GeoCollect®

Erdwärme auf hohem Niveau

- Privacy policy –

may 2018

Geocollect Gmbh
Milchstr. 8
D-20148 Hamburg
Germany

Preface

Dear Sirs,

A Geocollect-Plant as a source for a brine heat pump wants to be carefully planned. In the digital age, we offer our customers the opportunity to use all relevant information via our website. This requires data to be collected and processed. Whether on the Internet or when buying a Geocollector's, we have the principle: where data is stored and sent, a high level of data protection and data security must be ensured. This applies to data from customers, prospects and business partners as well as employee data. Because data protection is the protection of the person.

Our claim is that Geocollect GmbH is not only for safe Geothermal energy but also sets standards for data protection. That is why we consider it our duty as a European company to comply with the different legal requirements associated with the collection and processing of personal data. Top priority For us to have a uniform and globally valid STA-Standard when dealing with people related data. To uphold the personal rights and privacy of each individual is the basis for our trusting business relationships.

In our corporate data protection policy, we have set strict conditions for the processing of personal data of customers, prospects, business partners and employees. This corresponds to the requirementsN European Data ProtectionDirective and ensures compliance with the principles of the globalLtenden National and InternationalData protection laws. In this way we set a valid data protection and data security standard in our company. As a standard, we have defined seven data protection principles – including transparency, data economy and data security.

Our executives and employees are obligated to comply with this privacy policy and to uphold the respective data protection laws. As data protection officer for data protection, I take care that the legal regulations and principles on data protection in the Geocollect GmbH.

Our staff and I are at your disposal as a contact for questions regarding data protection and data security Geocollect GmbH.

Kai-Uwe Wohlers

Data protection officer

Table

I. Purpose of the Privacy policy

DIE Geocollect GmbH Commits itself under Your Social responsibility to Compliance with data privacy laws. This Privacy policy applies Worldwide and is based on globally accepted basic principles of data protection.

Safeguarding data protection is a basis for trustworthy Relationships.

The Privacy Policy Creates one of the necessary frameworks for worldwide data investigations[1]. You Guarantees the European Privacy policy[2] Appropriate level of data protection required by national law. Cross-border traffic to countries where there is no legal Adequate level of data protection[3] Is.

II. Scope and Amendment of the Privacy policy

The Privacy policy applies To Geocollect GmbH and all With her company law Dependent Company and their employees. Dependent in this sense means that the Geocollect GmbHImmediately or indirectly, due to the possession of the majority of voting rights, a majority in the management Or an agreement may require that this privacy policy be is taken over.

The Data protection Directive covers all processing of personal Data. In countries where data of legal persons are used in the same way as Personal data are protected, this privacy policy also applies in the same way For data of legal persons.

Anonymous[5] data, e.g. for statistical evaluations Or investigations, are not subject to this privacy policy.

ABweichende regulations on data protection may be With the data protectionRepresentative Be created if this is done after the National law. A change to this privacy policy is In agreement with the Data protection supervisor Within the Procedure to amend directives..

Changes that have a significant impact on compliance with The Data Protection Directive, the approval of this privacy policy shall be deemed to be Data protection authorities that are binding in-house data protection regulations Report annually.

The latest version of the privacy policy can be in the privacy statement on the Internet site of the Geocollect Gmbh Under https://Www.Geocollect.de/datenschutz Retrieve.

[1] See Xv.
[2] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing Personal Data and On the free movement of data; Available at Http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm#richtlinie
[3] See Xv.
[4] See Xv.
[5] See Xv.

III. Application of state law

This privacy policy contains the worldwide accepted data protection principles, without That existing state law is being replaced. It supplements the respective national data protection law.

The respective state law is applicable if there are any deviations from this privacy policy Demands or further requirements. The contents of this Privacy policy Be observed even if there is no corresponding state law.

The reporting requirements for data processing, which exist under state law, must be Be observed.

Each Department of Geocollect GmbH is for compliance with this privacy policy and The legal obligations. Does it have any reason to believe that legal Obligations are contrary to the obligations of this data protection Directive, The data protection officer shall be to inform

IV. Principles for processing Personal data

1. Fairness and legitimacy

In the processing of personal data, the personal rights of the person concerned must be[6] respected. Personal data must be collected and processed in a lawfully and fairly manner.

2. Purpose binding

The processing of personal data may only be for the purposes set out prior to the collection of the data. Subsequent changes of purpose are only possible to a limited extent and require justification.

3. Transparency

The person concerned must be informed about the handling of his data. Basically, Personal data to the person concerned. When collecting the data, the The person concerned can identify at least the following or be informed accordingly about:

- The identity of the responsible body[7]
- The purpose of data processing
- Third[8] Or Categories of third parties to which the data may be transmitted

4. Data avoidance and data economy

Prior to the processing of personal data, it is necessary to examine whether and to what extent necessary in order to achieve the purpose intended for processing. If It is possible to achieve the purpose and that the expenditure is proportionate to the The intended purpose is to use anonymised or statistical data.

Personal data may not be stored on stock for potential future purposes Unless this is prescribed or permitted by state law.

[6] See Xv.
[7] See Xv.
[8] See Xv.

5. Deletion

Personal data which, after the expiration of legal or business process related Retention periods no longer required[9] Must be deleted. exist in Specific case, to provide evidence of interests worthy of protection or for the historical importance of Information, the data must remain stored until the protection worthy of interest is legally was clarified.

6. Factual accuracy and data topicality

Personal data are correct, complete and, where necessary, on the current Stand to save. Appropriate measures must be taken to ensure that the Non-applicable, incomplete or outdated data deleted, corrected, supplemented or updated Be.

7. Confidentiality and data security

Data confidentiality applies to personal data. You need to be in personal contact Be treated confidentially and through appropriate organisational and technical measures Against unauthorized access, unlawful processing or disclosure, as well as Accidental loss, alteration or destruction.

V. Admissibility of data processing

The collection, processing and use of personal data is only permitted if one of the following permission facts exists. Such a license is also required if the purpose for the collection, processing and use of the personal data is to be changed from the original purpose.

1. Customer and partner data

1.1 Data processing for a contractual relationship

Personal data of the interested party, customer or partner may be used for the the reasons for the execution and termination of a contract. This Also includes the support of the Contracting Party, provided this is in the context of the purpose of the contract. In the run-up to a contract – i.e. in the contract development missions phase – The processing of personal data for the preparation of offers, the planning of GeoCollect Systems or for the fulfilment of other requests for a conclusion of the contract of the interested party. Interested parties may, during the initiation of the contract, use Of the data that you have communicated. Possibly by the prospective the restrictions expressed must be observed. For further promotional activities The following requirements must be observed under V. 1.2.

[9] See Xv.

1.2 Data processing for advertising purposes

If the person concerned has an information request the Geocollect GmbH (e.g. request for the sending of information material), the Data processing is permissible for the performance of this application.

Other legal requirements are required for binding or advertising activities.

The processing of personal data for the purposes of advertising or market and marketing Opinion research is permissible if this is the case with the purpose for which the data was originally have been collected. The person concerned shall be able to use his data for purposes of advertising. If data are collected exclusively for advertising purposes Are voluntarily indicated by the person concerned. The person concerned shall be free to Information for these purposes. In the context of communication The person concerned should be informed[10] Of the person concerned in the processing of his Data for advertising purposes. The person concerned shall be informed in the context Choose between the available contact channels such as mail, electronic mail and telephone (Consent SEe V. 1.3).

If the person concerned does not object to the use of his data for advertising purposes, a Use of his data for these purposes and they must be used for these purposes. Be blocked.

1.3 Consent to data processing

Data processing may take place on the basis of the consent of the person concerned. Before the The person concerned must be informed in accordance with IV. Information in this privacy policy.

For reasons of evidence, the declaration of consent is basically written or electronically Obtain. Under certain circumstances, e.g. in the case of telephone consultation, consent can also be Be granted. Their issuance must be documented.

1.4 Data processing due to legal permission

The processing of personal data is also permissible where state legislation Require or permit the processing of data. The nature and scope Data processing must be necessary for the legally permissible data processing and are governed by this legislation.

1.5 data processing due to justified interest

The processing of personal data may also take place if this is necessary to achieve the of a legitimate interest deR Geocollect GmbH is required. Legitimate interests are usually legal (e.g. enforcement of open receivables) or economic (e.g. avoidance of contract problems). Processing of personal data on the basis of the of a legitimate interest may not take place if there is an indication in individual cases That the interests of the person concerned are worthy of interest in the Processing. The interests worthy of protection must be examined for each processing.

1.6 Processing of particularly protected data

The processing of particularly protective[11] Personal data may only be made if the Required by law or the person concerned has expressly agreed to do so. The processing This data is permissible even if it is absolutely necessary to provide legal To assert, exercise or defend claims against the person concerned.

If the processing of particularly protected data is planned, the Data protection supervisor Information in advance.

[10] See Xv.
[11] See Xv.

1.7 Automated individual decisions

Automated processing of personal data, through which individual personality traits are (e.g. credit worthiness) must not be the exclusive basis for the assessment of the For decisions with negative legal consequences or significant adverse effects on the Concerned. The person concerned must be aware of the fact and the result of an automated Individual decision and the possibility of an opinion is given.

In order to avoid wrong decisions, a check and a plausibility check must be carried out by Be ensured by an employee.

1.8 User Data and Internet

When personal information is collected, processed and used on Web pages or in apps Concerned shall be provided with data protection information and, where appropriate, cookie Inform. The data protection notes and any cookie notices must be integrated in such a way that Easily identifiable, immediately accessible and constantly available to those affected.

Are used to evaluate the usage behavior of websites and apps usage profiles (tracking), the parties concerned must in any case be informed of the data protection Be informed. Personal tracking may only be carried out if the national Right to do so or the person concerned has consented. If the tracking is done under a pseudonym, In the data protection information, the person concerned shall be entitled to object to the Be opened (Opt-out).

In the case of web pages or apps in a domain subject to registration, access to personal Data, the identification and authentication of the persons concerned shall be In such a way as to ensure that adequate protection is achieved for the respective access.

2. Employee data

2.1 Data processing for the employment relationship

The employment relationship may be subject to the processing of the personal data The reasoning, implementation and termination of the employment contract are necessary. In the Initiation of an employment relationship, personal data may be processed by applicants Be. Upon refusal, the applicant's data shall be taken into account in the light of evidence deadlines, unless the applicant has in another storage for a subsequent selection process. Consent is also used for the use of Of the data for further application procedures or prior to the transfer of the application to Affiliates Required.

In the existing employment relationship, data processing must always be based on the purpose of the employment Provided that one of the following authorisations does not apply to the Data processing.

During the initiation of the employment relationship or in the existing employment relationship the collection of further information on the applicant in the case of a third party is necessary to take into account the respective national legal requirements. In case of doubt, a To obtain the consent of the person concerned.

For processing of personal data which are in the context of the employment relationship are not originally intended to fulfil the employment contract, a legal framework must be Legitimacy. This can be regulated by legal requirements, collective Employees ' representatives, a consent of the employee or the legitimate interests of the of the company.

2.2 Data processing due to legal permission

The processing of personal employee data is permissible even if state Require or permit data processing in accordance with the provisions of this Regulation. The type And the scope of the data processing must be for the legally permissible data processing be required and shall be governed by this legislation. If there is a legal Scope of action, the protection-worthy interests of the employee must be taken into Be.

2.3 Collective arrangements for data processing

If processing goes beyond the purpose of contract processing, it is also Permitted if it is allowed by a collective scheme. Collective arrangements are collective agreements Agreements between employers and employee representatives within the framework The possibilities of the respective labour law. The rules must be based on the specific The purpose of the desired processing and are covered by the state data privacy law. Gestaltbar.

2.4 Consent to data processing

Processing of employee data may take place on the basis of the consent of the person concerned.

Consent declarations must be made voluntarily. Involuntary consent are ineffective. For reasons of evidence, the declaration of consent is basically written or electronically. If the circumstances do not permit this, the consent may be given orally. In any case, their issuance must be duly documented Be. In the event of an informed voluntary disclosure of data by the person concerned, consent may be Be accepted if national law does not prescribe explicit consent.

Prior to consent, the person concerned must, in accordance with IV. 3. This Privacy policy Be informed.

2.5 Data processing due to justified interest

The processing of personal employee data may also take place if this is necessary to achieve the of a legitimate interest deR Geocollect GmbH is required. Legitimate Interests are generally legal (e.g. the assertion, exercise or defence Legal claims) or economically (e.g. valuation of companies).

The processing of personal data on the basis of a legitimate interest must not be Where there is an indication in individual cases of the need to protect the interests of The employee's interest in the processing. The existence of protection-worthy Interests must be checked for any processing.

Control measures requiring processing of employee data may only be carried out in the If there is a legal obligation to do so or if there is a justified reason to is given. Even in the event of a justified reason, the proportionality of the of the control measure. The legitimate interests of the company in the Implementation of the control measure (e.g. compliance with legal requirements and intra-company Must be against a possible protection worthy of the interest of the the measure concerned shall be weighed against the exclusion of the measure and the may only be carried out if they are appropriate. The legitimate interest of the Company and the potential protective interests of employees must be protected against any be identified and documented. In addition, according to national law, Existing further requirements (e.g. co-determination rights of the employee representation and information rights of the parties concerned).

2.6 Processing of particularly protected data

Personal data which are particularly protected may only be used under certain conditions Be processed. Particularly protective data are data on the racial and Ethnic origin, political opinions, religious or philosophical beliefs, About trade union affiliations or about health or sex life of the person concerned. Under state law, further categories of data may be considered particularly Protected or the content of the categories of data is filled in differently.

Similarly, data relating to offences may often only be subject to specific, state- Conditions laid down in the law.

The processing must be expressly permitted or required by law Be. In addition, processing may be permitted if it is necessary for the responsible Meet their rights and obligations in the field of labour law Can. The employee may also voluntarily consent to the processing.

If the processing of particularly protected data is planned, the Data protection supervisor Information in advance.

2.7 Automated decisions

In so far as personal data are processed automatically in the employment relationship, are evaluated by individual personality traits (e.g. in the context of personnel selection or the evaluation of skill profiles), such automated processing may Not be the exclusive basis for decisions with negative consequences or significant affect the employees concerned. To avoid wrong decisions, Must be ensured in automated procedures that a substantive assessment of the By a natural person and that assessment is the basis for the implementation of the Decision. The employee concerned must also be aware of the fact and the result of An automated individual decision and the possibility of an opinion be given.

2.8 Telecommunications and Internet

Telephone systems, e-mail addresses, intranet and Internet as well as internal social networks are Primarily in the context of the company's operational tasks. Put. They are work equipment and company resource. They may be used within the Applicable legislation and the company's internal guidelines. In Case of permitted use for private purposes, the telecommunications secrecy and the respective Comply with national applicable telecommunications law as far as they are applicable.

A general monitoring of telephone and e-mail communication or the intranet and Internet usage does not take place. To prevent attacks on the IT infrastructure or Individual users can take protective measures at the transitions into the Geocollect-Network implemented That block technically damaging content or analyze the patterns of attacks.

For reasons of security, the use of telephone systems, e-mail addresses, Of Intranets and the Internet as well as the internal social networks.

Personal evaluations of this data may only be made in the case of a specific Justified suspicion of infringement of laws or directives enR Geocollect GmbH Be. These checks may only be carried out by identifying areas, while respecting the principle of proportionality Be. The respective national laws must be observed as well as The existing Policies.

VI. Transfer of personal Data

A transmission of personal data to recipients outside the GeoCollect GmbH or to recipients within the GeoCollect GmbH is subject to the admissibility requirements of the processing of personal data under Section V. The recipient of the data must be obliged to use them only for the specified purposes.

In the case of a data transfer to a recipient outside the GeoCollect GmbH in a third country [12], this must guarantee a level of data protection equivalent to this data protection guideline. This does not apply if the transfer is due to a legal obligation.

If personal data are Society Based in the European Economic Area to a Affiliated Company Established outside the European Economic Area[13] (third country), the data-importing company shall be obliged to All inquiries of the supervisory authority responsible for the data exporting company with And the findings of the supervisory authority with regard to the transmitted Data.

In the event of a data subject's infringement of this Privacy Policy by a data subject, the data-exporting company established in the European Economic Area undertakes to assist those whose data have been collected in the European Economic Area both in providing fact-finding information and ensure the enforcement of its rights under this Privacy Policy to the Data Importing Company. In addition, the person concerned is entitled to assert his rights against the data-exporting company. In the event of an alleged infringement, the data-exporting company must provide evidence to the data subject that the data-importing company in a third country is not responsible for any further processing of the data received in breach of this privacy policy.

In the case of transfer of personal data from a company established in the European Economic Area to a related company established in a third country, the data submitting body shall have the data subject in the European Economic Area for attributable breaches of the company established in a third country against liability to this privacy policy, as if the data-transmitting body had committed the infringement. Jurisdiction is the competent court at the headquarters of the data-exporting body.

[12] See Xv.
[13] See Xv.

VII. Order data Processing

An order data processing occurs when a contractor is charged with the processing of personal data without the responsibility for the associated businesspRozess is transferred. In these cases, The External Contractors and Geocollect GmbH An agreement on an order data processing Complete. The contracting company retains the full Responsibility for the correct execution of the data processing. The Contractor May Process personal data only within the framework of the instructions of the client. In The following specifications must be followed in order to grant the contract; The contracting Department must ensure its implementation.

1. The contractor shall, in accordance with its suitability, ensure the necessary technical and organisational protection measures.

2. The order must be given in text form. The instructions for data processing and To document the responsibilities of the client and the contractor.

3. The Data protectionRepresentative The contractual standards provided must be Be observed.

4. Prior to the commencement of data processing, the client must be obliged to comply with the of the contractor. Compliance with data security requirements Can prove a contractor in particular by presenting an appropriate certification. Depending on the risk of data processing, control may be required during the contract period Repeated regularly.

5. In the case of cross-border processing of order data, the respective national Requirements for the transfer of personal data abroad. In particular, the processing of personal data from the European Union may be The economic area in a third country only if the contractor has a The Data Protection directive.

Appropriate instruments Can be:

A. Agreement of the EU standard contract terms for order data processing in third countries With the contractor and potential subcontractors.

B. Participation of the contractor in a certification system recognised by the EU To create an adequate level of data protection.

C. Recognition of binding company rules by the contractor to create a Appropriate level of data protection by the relevant data protection supervisory authorities.

VIII. Rights of the person concerned

Each person concerned may exercise the following rights. Your assertion is immediately The person responsible for the work and shall not be subject to any Disadvantages.

1. The person concerned may request information on which personal data Origin is stored about it for what purpose. If the employment relationship Right of access to the respective labour law in the documents of the employer. (e.g. personnel file), they shall remain unaffected.
2. If personal data are transmitted to third parties, it must also be possible to identify the Recipients or by the categories of recipients.
3. Should personal data be incorrect or incomplete, the person concerned may Rectification or amendment.
4. The person concerned may, for the purposes of the processing of his personal data, Advertising or market and opinion research. For these purposes, The data is locked.
5. The person concerned is entitled to request the deletion of his data if the legal basis The processing of the data is missing or dropped. The same applies in the case That the purpose of data processing is not due to time lapse or other reasons. Is. The existing retention obligations and the deletion of any protection worthy of the Interests must be respected.
6. The person concerned has a fundamental right of objection against the processing of his data, To be taken into account when its protection worthy of interest is due to a particular The personal situation, the interest in the processing outweighs. This does not apply if a Legislation to carry out the processing.

In addition, any person concerned may be subject to the data in paragraphs III. 2, IV., V., vi., IX., X, and XIV. Third-party beneficiary in accordance with paragraph 3, where an undertaking which has has undertaken to comply with the Data Protection Directive, the provisions of which And he is thus injured in his right.

IX. Confidentiality of processing

Personal data are subject to data confidentiality. An unauthorized collection, processing or use is forbidden to the employees. Any processing that is a Employee without being entrusted with the performance of his duties and in accordance with the to be entitled. There is a need toTo-Know-Principle: Employees may only access Personal data if and to the extent necessary for their respective tasks. is required. This requires the careful division and separation of roles and responsibilities As well as their implementation and maintenance within the framework of authorization concepts.

Employees may not personal data for their own private or economic Use it, transmit it to unauthorized persons or otherwise make it accessible.

Employees must be employed at the beginning of the employment relationship Obligation to maintain the confidentiality of data. This obligation Also After the end of the employment relationship.

X. Security of processing

Personal data are at all times against unauthorized access, unlawful processing Or disclosure, as well as to protect against loss, falsification or destruction. This Applies irrespective of whether the data processing is done electronically or in paper form. Before Introduction of new methods of data processing, in particular new IT systems, are technical Organisational measures for the protection of personal data and to establish and implement it. These measures have been taken at the state of the art, the processing of Risks and the protection needs of the data (determined by the information classification process) To Orient. In particular, the responsible department can Consult its Information Security Officer (ISO) and Data protection coordinator.

The technical and organisational measures for the protection of personal data are part of the Of Enterprise Information security management and must be continuously Technical developments and organizational changes.

XI. Data protection control

Compliance with the privacy policy and the applicable data protection laws will be regularly Reviewed by data protection audits and other controls. The implementation is The Privacyor commissioned external auditors. The results of the data protection controls are Data protection supervisor mItzuteilen.

On request, the results of data protection controls will be The competent Datenschutzaufsichts-Authority. The The competent Data protection supervisory authority may, within the limits of its national law, Control of compliance with the provisions of this directive. Perform.

XII. Data protection incidents

Each employee should be given his or her supervisor or The Data protection supervisorn Immediate cases of violations of this Privacy Policy or other provisions relating to the protection of personal data (data protection incidents[14]) Report. The manager responsible for the function or unit is Committed to the Data protection supervisor Data protection incidents immediately.

In cases of

- Unlawful transfer of personal data to third parties,
- Unlawful access by third parties to personal data, or
- In case of loss of personal data

Are the reports provided for in the company to the management Be carried out without delay in order to ensure that, under state law, existing reporting obligations Data protection incidents can be met.

[14] See Xv.

XIII. Responsibilities and sanctions

DHe/the managing directors and the heads of are responsible for the Data processing in your area of responsibility. They are therefore obliged to ensure that That the requirements of the legal framework contained in the Data Protection directive Data protection (e.g. national reporting obligations). It is a management task Managers, through organisational, personnel and technical measures To ensure proper data processing in compliance with data protection.

The implementation of these guidelines is the responsibility of the responsible employees. In Data protection controls by public authorities is the Data protection supervisor Immediately Information.

The respective Head are obliged to inform the Data protection supervisor In His To support their activities. The For Business processes and projects professionally responsible mustEn Data protection supervisor Inform in good time about new processing of personal data. In the case of data processing projects, Particular risks to the personal rights of the persons concerned. can result, the Data protection supervisor Even before the start of processing to participate. This applies in particular to special protection-related personal Data. Managers must ensure that their employees have the necessary level of Be trained to protect data. Improper processing of personal data or other violations of data protection law are also prosecuted in many States and may be subject to claims for damages. infringements for which Individual employees are responsible may lead to labour law penalties.

XIV. The Data protection officer

The Data Protection Officer, as an internal, non-technical body, works towards compliance with national and international data protection regulations. He is responsible for privacy policies and monitors compliance. The data protection officer is appointed by the management of GeoCollect GmbH.

Anyone affected can contact the data protection officer with suggestions, requests for information, or complaints in connection with data protection or data security issues. Inquiries and complaints are treated confidentially on request.

The privacy officer's decisions to remedy the breach of data protection must be taken into account by the management and the respective department heads. Inquiries from supervisory authorities must always be brought to the attention of the data protection officer.

The Data Protection Officer Can Be achieved as follows:

Geocollect GmbH
Data protection officer

Milchstr. 8

D20148 Hamburg, Germany

E-mail: Datenschutz@geocollect.de

XV. Definitions

- An appropriate level of data protection for third countries will be adopted by the EU Commission Recognised when the core of the private sphere, as it is in the EU Member States, is essentially protected. The EU Commission shall take into account, in its decision, all circumstances which arise from a data A category of data transfers. This Includes the assessment state law as well as the relevant rules and security measures in force. A.
- Data is anonymized when a person's reference is permanent and not Can be produced more or if the person reference is only disproportionately Considerable effort in time, cost and manpower could be restored.
- Particularly protective data are data on racial and ethnic origin, on the Political opinions, religious or philosophical beliefs, trade union affiliations Or on the health or sexual life of the person concerned. Because National law, further categories of data may be classified as particularly worthy of protection or the contents of the data categories are filled in differently. Similarly, data, Offences, are often only subject to special circumstances set up by state law and Requirements are processed.
- For the purposes of this data Protection directive, any natural person who has the data Be processed. In some countries, legal persons may also be affected.
- Data protection incidents are all events where there is a reasonable suspicion that the Personal data unlawfully spied, collected, altered, copied, transmitted or used. This can be due to actions by third parties as well as employees Refer.
- Third party is anyone outside the affected person and the person responsible for data processing Place. Data Processor are not third parties within the EU in the sense of data privacy law, Because they are legally assigned to the responsible body.
- Third countries within the meaning of the Data Protection Directive are all States outside the European Union/EEA. States whose level of data protection are exempted from the EU Commission has been recognised as appropriate.
- Consent is a voluntary, legally binding declaration of consent in a data processing.
- The processing of personal data is required if the intended purpose or The legitimate interest without the respective personal data or only with is to be achieved with disproportionately high costs.
- The European Economic Area (EEA) is an economic area associated with the EU, the Norway, Iceland and Liechtenstein.
- Personal data are all information about a specific or identifiable Natural person. A person is identifiable, for example, when the personal reference is A combination of information with even randomly available additional knowledge produced can be used.
- Transmission is any disclosure of protected data by the responsible body To third parties.
- Processing of personal data, any person with or without the help of automated procedures Carried out for the collection, storage, organisation, retention, alteration, Use, disclosure, transmission, dissemination or combination and Data comparison. This includes the disposal, deletion and blocking of data and Disks.

Geocollect GmbH
Milchstr. 8
D-20148 Hamburg, Germany