Privacy Policy

Data protection information and declaration

Object-Guard Inc. (hereinafter referred to as "the company"), in its capacity as a Data Controller, processes the personal data provided by you during the contract conclusion process related to the contractual relationship. We are committed to fully complying with all legal requirements governing the management of personal data, particularly adhering to the regulations stipulated by the state of California.

By entering into any contract with the company (for installation, repair, maintenance, monitoring), you acknowledge and agree that the monitoring station is located outside the United States and operates in Europe due to special security considerations. Furthermore, you acknowledge that the strict data protection directive of the GDPR applies to it.

In the event of any contract concluded with the company, you understand that your data will be used solely for the purpose of fulfilling the contract and will never be disclosed to third parties.

Name and contact details of data controller:

Company name: “Object-Guard” Inc.

Office& P.O. Box: 99 South Almaden Blvd., Suite 600, San Jose, CA, 95113,

Telephone: +1 (669) 499 3500

E-mail: monitoringcentre@object-guard.com

Tax:

Web: www.object-guard.com

I. During data management, we follow the following basic principles:

• The Data Controller processes personal data solely for the specified purposes and within the designated timeframe. Only essential personal data necessary for achieving the intended purpose of data management is handled by the Data Controller.

• Personal data obtained by the Data Controller during data management can only be accessed by individuals who are authorized on behalf of the Data Controller, including those in contractual relationships (e.g., subcontractors) or individuals in an employment relationship

with the Data Controller, provided they have a relevant role related to the specific data management process.
The scope of individuals affected includes natural persons who have entered into contracts with Object-Guard Inc., representatives and contacts of non-natural persons, as well as all individuals affected by contracts and their derivative representatives.
The types of personal data handled include:

1. Name
2. Address
3. Telephone numbers
4. Email addresses
5. Data related to the protected object, which are only necessary for the fulfillment of the contract

These types of personal data are detailed separately for each data management process.
Source of data: Exclusively voluntary provision of data by those concerned.
The deadline for data storage is as follows: Until the goal of data management is achieved, as a general rule. After the termination of the contract, the data will be stored until the general civil law limitation period expires, which is typically 5 (five) years. This duration takes into account the storage and deadline requirements of other documents created by law.

II. Method of data management: electronic and paper-based.
II/a. The personal data obtained and processed by Object-Guard Inc. is stored at various locations, including Object-Guard Inc. headquarters, sites and subcontractor sites, European servers, and U.S. servers.
Data transmission and processing are handled by Object-Guard Inc. and its subcontractors. Additionally, in the event of official requests, data may be shared with relevant authorities such as the police, fire department, FBI, government agencies, IRS, and others.

III. The purpose, legal basis and scope of personal data processing, as well as the duration of data processing:
III.1. Direct inquiry

We may contact you through a personal visit. In such a case, if you wish, we will send you our offer.

The legal basis for data management is your consent, which you can withdraw at any time. However, please note that withdrawing your consent does not affect the legality of data processing that occurred before the withdrawal. It's important to understand that if we are unable to process the personal data you provide, it may hinder our ability to respond to your questions or requests.

Purpose of data management: Contacting and sending the offer.

The time of data management is as follows: Messages and received personal data will be deleted within 30 (thirty) days if the offer is rejected. However, in case of acceptance of the offer, we will proceed according to the data management procedures applicable to the conclusion of the contract. It's important to note that no data processor will be used, nor will data be forwarded in this process.

III. 2. Recording of telephone conversations

Our company records both incoming and outgoing phone calls and manages the personal data provided during these calls. When initiating a call, our dispatcher will inform you that the call will be recorded. Upon request, audio recordings will be made available in accordance with the regulations outlined in the General Terms and Conditions (GTC).

The legal basis for data management differs based on the nature of the contract. If the contract is concluded with you as a private person, the legal basis is the performance of the contract. In other cases, the legal basis for data management is your consent. You have the right to withdraw your consent at any time; however, the withdrawal does not affect the legality of data processing that occurred prior to the withdrawal.

Purpose of data management: Recording and retrievability of instructions, as well as complaint handling.

Time of data management: Recorded calls are stored on an active server for 3 years and then archived for another 2 years. No data processor will be used or data will be forwarded.

III.3. Audio recording recorded through an emergency call unit

Scope of processed data: recorded conversation (voice recording)

Purpose of data management: Verification of the existence of an emergency and the appropriateness of the measure, traceability, and complaint handling.

Time of data management: Recorded conversations are stored for six (6) months from the date of recording, after which they are automatically deleted.

No data processor will be used.

Data transfer: Upon request from the individual affected by the data management, the audio recordings will be provided to them. Additionally, the recordings may be forwarded to the police or other authorities authorized by law. As part of the verification of contract performance, if data is transmitted to the entitled party, personal data of other individuals will be either deleted or rendered unrecognizable. It is ensured that data will not be transferred to third countries.

ARC Record of all consumer complaint:

Complaints are handled both in writing and verbally, as outlined in our contact details provided above and in the upper General Terms and Conditions (GTC). If you engage in a contract with us as an individual and disagree with the complaint handling process, or if an immediate investigation of the complaint is not feasible, a record of the complaint must be created. This record should include the following details: the name and address of the consumer, the location, time, and method of presenting the complaint, a comprehensive description of the consumer's complaint, a list of any documents, records, or other evidence submitted by the consumer, our company's response to the consumer's complaint, and the signature of the individual recording the report. Additionally, except for verbal complaints conveyed by telephone or other electronic communication services, the signature of the consumer, along with the location and time of the meeting, should be included. For oral complaints communicated via telephone or other electronic communication services, a unique identification number for the complaint should be provided.

Purpose of data management: Complaint management.

Time of data management: We must keep the record of the complaint and the copy of the response for 5 (Five) years. Data will not be transferred or a data processor will be used.

V. Data management related to monitoring, installation, repair or maintenance services: If you enter into a service contract for property monitoring or maintenance, we process the following personal data in order to fulfill the contract:

surname and first name;

birth name and first name;

place and time of birth;
His mother's name;
Home address;
mailing address;
phone number;
e-mail address, and in case of e-invoice request, invoicing e-mail address;
secret identifier password.

To fulfill the contract, it is necessary to provide the data of the person who can be notified in the specific cases outlined in the contract. The information required for the person to be notified includes the surname and first name, telephone number, and secret password of the authorized person.

As the end user, it is your responsibility to inform the person to be notified and obtain their consent to provide their data. If the person to be notified informs the Data Controller, i.e., our Company, that they do not consent to the provision or further processing of their data, the Data Controller will promptly delete the data of the individual from the list of those to be notified. In such cases, it is your responsibility to provide the data of another suitable person to be notified to ensure the continued provision of the service. Our Company, acting as the Data Controller, bears no responsibility for any damages resulting from the failure or delay in fulfilling this requirement.

If you are acting as a representative of a legal entity, an organization without legal personality, or a condominium, in addition to the data you represent, we will need the following personal information: full name, phone number, and email address.
If the identity of the client and the bill payer are separate, in addition to your data, it is necessary to provide the bill payer's data as described above.
Legal basis for data management: Legitimate interest in the performance of a contract.
Purpose of data management: Preparation, creation, fulfillment, contact and invoicing of the contract. The provision of data is a condition for concluding a contract.

Time of data management: After the termination of the contract, personal data will be archived and stored for 6 (six) months, unless a complaint handling procedure or legal dispute is in progress. In such cases, the data will be stored until a decision, ruling, or notification on the conclusion of the procedure or legal dispute is reached.
We store documents and data required by current accounting and tax law rules for 3 (three) years. After that period, the personal data will be deleted.
Data transfer: The processed data may be shared with our subcontractors. These subcontractors have acknowledged the contents of this data management information as binding for them and have declared their compliance with data protection regulations. Upon official request, we may also forward the processed data to the police. No data processor will be used in this process.

VI. Data management related to website viewing:
When you visit our website www.object-guard.com, certain data, including your device's IP address (e.g., laptop, PC, phone, tablet), is automatically recorded. This recorded data is logged by the web server serving the website without any special declaration or action from you. The system then generates statistical data from this information. These data are used solely in an aggregated and processed form for purposes such as identifying and correcting errors in our services, improving their quality, and for statistical analysis. It's important to note that this data cannot be combined with other personal data unless required by law.
The purpose of data management includes the technical development of the IT system, monitoring the operation of the service, compiling statistics, and protecting the rights of visitors. Additionally, in cases of abuse, the data may be utilized to identify the source of the abuse in collaboration with the visitors' internet service provider and relevant authorities. It's important to note that providing data is mandatory, and access to the website is not possible without it.
Duration of data management: 30 (thirty) days from the date of viewing the website. VI.1. Cookies and similar technologies:

A cookie is a small text file that is stored on the hard drive of a computer or mobile device for a set expiration time. It becomes active and reports back to the web server on subsequent visits. Websites utilize cookies to record information related to the visit, such as pages visited, time

spent on pages, browsing data, and exits, as well as personal settings. This tool is used to create a user-friendly website and enhance the online experience of visitors. There are two types of cookies: "session cookies" and "permanent cookies", both of which are stored in the browser until the user deletes them.

• "Session cookies" are only stored temporarily by the computer, notebook, or mobile device, until you leave the given website. These cookies assist the system in remembering information so that you do not have to repeatedly enter or fill in that information. The validity period of session cookies is limited to the user's current session, and their purpose is to prevent data loss, for example, when filling out a longer form. This type of cookie is automatically deleted from the visitor's computer at the end of the session or when the browser is closed.

• "Persistent cookies" are stored on the computer, notebook, or mobile device even after leaving the website. These cookies enable the website to recognize you as a returning visitor. They are suitable for identifying you through a server-side identifier-user association, making them essential for correct operation in cases where user authentication is necessary, such as in an online store, netbank, or webmail service. Persistent cookies do not contain personal data themselves and are only effective in identifying the user when combined with the order stored in the server's database. However, the risk associated with such cookies is that they do not actually identify the user, but rather the browser. For instance, if someone accesses an online store from a public place, such as an internet cafe or library, and fails to log out upon leaving, another person using the same computer may gain unauthorized access to the online store under the original user's name.

Our company uses cookies that are essential for the operation of the website and statistical data collection cookies. Purpose and duration of data management: Our website utilizes session cookies to track your actions during your visit. These cookies record your interactions, such as entries made in request forms, and the addresses you viewed to facilitate navigation. This data is deleted when you leave the website. The use of session cookies is essential for the proper functioning of the website, and without them, certain features may not work correctly.

Additionally, we employ cookies that collect statistical data during their operation. These cookies monitor your usage patterns on the website, including the topics you view, your clicks, scrolling behavior, and visited pages. However, they only collect information anonymously. This enables us to gather insights into website traffic, such as the number of monthly visitors,

and helps us tailor our site to better meet user needs. Google Analytics is also utilized to collect such data, identified by the "_gat" extension cookie. For more information about Google Analytics data protection policies, please refer to the provided link:
https://support.google.com/analytics/answer/6004245?hl=hu

VI.2. Data management related to Instagram availability:
Our company maintains a presence on Instagram under the username #alarmreacting. Instagram users can choose to subscribe to our page by clicking the "like" or "follow" button, and unsubscribe by clicking the "unfollow" button or adjusting their message wall settings to remove our updates. By following us, your profile becomes visible to us, but we do not store or manage any data about it internally. We solely utilize this platform to share our news updates. Meta (Facebook), the parent company of Instagram, acts as an independent data controller for the platform. You can find information about their data management practices at the following links:
- https://www.facebook.com/policies/cookies/
- https://www.facebook.com/about/privacy/update
We do not utilize any data processors or transfer data outside of Instagram.
Legal basis for data management: Your consent. You have the right to withdraw your consent at any time by unfollowing us. However, the withdrawal of consent does not affect the legality of data processing prior to the withdrawal.
Purpose of data management: The purpose is to inform you about current information, products, news related to us, and to provide educational articles and materials.
Duration of data management: Our posts will only appear in your news feed as long as you choose to follow us. If you unfollow us, our posts will no longer appear in your feed. You can still access our posts even if you do not follow us, but you will not receive separate notifications about them.
VII.. Possibilities for legal enforcement (rights concerned):
Right to information
At the request of the data subject, the Data Controller shall provide comprehensive information regarding the data subject's managed or processed data, including its source, purpose, legal basis, duration of processing, details of the data processor, activities related to data processing, circumstances, effects, and consequences of any data protection incidents, as well as measures

taken to prevent them. Additionally, the data subject has the right to know who has accessed their personal data and for what purpose. If the data has been forwarded, the data subject can also request an extract from the data transfer register.

The Data Controller must provide this information promptly, within 30 days at the latest, in an understandable format. The provision of information is free of charge for the first request in a given year. However, the Data Controller may refuse to provide information if the requester has already made a similar request in the current year, or if the requester fails to credibly prove their identity as the data subject. Information may also be denied if prohibited by law or if the Data Controller receives data with restrictions on the right to information from another data controller.

Information will be provided only to the data subject or individuals authorized by them in a legally binding private document. In case of refusal, the Data Controller will specify the legal basis for the refusal. At the request of the data subject, the Data Controller shall provide comprehensive information regarding the data subject's managed or processed data, including its source, purpose, legal basis, duration of processing, details of the data processor, activities related to data processing, circumstances, effects, and consequences of any data protection incidents, as well as measures taken to prevent them. Additionally, the data subject has the right to know who has accessed their personal data and for what purpose. If the data has been forwarded, the data subject can also request an extract from the data transfer register.

The Data Controller must provide this information promptly, within 30 days at the latest, in an understandable format. The provision of information is free of charge for the first request in a given year. However, the Data Controller may refuse to provide information if the requester has already made a similar request in the current year, or if the requester fails to credibly prove their identity as the data subject. Information may also be denied if prohibited by law or if the Data Controller receives data with restrictions on the right to information from another data controller.

Information will be provided only to the data subject or individuals authorized by them in a legally binding private document. In case of refusal, the Data Controller will specify the legal basis for the refusal.

Right to rectification

The data subject has the right to request the correction of their personal data if it is inaccurate or incomplete. The Data Controller must correct any inaccuracies without undue delay upon receiving such a request. If the Data Controller has accurate data available, they will promptly update the personal data.

The Data Controller will review correction requests promptly, within 30 days at the latest, and inform the data subject in writing of the decision and any further steps that may be taken.

Right to erasure

The data subject has the right to request the deletion of their personal data from the Data Controller without undue delay if one of the following reasons applies:

- The personal data are no longer necessary for the purpose for which they were collected or processed.
- The data subject withdraws their consent, and there is no other legal basis for the data processing.
- The data subject objects to the processing of their data, and there are no overriding legitimate grounds for the processing.
- The personal data has been unlawfully processed.
- The deletion of personal data is required to comply with a legal obligation under EU or member state law applicable to the Data Controller.

The right to restrict data processing

The data subject has the right to request the Data Controller to restrict the processing of their personal data if one of the following conditions is met:

- The data subject contests the accuracy of the personal data, in which case the restriction applies until the accuracy of the personal data is verified.
- The processing of personal data is unlawful, and the data subject opposes the erasure of the data and instead requests the restriction of its use.
- The Data Controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise, or defense of legal claims.
- The data subject has objected to the processing of their data; in this case, the restriction applies until it is determined whether the legitimate grounds of the Data Controller override those of the data subject.

Right to protest

The data subject has the right to object to the processing of their personal data. The Data Controller shall promptly review the objection, within 30 (thirty) days of its submission, and make a decision on its merits, informing the applicant of the decision in writing.

The data subject may object to the processing of their personal data in the following cases:

- If the processing or transmission of personal data is necessary solely for the fulfillment of the legal obligation of the Data Controller or for the legitimate interests of the Data Controller, data recipient, or a third party, except in cases where data processing is mandatory.
- If personal data is used or transmitted for the purpose of direct marketing, public opinion polls, or scientific research.
- In other cases defined by law.

If the data subject's objection is found to be well-founded, the Data Controller shall cease the processing of the data, including any further data collection and transmission. They shall also delete or limit the data and inform all parties to whom the personal data affected by the objection was previously transmitted about the objection and the measures taken based on it. Those parties are obliged to take action to enforce the right to object.

If the Data Controller does not agree with the objection of the data subject, or if they fail to meet the deadline for examining and deciding on the objection, the data subject may appeal to the court within 30 days from the notification of the decision or the last day of the deadline.

Data subject rights related to automated decision-making and profiling

The Data Subject has the right to request that a decision based solely on automated data processing, which would have a legal effect on them or similarly significantly affect them, not be applied to them, unless the decision falls under one of the following exceptions:

1. It is necessary to conclude or fulfill a contract between the Data Subject and the Data Controller.
2. It is permitted by EU or member state law applicable to the Data Controller, which also provides for suitable measures to safeguard the rights, freedoms, and legitimate interests of the Data Subject.
3. It is based on the explicit consent of the Data Subject.

In cases outlined in points 1 and 3, the Data Controller is obligated to implement suitable measures to safeguard the rights, freedoms, and legitimate interests of the Data Subject. These

measures should include, at minimum, the Data Subject's right to request human intervention from the Data Controller, to express their viewpoint, and to contest the decision.

The Data Controller notifies all recipients to whom the personal data was disclosed about any corrections, deletions, or restrictions on data processing, unless such notification is impossible or would require disproportionate effort. Upon request of the Data Subject, the Data Controller provides information about these recipients.

Informing the Data Subject about the data protection incident

If a data breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Controller must promptly notify the Data Subject of the breach. This notification should include a clear and understandable description of the incident, contact details of the data protection officer or another contact person for further information, potential consequences of the breach, and the measures taken or planned by the Data Controller to address the breach, including any steps to mitigate potential adverse effects.

The Data Subject need not be informed if any of the following conditions are met:

1. The Data Controller has implemented suitable technical and organizational safeguards, including encryption, to protect the data affected by the breach, making it unintelligible to unauthorized persons.
2. Following the incident, the Data Controller has implemented additional measures to reduce the likelihood of similar risks to the rights and freedoms of the Data Subjects in the future.
3. Providing notification would be excessively burdensome or technically infeasible.

In such scenarios, Data Subjects must be informed through publicly available channels or equivalent measures that ensure effective communication with the affected individuals. If the Data Controller has not yet notified the Data Subjects of the data protection incident and the supervisory authority determines that the incident poses a high risk, it may instruct the Data Controller to inform the Data Subjects. Alternatively, the authority may determine that there are conditions under which notification is not necessary.

The Data Controller ensures that the Data Subject's rights outlined in this chapter and in relevant legislation are easily exercisable. Refusal to comply with a Data Subject's request to exercise their rights is not permissible unless it is proven that the Data Subject cannot be identified. The Data Controller promptly informs the Data Subject of the measures taken in response to their request to exercise their rights, doing so within 30 days of receiving the

request at the latest. In cases where necessary due to the complexity of the request or the volume of requests, this deadline may be extended by up to two months. The Data Controller notifies the Data Subject of any deadline extensions, providing reasons for the delay, within one month of receiving the request.

If possible, the information must be provided electronically, unless the Data Subject requests otherwise.

If the Data Controller fails to take measures following the Data Subject's request, it must promptly inform the Data Subject of the reasons for the failure to act, doing so within 30 days of receiving the request. Additionally, the Data Subject must be notified that they have the right to file a complaint with a supervisory authority and to pursue legal action to seek redress.

The data controller provides information on personal data management, information on the Data Subject's rights, and the measures free of charge. However, if the Data Subject's request is clearly unfounded or, especially due to its repetitive nature, excessive, the Data Controller may consider the administrative costs associated with providing the requested information or taking the requested action.

1. you can charge a fee, or
2. may refuse to take action based on the request.

It is the responsibility of the Data Controller to prove that the request is clearly unfounded or excessive. If the Data Controller has reasonable doubts about the identity of the natural person who submitted the request, it may request the provision of additional information necessary to confirm the Data Subject's identity.

If the Data Subject believes that their rights related to the management of their personal data have been violated, they can contact the Data Controller for information and to exercise their rights using the contact details provided earlier.