/answer/95647?hl=hr>

Firefox:

<https://support.mozilla.org/hr/kb/Uklju%C4%8Divanje%20i%20isklju%C4%8Divanje%20kola%C4%8Di%C4%87a>

Internet Explorer:

<http://windows.microsoft.com/hr-HR/internet-explorer/delete-manage-cookies#ie=ie-11>

Opera:

<http://help.opera.com/Windows/10.00/en/cookies.html>

Safari:

<https://support.apple.com/hr-hr/HT201265>

REQUEST FOR ACCESS TO PERSONAL DATA

I, _____, hereby request from GAURUS d.o.o. (Company), as the controller of my personal data, a confirmation of whether the Company processes my personal data and, if it processes them, the delivery of a written notification about the data it processes, including:

- | | |
|---|--|
| (a) processing purposes; | (e) my rights regarding the processing of these data; |
| (b) categories of the personal data in question; | (f) if personal data are not collected from the data subject, information about their source; |
| (c) recipients to whom personal data has been disclosed or will be disclosed, in particular to third-country recipients or international organizations; | (g) the existence of automated decision-making, including profiling; |
| (d) period in which personal data will be stored; | (h) whether personal data is transferred to a third country or an international organization, and if transferred, about the appropriate protective measures related to the transfer. |

This request applies to all my personal data collected and processed by the Company for any purpose.

Submit the written notification to: _____.

(handwritten signature of the data subject)

REMARK: It is necessary to specify the address and method of delivery of the notification (e.g. e-mail, delivery by post, in person, etc.).

REQUEST FOR RECTIFICATION AND/OR HAVING INCOMPLETE PERSONAL DATA COMPLETED

I, _____, hereby request from GAURUS d.o.o. (Company), as the controller of my personal data, the following actions:

- 1) rectification of my personal data that are inaccurate, which are: _____
_____;
- 2) completion of my personal data that are incomplete, which are: _____
_____.

(handwritten signature of the data subject)

REMARK: It is necessary to circle the requested action and indicate for which data and in what way the rectification and/or completion was requested.

REQUEST FOR ERASURE OF PERSONAL DATA

I, _____, hereby request from GAURUS d.o.o. (**Company**), as the controller of my personal data, permanent erasure of my personal data on the following grounds:

- 1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
- 2) the consent for the processing of personal data, which was the basis for the processing of personal data, was withdrawn,
- 3) an objection has been lodged against the processing of data collected on the basis of legitimate interest or for marketing purposes,
- 4) a competent authority has determined that the processing of personal data is unlawful,
- 5) the data must be erased for the purpose of compliance with the Company's legal obligations prescribed by applicable law,

This request relates to the following personal data: _____
_____.

Explanation:

_____.

(handwritten signature of the data subject)

REMARK: It is necessary to circle the appropriate grounds for erasure and indicate for which data erasure is requested, including a brief explanation of the request for erasure.

REQUEST FOR RESTRICTION OF PERSONAL DATA PROCESSING

I, _____, hereby request from GAURUS d.o.o. (Company), as the controller of my personal data, the restriction of personal data processing due to:

- 1) I contested the accuracy of the personal data;
- 2) it has been determined that the processing of personal data is unlawful, but I do not request the erasure of my personal data;
- 3) The company no longer needs personal data for processing purposes, but I require them to establish, exercise or defend my legal claims;
- 4) I objected to the legitimate interests of the Company on the basis of which my personal data are collected and processed.

This request relates to the following personal data: _____
_____.

(handwritten signature of the data subject)

REMARK: It is necessary to circle the appropriate grounds for the restriction of processing and to specify the personal data for which restriction is requested, including a brief explanation of the request for restriction.
While the restriction of personal data processing lasts, the Company may still process data in order to fulfill its legal claims or protect the rights of other persons.
The Company will inform the data subject before discontinuing the restriction of processing.

REQUEST FOR TRANSFER OF PERSONAL DATA

I, _____, hereby request from GAURUS d.o.o. (Company), as the controller of my personal data, to directly transfer my personal data to another controller, namely:

- 1) name and last name;
- 2) address of permanent (or temporary) residence or headquarters;
- 3) personal identification number, registration or other appropriate number under which I am registered in official registers;
- 4) place and date of birth or incorporation;
- 5) the function I perform;
- 6) telephone, mobile or fax number, e-mail address;
- 7) data on identity documents (identity card, passport, etc.);
- 8) data on bank accounts and transactions;
- 9) public and private documents issued by competent persons (certificates of health and pension insurance, etc.);
- 10) data on salary and salary supplements;;
- 11) applications, registrations, references, diplomas, certificates, decisions, etc. for work and for other (e.g. student contracts, volunteering) positions;
- 12) photographs;
- 13) data on health status;
- 14) other _____ ;
- 15) all my personal data collected and processed by the Company,

Another controller to whom I want my personal data to be transferred directly:

Name and last name/company _____
Personal identification number _____
Address/headquarters _____
E-mail _____

(handwritten signature of the data subject)

REMARK: It is necessary to circle the personal data for which transfer to another controller is requested.