Privacy statement of ProCredit Banka AD Skopje

The protection of the privacy and confidentiality of the data of the bank's customers/associates/employees is of the utmost importance to Procredit Banka AD Skopje and is one of the basic principles on which the bank's work is based.

With the Privacy Statement we aim to explain the process of collecting and processing your data.

The following information is intended to give you an overview of how we process your personal data as well as information about your rights under the applicable data protection regulation. What specific data is processed and how it is used depends primarily on the services you have applied for or agreed with the bank.

Any activity related to personal data is carried out by the Bank in accordance with the Personal Data Protection Law and bylaws adopted under this Law with all amendments.

This document consists of the following content:

1. Definitions

The notice for data protection of ProCredit Bank AD Skopje is based on the terms used by the applicable legislation, i.e. the Law on Personal Data Protection and all bylaws arising from it. Data protection notice should be readable and understandable to the public, as well as to our clients and business partners. To ensure this, we would first like to explain the terminology used. In this Data Protection Notice, we use, inter alia, the following terms:

a) "Personal data" means any information relating to an identified natural person or an identifiable natural person (personal data subject), and an identifiable natural person is a person whose identity can be established directly or indirectly, in particular on the basis of an identifier such as name, surname,

personal identification number of the citizen, location data, online identifier, or on the basis of one or more characteristics specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

b) "Personal data subject" Personal data subject is any identified or identifiable natural person whose personal data is processed by the controller responsible for processing.

c) "Personal data processing" means any operation or set of operations performed on personal data, or a group of personal data, automatically or otherwise, such as: collecting, recording, organizing, structuring, storing, adjusting or change, withdrawal, consultation, inspection, use, disclosure through transmission, publication or otherwise making available, harmonizing or combining, limiting, deleting or destroying.

d**) "Restriction"** of the processing of personal data" is the designation of the personal data that are stored, in order to limit their processing in the future;

e) "Profiling" is any form of automatic processing of personal data, which consists of the use of personal data for the assessment of certain personal aspects related to the natural person, and especially for the analysis or forecasting of aspects related to the performance of professional duties of that natural person, his economic condition, health, personal preferences, interests, confidentiality, conduct, location or movement;

f) "Pseudonymization" is the processing of personal data in such a way that personal data can no longer be linked to a particular personal data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures to ensure that personal data are not linked to an identified natural person or an identifiable natural person;

g) "Controller" is a natural or legal person, body of state authority, state body or legal entity established by the state for exercising public authority, agency or other body, which independently or together with others determines the goals and the manner of processing personal data, and when the purposes and the manner of processing the personal data are determined by law, the same law determines the controller or the special criteria for its determination;

h) "Personal data collection processor" means a natural or legal person, a body of state authority, a state body or a legal entity established by the state for the exercise of public authority, an agency or other body that processes personal data on behalf of the controller;

i) "User" means a natural or legal person, a body of state authority, a state body or a legal entity established by the State for the exercise of public authority, an agency or another body to which personal data are disclosed, whether it is a third party or not. However, state authorities and state authorities to whom personal data are disclosed in a special investigation in accordance with the law are not considered users, and the processing of such data by these authorities must be in accordance with the applicable rules for protection of personal data according to the purposes of that processing;

j) "Third party" means any natural or legal person, body of state authority, state body or legal entity established by the State for the exercise of public authority, agency or other body, which is not a personal data subject, controller, processor or person , which under the direct authorization of the controller or processor is authorized to process the data;

k) "Consent" of the personal data subject is any freely given, concrete, informed and unambiguous declared will of the personal data subject, through a statement or clearly confirmed action, which expresses consent for the processing of his personal data;

2. To whom this Privacy Statement refers?

ProCredit Bank collects, preserves, and processes personal data disclosed to the bank by potential and/or existing clients and, in general, persons who carry out business activities with the bank in any capacity at all stages of business co-operation.

ProCredit Bank's privacy statement refers to all personal data subjects who have entered into a business relationship with the bank and/or have applied for a business relationship with the bank, including but not limited to: clients, associates, employees, members of legally stipulated boards, practitioners, applicants for work (*way of processing the personal data of employees, interns, applicants for work, in addition to this privacy statement, are governed by internal acts*).

Primarily the Bank collects those personal data that the personal data subjects themselves have disclosed at the bank's disposal, when filling in a client registration application in the first business contact with the Bank (in the case of clients), basic data for the subject when applying for employment (all necessary information to meet the legal obligations in accordance with the Labour Relations Act and applicable collective agreements).

3. Which sources and data does ProCredit Bank use?

We process your personal data whenever you contact us, e.g. when you fill out an application form over the Internet to open an account, or if you are already a client, when you contact us by email or phone or when you use our products and services under the terms of our business relationship. In addition, if necessary for the purpose of providing our services, we process personal data that we legitimately provide from publicly available sources (e.g. commercial registers, association registers, other public registers, stamp, Internet), or from other companies belonging to the ProCredit group or other third parties that legally and legitimately provide data to us.

Relevant personal data includes your name, address, and other contact information, date and place of birth, your name, nationality, as well as verification data (e.g., ID data) and authentication (for example, your signature of a copy) of your identity. Additionally, relevant personal data may include transaction data (e.g. payment orders), data relating to the fulfilment of our contractual obligations (e.g. account turnover data), information about your financial situation (e.g., payment trends), advertising and marketing data, data documentation (e.g. recordings of phone calls made for issuing instructions), audio-visual data – where applicable and legally permitted, we process surveillance videos in the Bank's branches, and/or recordings of phone calls when talking to our customers with the customer care center. We can use these recordings to confirm your requests made by phone, and/or to prevent fraud, data for children only when using a service/product in the Bank and other data comparable to the above categories (e.g. sociodemographic data as civic status).

In particular, the bank may process the following personal data:

- **Personal data provided by subjects:**

- Identification data (first and last name, date and place of birth, ID or passport data, sole registration number/personal identification number, etc.)
- Demographic data (gender, nationality, marital status),
- Contact data (phone number, address, e-mail address, etc.),
- Financial data (salary and property information, tax number),
- Data for accessing electronic applications, example of e-banking announcement data (example username, etc.).

- **Personal data collected by the Bank, such as:**
  - Personal data related to the implementation of measures of analysis, detection of certain persons or subjects to whom financial restrictive measures have been imposed, such as in preventing money laundering and financing terrorism;
  - Personal data regarding creditworthiness monitoring and assessment, risk management and generally the needs of the clients/associates with ProCredit Bank;
  - In accordance with the applicable legal framework for the submission of data to supervisory authorities;
  - In the context of correspondence and general communication of clients with the bank;
  - Economic data that assess investment, financial status and clients behavior;
  - "cookies" and accompanying technologies that allow access and use of specific pages and/or websites;
  - Information provided by supervisory, judicial and other public and independent authorities, related to criminal convictions, violations, implementation of measures to protect the public interest, confiscations and pledges;
  - Data affecting clients and are publicly available over the Internet or otherwise;
  - Data on employees of ProCredit Bank, persons doing internship or volunteer work at the Bank in accordance with the applicable legal framework in this area;
  - Data on candidates for employment in the Bank;
  - Personal data collected when using the Bank's website.

The personal data processed by Procredit Bank is stored in hard copy and/or electronic form.

The Bank is taking appropriate measures to protect personal data for minors, in accordance with the applicable regulation. The data on minors are kept only by the bank if the personal data is provided by persons who have custody of minors and only for the needs of the business relationship with the Bank for the benefit of minors, except when otherwise stipulated by law.

We emphasis that the Bank processes personal data only in the volume necessary for processing purposes.

Also, the products and services provided by ProCredit Bank are by no means intended for direct use by minors. Additionally, the Bank does not provide any type of IT services for children in the context of Article 12 of the Personal Data Protection Law.

4. Contact information of the controller that processes your data and where to contact on this issue

Your data is processed by:

ProCredit Bank AD Skopje
Manapo Street, number 7
1000 Skopje
Republic of North Macedonia
Email: mkd.info@procredit-group.com
Website: www.pcb.mk

You can contact our Personal Data Protection Officer by email or phone:
Jasmina Karadinovska Murtanovska
ProCredit Bank AD Skopje
Manapo Street, number 7
1000 Skopje
Tel: +389 2321 95 95
Email: mkd.dataprotection@procredit-group.com
Website: www.pcb.mk

5. What are the objectives of processing the data and on what basis can the Bank process it?

We process personal data in accordance with the requirements of the Personal Data Protection Law as well as other applicable laws and bylaws in the Republic of North Macedonia for personal data protection in the following situations:

a) To fulfill our contractual obligations (Article 10 paragraph (1) indent 2 of the LPDP)
The data are processed to perform banking transactions and financial services in order to perform / fulfill the obligations of the contracts concluded with our clients or with purpose to take steps at the request of our clients before concluding such an agreement. The purposes for which personal data are processed depend primarily on the specific product / service (e.g. current account, deposits) and may include financial needs analysis, advice, and transaction execution.

b) The processing is necessary for the purposes of the legitimate interests of the controller or of a third party, except when such interests do not prevail over the interests or fundamental rights and freedoms of the personal data subject seeking protection of personal data (Article 10 paragraph (1) indent 6 of the LPDP)
If necessary, we process your data to some extent above what is strictly necessary for the performance of the contract in order to protect our legitimate interests or the interests of third parties. Examples of such processing are:
- Measures for management of business activities and measures aimed at development of services and products;
- Ensuring IT security and IT operations of the bank;
- Revision and optimization of procedures used for needs analysis conducted in order to address customers directly;
- Advertising or market research and opinion, unless you have exercised your right to object to the use of your data for these purposes;
- Video surveillance for the purpose of preserving the right to access control, gathering evidence in the event of robbery and fraud, protection of life or health of people, protection of property, protection of life and health of employees due to the nature of work (Article 90 of LPDP) ;
-Measures to ensure the safety of buildings and equipment (e.g. monitoring access to restricted areas);
- Measures to preserve the right of access control.

c) Based on your consent (Article 10 paragraph (1) indent 1 of the LPDP)
Provided that you have given consent for the processing of your personal data for certain purposes (for example: to transfer your data to other entities in the group of which part of the bank, to analyze the payment transaction data for marketing purposes), this processing is legitimate based on your consent. Consent may be withdrawn at any time.
Withdrawal of consent does not affect the legitimacy of the data processing before withdrawal.

d) To comply with a legal obligation or to act in the public interest (Article 10 paragraph (1) indent 3 of the PDPL)
In addition, we as a bank are subject to various legal obligations, i.e. requirements based on certain laws (e.g. Law on Banks, Law on Prevention of Money Laundering and Financing of Terrorism, Laws on Taxation, Laws on Payment Operations) and requests of supervisory bodies (for example, the National Bank of the Republic of North Macedonia, the Agency for Protection of personal data). The purposes of data processing in such cases include verification of identity and age, prevention of fraud and money laundering, compliance with reporting requirements in accordance with applicable tax laws, as well as assessment and purpose of risk management in the bank and in the group ProCredit.

6. Who has access to your data?

Within the bank, access to your data is given to those organizational units that are needed to meet our contractual and legal obligations. Service providers and agents hired by us may also obtain information about their purposes, they are obliged to maintain your data as banking secrecy. This applies to companies in the categories of IT services, payment transactions, telecommunications, and marketing.

Regarding the transfer of data to recipients outside our bank, it should first be noted that, as a bank, we are obliged to maintain the confidentiality of all facts and assessments about the client that become known only to us (banking secret in accordance Banking Law). We are permitted to transfer your data if required by law, or if you have given your consent, or if the bank is authorized to disclose details of financial matters. Under these preconditions, the following may, among others, be recipients of personal data:
• Public institutions (e.g. National Bank, Financial Intelligence Unit, Financial Police Directorate, other financial authorities, law enforcement agencies), if there is a legal or official requirement.
• Other credit or financial services institutions or third parties to whom we transfer your personal information in order to execute our agreement with you (e.g. correspondent banks, credit agencies, depending on the nature of the agreement).
• Other companies belonging to the ProCredit group for risk management purposes in accordance with legal or official obligations.

Additionally, the bank may transfer your data to data recipients for whom you have given your consent for such data transfer.

7. Is the data submitted to a third country or to an international organization?

The data is transferred to the entities in the countries in the European Union, i.e. in the Federal Republic of Germany to entities belonging to the ProCredit group in order to fulfill the contractual

obligations arising from the contract with you as a customer. The data is transferred to entities outside the European Union and EEC ("Third countries"), if it is necessary for example in the following situations:
• it is required to carry out your instructions (e.g. Payment orders)
• it is legally required e.g. reporting requirements under applicable law), or
• you have given consent

In accordance with the Law on the Protection of Personal Data, when transferring personal data to the EU and/or in the EEA, the Bank is obliged to notify the Agency for personal data protection, and for transfer outside the EU and the EEA in accordance with the Personal Data Protection Act, the Bank will request approval from the Agency for Personal Data Protection.

8. How long will the Bank keep your personal data?

We process and store your personal data as long as we need it to fulfill our contractual and legal obligations. In this context, it should be noted that our business relationship is a continuing obligation and is expected to last for a number of years. If the data are no longer required to meet contractual or legal obligations, they are regularly deleted, unless further processing - for a limited period - is necessary for the following purposes:
• Compliance with the minimum retention periods according to the applicable laws and bylaws in the Republic of North Macedonia (for example: Law on Prevention of Money Laundering and Financing of Terrorism, Law on Trade Companies, Law on Banks, Law on Enforcement, Regulation on Macedonian Credit Bureau and credit register, payment operations regulations, etc.).

9. What are your rights regarding personal data protection?

When your data is processed, you have certain privacy rights. If you have questions regarding your rights, please contact us by email at the listed contact details.

Your rights are the following:

- **The right to be informed** - To emphasize the need for transparency in the use of personal data, we ensure fair processing of information through this privacy policy.
- Right of access - You have the right to ask the bank to review your personal data that we process.
- Right to correction - If your personal data is incorrect, you have the right to ask us to correct it. If we share your data with a third party, we will notify it if we change your data at your request.
- **Right to erasure ('right to be forgotten')** - ProCredit Bank is legally obliged to keep your personal data. Your right to be forgotten, i.e. the data that the bank processes / has processed to be completely deleted will be applicable if:

- Your data is no longer needed for its original purpose;
- You withdraw the given consent for processing;
- You object to the processing of your data for legitimate interests of the bank;
- ProCredit Bank illegally processes your personal data; or
- Local law requires that we delete your personal information

- Right to restrict processing - You have the right to ask the bank to restrict the use and processing of your personal data if:

- You believe that your personal information is incorrect;
- You believe we are processing the data illegally; or
- You object to the processing of your data for legitimate interests of the bank;

- Right to object - If you have legitimate reasons, you have the right to object to the processing of your personal data by ProCredit Bank. The bank will review your complaint and determine if the processing of your data has any negative impact due to which it would be necessary to stop the processing of your personal data;
- Right to data portability - You have the right to receive what personal data is being processed and to receive that information in an electronically readable format, or you may request that we transfer it to another controller if it is technically feasible. This right applies to those personal data that you have submitted to the bank in electronic form.

You may withdraw your consent to the processing of your personal data at any time. Please note that the withdrawal of consent is valid only for future processing of personal data, and not for the processing of personal data before the moment of withdrawal of consent.

A form of the request to exercise the rights as subjects of personal data is available at the following link: https://www.pcb.mk/politika-na-privatnost.nspx and as well can be submitted to the bank's attention on following address: "7 Manapo Street, 1000 Skopje", with indication "for The Officer for the Protection of Personal Data" or electronically at the address: mkd.dataprotection@procredit-group.com.


Request on exercise the rights of person

Before submitting such request, all subjects of personal data are encouraged and asked to read the applicable legal provisions cited above containing conditions and limitations when and how these rights are exercised.

We also note that the bank will provide the requested information without compensation, within the legally stipulated deadlines, except in the case where the requests are clearly unfounded or excessive, especially if the same requests are repeated. In these cases, the bank will refuse to act on the request or charge compensation, considering the volume, complexity and time it takes to provide the information or act on request, for which you will be properly informed.

10. Should you disclose your personal data to the Bank?

According to the terms of our business relationship, you are required to provide the personal data necessary to establish and conduct a business relationship and to fulfill the contractual obligations related to that relationship or the data that we are legally obliged to collect. Without this information we will generally not be able to enter into or fulfill an agreement with you.

In particular, the conditions for compliance with the applicable anti-money laundering regulations oblige us, before establishing a business relationship, to verify your identity based on an identity document and to state your name and surname, place of birth, date of birth, nationality and address, as well as data on the personal identification document. To enable the bank to meet this legal obligation, you are required according to the applicable legislation in the Republic of North Macedonia to provide us with the necessary information and documents and to inform us without delay of any changes that will occur during the established business relationship. If you do not submit the necessary information and documentation to the bank, the business relationship will not be extended or established.

11. To what extent is decision making is automated and is profiling done?

When processing your personal data, it is sometimes necessary to use profiling or other automated methods related to the following:

- **Credit exposure checks to determine if your loan application will be accepted.** This includes calculating the probability that the payment obligations will be met by the client in accordance with the relevant agreement. Input variables for this calculation may include, for example, amount of income, expenses, current liabilities, occupation, employer, duration of employment, business history to date, timely repayment of previous loans and information received from credit agencies. This assessment is based on mathematics statistics and best practices. The total values support decision-making in concluding contracts for our products/services, and are taken into account in managing the risks to which the bank is exposed.
- **Checks against money laundering, terrorist financing and other sanctions**
- **Identity and address checks**
- **Tracking your account** to prevent fraud and other financial crime
- **Screening of clients** who may be assessed as "politically exposed" (for example, if you are a public official)
- **Assessments required by our regulators and relevant authorities** to ensure that we meet our regulatory obligations
- **For decision making process whether the account is dormant** (i.e. no longer used) and, if so, process of closing of the account is performed.

As a principle, ProCredit Bank AD Skopje does not use fully automated decision-making as stated in Article 26 of the LPDP for the purpose of establishing and conducting a business relationship. If we apply such procedures in individual cases, we will notify you separately, if we are legally obliged to do so.

12. Video surveillance system

The Bank performs video surveillance only of the space sufficient to meet the objectives for which it is set, i.e. to protect the life and health of people, protect the ownership, protect the life and health of employees, and/or to ensure control of entry and exit from the official premises of the Bank.

Recordings taken when performing video surveillance shall be kept until the objectives for which surveillance is carried out is met, but not longer than 30 days. After this deadline, the recordings are deleted from the video surveillance system. Recordings may be kept for a longer period of time if such storage complies with a law containing safeguards and other measures to protect the rights and freedoms of subjects available data, but not longer than meeting the objectives. The recordings may also be kept for a longer period of time when necessary to fulfil the Legitimate Interest of the Bank in conducting appropriate procedures in accordance with the law.

In a visible and clear place where video surveillance is placed, the bank has appropriate notification (label) that points out that video surveillance is carried out, as well the following information is placed: data on the controller's name, the purpose of video surveillance, the deadline for keeping recordings, the rights of subjects of personal data, and how additional information can be obtained.

For more information about the bank's video surveillance system, you can consult the Privacy Statement on video surveillance posted on the Bank's website (https://www.pcb.mk/politika-na-privatnost.nspx) as well as in the Bank's service centers in hard copy.

13. Recording phone calls

ProCredit Bank uses technical means to record phone calls with customers regarding the execution of transactions by customers with certain organizational units of the Bank, in carrying out and providing appropriate activities regarding the execution of transactions and requests/complaints from customers in accordance with the applicable legal regulation. In such cases, appropriate notification is provided to customers and to ProCredit Bank's business partners/associates before any recording of any phone call.

14. Marketing

The Bank may use the personal data of personal data subjects to inform them of the Bank's products/services and/or promotional activities that may interest them only after obtaining direct consent to it. The Bank uses this data explicitly to promote its own products/services to subjects of personal data who have given such consent.

We note that the consent given for this purpose can be withdrawn at any time without compensation, through the following channels:

- directly to the Bank's service centers by updating the Customer Registration Application,
- by submitting a request to withdraw the consent of the bank's info e-mail address mkd.info@procredit-group.com or to the e-mail address for the protection of available data mkd.dataprotection@procredit-group.com.

15. How ProCredit Bank protects your personal data

When processing your personal data, the bank takes appropriate technical and organizational measures (policies and procedures, IT security, etc.) to ensure the confidentiality and integrity of your personal data and the manner of their processing. We apply an internal framework of policies and standards throughout our business to keep your personal data safe. These policies and standards are periodically revised to comply with applicable regulations and market changes.

ProCredit Bank employees are also committed to confidentiality and may not disclose your information illegally or unnecessarily. To help us continue to protect your data, whenever you suspect that your personal data has been compromised, contact the bank through the contact details listed in item 4.

16. Amending/supplementing the Privacy Statement

The privacy statement was adopted on July 28, 2021.

The Bank has the right to amend/update/supplement this Privacy Statement of ProCredit Banka AD Skopje, in order to comply with the applicable regulation and/or internal acts of ProCredit Holding, if they are more specific or restrictive in relation to national legislation.

In such a case, ProCredit Bank will publish the amended Privacy Statement of ProCredit Banka AD Skopje on its website by specifying the date of the amendment and what the policy changes are.

16.1 ProCredit Bank's privacy statement was adopted on 21.09.2023. The following changes are being implemented:

- Improving the review of the Statement by introducing content on it and renumbering certain titles;
- Supplementation in the part of which personal data subjects it refers to, as well as to which personal data processing operations it refers to;
- Information has been added in the part of exercising the rights of subjects of personal data by specifying how the request for the exercise of rights can be submitted;
- Clarifications have been added on the processing of personal data in the video surveillance system, phone calls and processing for marketing purposes,
- Information for amending/supplementing the Statement has been added.

Version 1.1. adopted on 21.09.2023.

Privacy statement of Quipu

Data Protection Declaration

1. Introduction and principles

Quipu GmbH takes the protection of your data seriously. The use of the Internet pages of Quipu GmbH is possible without any indication of personal data; however, if a data subject requests services via our website, or applies for an employment position, processing of personal data could become necessary. If the processing of personal data is necessary and there is no statutory basis for such processing, we generally obtain consent from the data subject.

The processing of personal data, such as the name, address, e-mail address, or telephone number of a data subject shall always be in line with the General Data Protection Regulation (GDPR) and in accordance with the country-specific data protection regulations applicable to Quipu GmbH. By means of this data protection declaration, our enterprise would like to inform the general public of the nature, scope, and purpose of the personal data we collect, use and process. Furthermore, data subjects are informed, by means of this data protection declaration, of the rights to which they are entitled.

As the data controller, Quipu GmbH has implemented numerous technical and organizational measures to ensure the most complete protection of personal data processed through this website. This includes the use of encryption, pseudonymisation, and restricting our employee access to your data to the minimum.

2. Name and Address of the controller

Controller for the purposes of the General Data Protection Regulation (GDPR), other data protection laws applicable in Member states of the European Union and other provisions related to data protection is:

Quipu GmbH

Königsberger Str. 1

60487 Frankfurt

Germany

Phone: +49 69 50 69 90-0

Email: quipu@quipu.de

Website: **www.quipu.de**

3. Name and Address of the Data Protection Officer

Gleb Stolyarov

c/o Quipu GmbH

Königsberger Str. 1

60487 Frankfurt

Germany

Phone: +49 69 50 69 90-0

Email: **dpo@quipu.de**

Website: **www.quipu.de**

4. Cookies

The Internet pages of Quipu GmbH use cookies. Cookies are text files that are stored in a computer system via an Internet browser.

Many Internet sites and servers use cookies. Many cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a character string through which Internet pages and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows visited Internet sites and servers to differentiate the individual browser of the data subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified using the unique cookie ID.

Through the use of cookies, Quipu GmbH can provide the users of this website with more user-friendly services that would not be possible without the cookie setting.

The data subject may, at any time, prevent the setting of cookies through our website by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an Internet browser or other software programs. This is possible in all popular Internet browsers. If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of our website may be entirely usable.

Cookies we place on your computer are automatically deleted after each session on the website.

See section 6 for how Google Analytics uses cookies, and opt-out possibilities.

5. Collection of general data and information

The website of Quipu GmbH collects a series of general data and information when a data subject or automated system calls up the website. This general data and information are stored in the server log files. Collected may be (1) the browser types and versions used, (2) the operating system used by the accessing system, (3) the website from which an accessing system reaches our website (so-called referrers), (4) the sub-websites, (5) the date and time of access to the Internet site, (6) an Internet protocol address (IP address), (7) the Internet service provider of the accessing system, and (8) any other similar data and information that may be used in the event of attacks on our information technology systems.

When using these general data and information, Quipu GmbH does not draw any conclusions about the data subject. Rather, this information is needed to (1) deliver the content of our website correctly, (2) analyse traffic in order to gauge interest in company and offerings, (3) ensure the long-term viability of our information technology systems and website technology, and (4) provide law enforcement authorities with the information necessary for criminal prosecution in case of a cyber-attack. Therefore, Quipu GmbH analyses anonymously collected data and information statistically, with the aim of increasing the data protection and data security of our enterprise, and to ensure an optimal level of protection for the personal data we process. The anonymous data of the server log files are stored separately from all personal data provided by a data subject.

6. Registration on our website

The data subject has the possibility to register on our website with the indication of personal data. For example, through a form, you may request a software demo. Which personal data are transmitted to the controller is determined by the respective input mask used for the registration. The personal data entered by the data subject are collected and stored exclusively for internal use by the controller, and for his own purposes. The controller may request transfer to one or more processors (e.g. a parcel service) that also uses personal data for an internal purpose which is attributable to the controller.

By registering on the website of the controller, the IP address—assigned by the Internet service provider (ISP) and used by the data subject—date, and time of the registration are also stored. The storage of this data takes place against the background that this is the only way to prevent the misuse of our services, and, if necessary, to make it possible to investigate committed offenses. Insofar, the storage of this data is necessary to secure the controller. This data is not

passed on to third parties unless there is a statutory obligation to pass on the data, or if the transfer serves the aim of criminal prosecution.

The registration of the data subject, with the voluntary indication of personal data, is intended to enable the controller to offer the data subject contents or services that may only be offered to registered users due to the nature of the matter in question. Registered persons are free to change the personal data specified during the registration at any time, or to have them completely deleted from the data stock of the controller.

The data controller shall, at any time, provide information upon request to each data subject as to what personal data are stored about the data subject. In addition, the data controller shall correct or erase personal data at the request or indication of the data subject, insofar as there are no statutory storage obligations. Please refer to the contract details above for any such requests.

Data is retained, only for so long as is deemed necessary according to the purpose for which it is purposed.

7. Use of Google Analytics

This website uses Google Analytics, a web analysis service from Google Inc. Google Analytics utilizes cookies to analyse web use and improve the efficiency of the website.

Through this cookie use, information about your session is saved in Google servers in the USA. While we do register IP-addresses, they are anonymised, and as such your IP addresses is not accessible to Google.

We use this service to understand how users access and utilize our website, so that we can continue to improve our service. Shall you wish to opt out, you may either block the use of cookies directly in your browser, as described above in section 3, or alternatively you may **block the use of cookies by installing a plug-in** which Google has developed for this purpose.

8. Routine erasure and blocking of personal data

The data controller shall process and store the personal data of the data subject only for the period necessary to achieve the purpose of storage, or as far as this is granted by the European legislator or other legislators in laws or regulations to which the controller is subject.

If the storage purpose is not applicable, or if a storage period prescribed by the European legislator or another competent legislator expires, the personal data are routinely blocked or erased in accordance with legal requirements.

9. Rights of the data subject

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact the controller.

b) Right of access

Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this information. Furthermore, the European directives and regulations grant the data subject access to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organisation. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Quipu reserves the right to verify the identity of the requester. Additionally, shall requests be excessive or repetitive in nature; Quipu may charge a fee, commensurate with the cost of preparing and transferring the aforementioned data.

If a data subject wishes to avail himself of this right of access, he or she may, at any time, contact the controller.

c) Right to rectification

Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact the controller.

d) Right to erasure (Right to be forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent to which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- The personal data have been unlawfully processed.
- The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by Quipu GmbH, he or she may, at any time, contact the controller. An employee of Quipu GmbH shall promptly ensure that the erasure request is complied with immediately.

Where the controller has made personal data public and is obliged pursuant to Article 17(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. An employees of Quipu GmbH will arrange the necessary measures in individual cases.

e) Right of restriction of processing

Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.
- The data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by Quipu GmbH, he or she may at any time contact the controller. The employee of Quipu GmbH will arrange the restriction of the processing.

f) Right to data portability

Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used

and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

In order to assert the right to data portability, the data subject may at any time contact Quipu GmbH.

g) Right to object

Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

Quipu GmbH shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

If Quipu GmbH processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing activities. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to Quipu GmbH to the processing for direct marketing purposes, Quipu GmbH will no longer process the personal data for these purposes.

In order to exercise the right to object, the data subject may contact the controller. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

h) Right to withdraw data protection consent

Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may, at any time, contact Quipu GmbH.

i) Right to lodge complaint

As a data subject, you have the right to lodge a complaint with the supervisory authority. The data protection authority responsible for the territory in which Quipu's head office is located is:

Der Hessische Datenschutzbeauftragte

Web page: **https://datenschutz.hessen.de/**

Email address: **Poststelle@datenschutz.hessen.de**

Tel.: +49 611 1408 – 0

10. Data protection for applications and the application procedures

The data controller shall collect and process the personal data of applicants for the purpose of the processing of the application procedure. The processing may also be carried out electronically. This is the case, in particular, if an applicant submits corresponding application documents by e-mail or by means of a web form on the website to the controller. If the data controller concludes an employment contract with an applicant, the submitted data will be stored for the purpose of processing the employment relationship in compliance with legal requirements. If no employment contract is concluded with the applicant by the controller, the application documents shall be erased six months after notification of the refusal decision. For more information on processing of personal data entered via the CV uploader, please refer to the CV-uploader privacy statement.

11. Legal basis for the processing

Art. 6(1) lit. a GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by

which processing of personal data is required, such as for the fulfilment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR. Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

12. The legitimate interests pursued by the controller or by a third party

Where the processing of personal data is based on Article 6(1) lit. f GDPR our legitimate interest is to carry out our business in favour of the well-being of all our employees and the shareholders.

13. Period for which the personal data will be stored

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfilment of the contract or the initiation of a contract.

14. Provision of personal data as statutory or contractual requirement; Requirement necessary to enter into a contract; Obligation of the data subject to provide the personal data; possible consequences of failure to provide such data

We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner). Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provide us with personal data when our company signs a contract with him or her. The non-provision of the personal data would have the consequence that the contract with the data subject could not be concluded. Before personal data is provided by the data subject, the data subject must contact any employee. The employee clarifies to the data subject whether the

provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of non-provision of the personal data.

15. Existence of automated decision-making

As a responsible company, we do not use automatic decision-making or profiling.

16. Subscription to our newsletters

On the website of Quipu GmbH, users are given the opportunity to subscribe to our enterprise's newsletter. The input mask used for this purpose is intended for the subscribers' email address.

Quipu uses the online marketing platform "MailChimp", operated by The Rocket Science Group LLC, a company headquartered in the State of Georgia in the United States of America. In signing up for the newsletter, the data subject uploads his/her email address to the MailChimp server. Refer to MailChimp's privacy statement for further info: **https://mailchimp.com/legal/privacy/.**

Quipu GmbH informs its customers and business partners by means of a newsletter about enterprise offers. The enterprise's newsletter may only be received by the data subject if (1) the data subject has a valid e-mail address and (2) the data subject confirms for the newsletter subscription. A confirmation e-mail will be sent to the e-mail address registered by a data subject for the first time for newsletter shipping. This confirmation e-mail is used to verify the owner of the e-mail address as the data subject, who requested the subscription.

During the registration for the newsletter, we may also store the IP address of the computer system assigned by the Internet service provider (ISP) and used by the data subject at the time of the registration, as well as the date and time of the registration. The collection of this data is necessary in order to understand the (possible) misuse of the e-mail address of a data subject at a later date, and it therefore serves the aim of the legal protection of the controller.

The personal data collected as part of a registration for the newsletter will only be used to send our newsletter. In addition, subscribers to the newsletter may be informed by e-mail, as long as this is necessary for the operation of the newsletter service or a registration in question, as this could be the case in the event of modifications to the newsletter offer, or in the event of a change in technical circumstances. There will be no transfer of personal data collected by the newsletter service to third parties. The subscription to our newsletter may be terminated by the data subject at any time. The consent to the storage of personal data, which the data subject has given for shipping the newsletter, may be revoked at any time. For the purpose of revocation of consent, a corresponding link is found in each newsletter. It is also possible to unsubscribe from the

newsletter at any time directly on the website of the controller, or to communicate this to the controller in a different way.

17. Newsletter Tracking

The newsletter of the Quipu GmbH contains so-called tracking pixels, we web beacons. A tracking pixel is a miniature graphic embedded in such e-mails, which are sent in HTML format to enable log file recording and analysis. This allows a statistical analysis of the success or failure of online marketing campaigns. Based on the embedded tracking pixel, Quipu GmbH may see if and when an e-mail was opened by a data subject, and which links in the e-mail were called up by data subjects.

Such personal data collected in the tracking pixels contained in the newsletters are stored and analyzed by the Quipu in order to optimize the shipping of the newsletter, as well as to adapt the content of future newsletters even better to the interests of the data subject. These personal data will not be passed on to third parties. Data subjects are at any time entitled to revoke the respective separate declaration of consent issued by means of the double-opt-in procedure. After a revocation, these personal data will be deleted by the controller. Quipu GmbH automatically regards a withdrawal from the receipt of the newsletter as a revocation.

18. Data protection provisions about the application and use of Facebook

On this website, the controller has integrated components of the enterprise Facebook. Facebook is a social network.

A social network is a place for social meetings on the Internet, an online community, which usually allows users to communicate with each other and interact in a virtual space. A social network may serve as a platform for the exchange of opinions and experiences, or enable the Internet community to provide personal or business-related information. Facebook allows social network users to include the creation of private profiles, upload photos, and network through friend requests.

The operating company of Facebook is Facebook, Inc., 1 Hacker Way, Menlo Park, CA 94025, United States. If a person lives outside of the United States or Canada, the entity responsible for your data is the Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

With each call-up to one of the individual pages of this Internet website operated by the Quipu and into which a Facebook component (Facebook plug-ins) was integrated, the web browser on the information technology system of the data subject is automatically prompted to download

display of the corresponding Facebook component from Facebook through the Facebook component. An overview of all the Facebook Plug-ins may be accessed under https://developers.facebook.com/docs/plugins/. During the course of this technical procedure, Facebook is made aware of what specific sub-site of our website was visited by the data subject.

If the data subject is logged in at the same time on Facebook, Facebook detects with every call-up to our website by the data subject—and for the entire duration of their stay on our Internet site—which specific sub-site of our Internet page was visited by the data subject. This information is collected through the Facebook component and associated with the respective Facebook account of the data subject. If the data subject clicks on one of the Facebook buttons integrated into our website, e.g. the "Like" button, or if the data subject submits a comment, then Facebook matches this information with the personal Facebook user account of the data subject and stores the personal data.

Facebook always receives, through the Facebook component, information about a visit to our website by the data subject, whenever the data subject is logged in at the same time on Facebook during the time of the call-up to our website. This occurs regardless of whether the data subject clicks on the Facebook component or not. If such a transmission of information to Facebook is not desirable for the data subject, then he or she may prevent this by logging off from their Facebook account before a call-up to our website is made.

The data protection guideline published by Facebook, which is available at https://facebook.com/about/privacy/, provides information about the collection, processing and use of personal data by Facebook. In addition, it is explained there what setting options Facebook offers to protect the privacy of the data subject. In addition, different configuration options are made available to allow the elimination of data transmission to Facebook. These applications may be used by the data subject to eliminate a data transmission to Facebook.

19. Data protection provisions about the application and use of Google+

On this website, the controller has integrated the Google+ button as a component. Google+ is a so-called social network. Google+ allows users of the social network to include the creation of private profiles, upload photos and network through friend requests.

The operating company of Google+ is Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, UNITED STATES.

With each call-up to one of the individual pages of this website, which is operated by Quipu and on which a Google+ button has been integrated, the Internet browser on the information

technology system of the data subject automatically downloads a display of the corresponding Google+ button of Google through the respective Google+ button component. During the course of this technical procedure, Google is made aware of what specific sub-page of our website was visited by the data subject. More detailed information about Google+ is available under **https://developers.google.com/+/.**

If the data subject is logged in at the same time to Google+, Google recognizes with each call-up to our website by the data subject and for the entire duration of his or her stay on our Internet site, which specific sub-pages of our Internet page were visited by the data subject. This information is collected through the Google+ button and Google matches this with the respective Google+ account associated with the data subject.

If the data subject clicks on the Google+ button integrated on our website and thus gives a Google+ 1 recommendation, then Google assigns this information to the personal Google+ user account of the data subject and stores the personal data. Google stores the Google+ 1 recommendation of the data subject, making it publicly available in accordance with the terms and conditions accepted by the data subject in this regard. Subsequently, a Google+ 1 recommendation given by the data subject on this website together with other personal data, such as the Google+ account name used by the data subject and the stored photo, is stored and processed on other Google services, such as search-engine results of the Google search engine, the Google account of the data subject or in other places, e.g. on Internet pages, or in relation to advertisements. Google is also able to link the visit to this website with other personal data stored on Google. Google further records this personal information with the purpose of improving or optimizing the various Google services.

Through the Google+ button, Google receives information that the data subject visited our website, if the data subject at the time of the call-up to our website is logged in to Google+. This occurs regardless of whether the data subject clicks or doesn't click on the Google+ button.

If the data subject does not wish to transmit personal data to Google, he or she may prevent such transmission by logging out of his Google+ account before calling up our website.

Further information and the data protection provisions of Google may be retrieved under **https://www.google.com/intl/en/policies/privacy/.** More references from Google about the Google+ 1 button may be obtained under **https://developers.google.com/+/web/buttons-policy**.

20. Data protection provisions about the application and use of LinkedIn

Quipu GmbH has integrated components of the LinkedIn Corporation on this website. LinkedIn is a web-based social network that enables users with existing business contacts to connect and to make new business contacts. Over 400 million registered people in more than 200 countries use LinkedIn. Thus, LinkedIn is currently the largest platform for business contacts and one of the most visited websites in the world.

The operating company of LinkedIn is LinkedIn Corporation, 2029 Stierlin Court Mountain View, CA 94043, UNITED STATES. For privacy matters outside of the UNITED STATES LinkedIn Ireland, Privacy Policy Issues, Wilton Plaza, Wilton Place, Dublin 2, Ireland, is responsible.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a LinkedIn component (LinkedIn plug-in) was integrated, the Internet browser on the information technology system of the data subject is automatically prompted to the download of a display of the corresponding LinkedIn component of LinkedIn. Further information about the LinkedIn plug-in may be accessed under https://developer.linkedin.com/plugins. During the course of this technical procedure, LinkedIn gains knowledge of what specific sub-page of our website was visited by the data subject.

If the data subject is logged in at the same time on LinkedIn, LinkedIn detects with every call-up to our website by the data subject—and for the entire duration of their stay on our Internet site—which specific sub-page of our Internet page was visited by the data subject. This information is collected through the LinkedIn component and associated with the respective LinkedIn account of the data subject. If the data subject clicks on one of the LinkedIn buttons integrated on our website, then LinkedIn assigns this information to the personal LinkedIn user account of the data subject and stores the personal data.

LinkedIn receives information via the LinkedIn component that the data subject has visited our website, provided that the data subject is logged in at LinkedIn at the time of the call-up to our website. This occurs regardless of whether the person clicks on the LinkedIn button or not. If such a transmission of information to LinkedIn is not desirable for the data subject, then he or she may prevent this by logging off from their LinkedIn account before a call-up to our website is made.

LinkedIn provides under **https://www.linkedin.com/psettings/guest-controls** the possibility to unsubscribe from and targeted ads, as well as the ability to manage ad settings. The setting of cookies may be denied under **https://www.linkedin.com/legal/cookie-policy.** The applicable privacy policy for LinkedIn is available under **https://www.linkedin.com/legal/privacy-policy.** The LinkedIn Cookie Policy is available under **https://www.linkedin.com/legal/cookie-policy.**

21. Data protection provisions about the application and use of Twitter

On this website, Quipu GmbH has integrated components of Twitter. Twitter is a multilingual, publicly-accessible microblogging service on which users may publish and spread so-called 'tweets,' e.g. short messages, which are limited to 280 characters. These short messages are available for everyone, including those who are not logged on to Twitter. The tweets are also displayed to so-called followers of the respective user. Followers are other Twitter users who follow a user's tweets. Furthermore, Twitter allows you to address a wide audience via hashtags, links or retweets.

The operating company of Twitter is Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, UNITED STATES.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a Twitter component (Twitter button) was integrated, the Internet browser on the information technology system of the data subject is automatically prompted to download a display of the corresponding Twitter component of Twitter. Further information about the Twitter buttons is available under **https://about.twitter.com/de/resources/buttons.** During the course of this technical procedure, Twitter gains knowledge of what specific sub-page of our website was visited by the data subject. The purpose of the integration of the Twitter component is a retransmission of the contents of this website to allow our users to introduce this web page to the digital world and increase our visitor numbers.

If the data subject is logged in at the same time on Twitter, Twitter detects with every call-up to our website by the data subject and for the entire duration of their stay on our Internet site which specific sub-page of our Internet page was visited by the data subject. This information is collected through the Twitter component and associated with the respective Twitter account of the data subject. If the data subject clicks on one of the Twitter buttons integrated on our website, then Twitter assigns this information to the personal Twitter user account of the data subject and stores the personal data.

Twitter receives information via the Twitter component that the data subject has visited our website, provided that the data subject is logged in on Twitter at the time of the call-up to our website. This occurs regardless of whether the person clicks on the Twitter component or not. If such a transmission of information to Twitter is not desirable for the data subject, then he or she may prevent this by logging off from their Twitter account before a call-up to our website is made.

The applicable data protection provisions of Twitter may be accessed under **https://twitter.com/privacy?lang=en.**

Please also read our Legal Notice.

Privacy statement of Piksel

Privacy Policy

At Piksel.mk, accessible from https://piksel.mk/, one of our main priorities is the privacy of our visitors. This Privacy Policy document contains types of information that is collected and recorded by Piksel.mk and how we use it.

If you have additional questions or require more information about our Privacy Policy, do not hesitate to contact us.

This Privacy Policy applies only to our online activities and is valid for visitors to our website with regards to the information that they shared and/or collect in Piksel.mk. This policy is not applicable to any information collected offline or via channels other than this website.

Consent

By using our website, you hereby consent to our Privacy Policy and agree to its terms.

Information we collect

The personal information that you are asked to provide, and the reasons why you are asked to provide it, will be made clear to you at the point we ask you to provide your personal information.

If you contact us directly, we may receive additional information about you such as your name, email address, phone number, the contents of the message and/or attachments you may send us, and any other information you may choose to provide.

When you register for an Account, we may ask for your contact information, including items such as name, company name, address, email address, and telephone number.

How we use your information

We use the information we collect in various ways, including to:

Provide, operate, and maintain our website

Improve, personalize, and expand our website

Understand and analyze how you use our website

Develop new products, services, features, and functionality

Communicate with you, either directly or through one of our partners, including for customer service, to provide you with updates and other information relating to the website, and for marketing and promotional purposes

Send you emails

Find and prevent fraud

Log Files

Piksel.mk follows a standard procedure of using log files. These files log visitors when they visit websites. All hosting companies do this and are a part of hosting services' analytics. The information collected by log files include internet protocol (IP) addresses, browser type, Internet Service Provider (ISP), date and time stamp, referring/exit pages, and possibly the number of clicks. These are not linked to any information that is personally identifiable. The purpose of the information is for analyzing trends, administering the site, tracking users' movement on the website, and gathering demographic information.

Cookies and Web Beacons

Like any other website, Piksel.mk uses "cookies". These cookies are used to store information including visitors' preferences, and the pages on the website that the visitor accessed or visited. The information is used to optimize the users' experience by customizing our web page content based on visitors' browser type and/or other information.

Advertising Partners Privacy Policies

You may consult this list to find the Privacy Policy for each of the advertising partners of Piksel.mk.

Third-party ad servers or ad networks use technologies like cookies, JavaScript, or Web Beacons that are used in their respective advertisements and links that appear on Piksel.mk, which are sent directly to users' browser. They automatically receive your IP address when this occurs.

These technologies are used to measure the effectiveness of their advertising campaigns and/or to personalize the advertising content that you see on websites that you visit.

Note that Piksel.mk has no access to or control over these cookies that are used by third-party advertisers.

Third Party Privacy Policies

Piksel.mk's Privacy Policy does not apply to other advertisers or websites. Thus, we are advising you to consult the respective Privacy Policies of these third-party ad servers for more detailed information. It may include their practices and instructions about how to opt out of certain options.

You can choose to disable cookies through your individual browser options. To know more detailed information about cookie management with specific web browsers, it can be found at the browsers' respective websites.

GDPR Data Protection Rights

We would like to make sure you are fully aware of all of your data protection rights. Every user is entitled to the following:

The right to access – You have the right to request copies of your personal data. We may charge you a small fee for this service.

The right to rectification – You have the right to request that we correct any information you believe is inaccurate. You also have the right to request that we complete the information you believe is incomplete.

The right to erasure – You have the right to request that we erase your personal data, under certain conditions.

The right to restrict processing – You have the right to request that we restrict the processing of your personal data under certain conditions.

The right to object to processing – You have the right to object to our processing of your personal data under certain conditions.

The right to data portability – You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us.

Children's Information

Another part of our priority is adding protection for children while using the internet. We encourage parents and guardians to observe, participate in, and/or monitor and guide their online activity.

Piksel.mk does not knowingly collect any Personal Identifiable Information from children under the age of 13. If you think that your child provided this kind of information on our website, we strongly encourage you to contact us immediately and we will do our best to promptly remove such information from our records.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. Thus, we advise you to review this page periodically for any changes. We will notify you of any changes by posting the new Privacy Policy on this page. These changes are effective immediately, after they are posted on this page.

Contact Us

If you have any questions or suggestions about our Privacy Policy, do not hesitate to contact us.