

TABLE OF CONTENTS

1	INTRODUCTION.....	2
2	NAME AND ADDRESS OF THE CONTROLLER	3
3	NAME & CONTACT DETAILS OF REPRESENTATIVE	3
4	CONTACT DETAILS OF DATA PROTECTION OFFICER	4
5	SUPERVISORY AUTHORITY.....	4
6	HOW WE USE YOUR PERSONAL DATA.....	5
7	COLLECTION OF GENERAL DATA, PURPOSE, AND USE	6
8	HANDLING OF SENSITIVE DATA	8
9	SOURCE OF PERSONAL DATA.....	8
10	DO NOT SELL MY PERSONAL INFORMATION	10
11	CONTACT POSSIBILITY VIA THE WEBSITE.....	10
12	RIGHTS OF THE DATA SUBJECT UNDER GDPR	10
13	RIGHTS OF THE DATA SUBJECT UNDER CCPA.....	14
14	VERIFICATION PROCESS FOR IDENTITY OF REQUESTOR	16
15	TRANSFER OF PERSONAL DATA.....	17
16	RETENTION PERIODS FOR PERSONAL DATA.....	18
17	ROUTINE ERASURE AND BLOCKING OF PERSONAL DATA.....	18
18	AUTOMATED DECISION-MAKING.....	19
19	DATA PROTECTION MEASURES	19
20	PERSONS UNDER THE AGE OF 18	20
21	DATA COLLECTED IN 12 MONTHS.....	21
22	PRIVACY POLICY UPDATE.....	21

PRIVACY NOTICE

Last Updated: Friday, July 19, 2024

1 INTRODUCTION

- 1.1 We are delighted that you have shown interest in the services of G&H Automation Services LLC ("GHAS" "We" or "Company"). This document contains the privacy provisions with regard to your access and use of our website accessible via www.gnhautomation.com ("Website"). Data protection is a particularly high priority for the management of GHAS. The use of the Website of GHAS is possible without any indication of personal data; however, if a Data Subject wants to use special services via our Website, processing of personal data may 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.
- 1.2 The processing of personal data, such as the name, address, email address, or telephone number of a Data Subject shall always be in line with the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and in accordance with the country-specific data protection regulations applicable to GHAS. Utilizing 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 through this data protection declaration of the rights to which they are entitled.
- 1.3 As the controller, GHAS has implemented numerous technical and organizational measures to ensure the complete protection of personal data processed through this Website. However, Internet-based data transmissions may, in principle, have security gaps, so absolute protection may not be guaranteed. For this reason, every Data Subject is free to transfer personal data to us via alternative means, e.g., by email.

2 NAME AND ADDRESS OF THE CONTROLLER

Controller for 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:

Name: G&H Automation Services LLC

Address: 31-12 33rd Street, #2C,
Long Island City, NY 11106,
United States.

Email: support@gnhautomation.com

Website: <https://www.gnhautomation.com/>

3 NAME & CONTACT DETAILS OF REPRESENTATIVE

In accordance with data protection regulations, we provide the following information regarding our representatives:

3.1 EU Representative:

Email: eurep@gnhautomation.com

Address: Allée Félix Faure, Les Pavillons-sous-Bois,
Île-De-France, 93320

3.2 UK Representative:

Email: ukrep@gnhautomation.com

Address: Grégory Jannin, Unit 133832, PO BOX 7169,
Poole, BH15 9EL

For any inquiries or communication related to data protection matters, you may contact the appropriate representative based on your location. We are dedicated to facilitating communication and ensuring compliance with data protection requirements.

4 CONTACT DETAILS OF DATA PROTECTION OFFICER

Our legal team serves as the Data Protection Officer (DPO) responsible for ensuring compliance with data protection regulations. You can contact our legal team, acting in the capacity of the DPO, at the following details:

Name: GHAS Legal Team

Email: legal@gnhautomation.com

Address: G&H Automation Services LLC,
31-12 33rd street, #2C, Long Island City,
NY 11106, United States

Phone: +1 (917) 791-0561

If you have any questions, concerns, or requests related to the processing of your personal data or data protection matters, feel free to reach out to our DPO. We are committed to addressing your inquiries promptly and ensuring the protection of your privacy rights.

5 SUPERVISORY AUTHORITY

Data Subjects have the right to lodge a complaint with a supervisory authority if they believe that the processing of their personal data violates data protection regulations.

If you wish to exercise this right, you can find contact information for supervisory authorities worldwide through the following links:

UK: <https://ico.org.uk/>

EU: https://edpb.europa.eu/about-edpb/about-edpb/members_en

6 HOW WE USE YOUR PERSONAL DATA

Purpose/Activity	Type of Data	Lawful Basis of Processing	Legitimate Interests for Processing	Categories of Personal Data Obtained	Recipients or Categories of Recipients of Personal Data
Email Verification	Contact Information (Email)	Contractual Necessity or Consent	Providing contracted services, meeting specific client requirements	Email	Relevant internal teams based on the nature of the service
Gender Verification	Personal Information (Name)	Contractual Necessity or Consent	Providing contracted services, meeting specific client requirements	Name	Relevant internal teams based on the nature of the service
Phone Number Validation	Contact Information (Phone Number)	Contractual Necessity or Consent	Providing contracted services, meeting specific client requirements	Phone Number	Relevant internal teams based on the nature of the service
Data Migration	Various Data	Contractual Necessity	Providing contracted services, meeting specific client requirements	Relevant data based on the specific service provided	Relevant internal teams based on the nature of the service
Data Backup	Various Data	Legitimate Interest	Providing contracted services, meeting specific client requirements	Relevant data based on the specific service provided	Relevant internal teams based on the nature of the service
Other Services	Varied Data depending on the service	Contractual Necessity or Consent	Providing contracted services, meeting specific client requirements	Relevant data based on the specific service provided	Relevant internal teams based on the nature of the service
Client Management	Contact Information, Purchase History	Contractual Necessity, Legitimate interests	Fulfilling contractual obligations, Communication	Name, Address, Email, Phone, Purchase Details	Internal Departments (Sales, Support)
Employee Management	Personal Information, Employment History	Legal Obligation, Contractual Necessity	HR Processes, Payroll	Name, Address, Social Security Number, Bank Details	HR Department, Payroll Processor, Management
Marketing and Communication	Contact Information, Preferences	Consent, Legitimate Interest	Promoting products/services, Networking	Name, Email, Marketing Preferences	Marketing Department, CRM System
Compliance and Reporting	Various depending on regulatory requirements	Legal Obligation	Compliance with Laws and Regulations	Varies based on regulatory requirements	Regulatory Authorities, Legal Department

7 COLLECTION OF GENERAL DATA, PURPOSE, AND USE

7.1 Collection of Data. The Website of GHAS 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. The general data collected may be categorized as follows:

- ☐ Identifiers. Name, alias, postal address, IP address, or other similar identifiers. This data is collected to identify individuals, manage accounts, and facilitate communication.
- ☐ Contact Information. Email address and phone number. This data is collected to communicate with individuals, provide services, and respond to inquiries.
- ☐ Financial Information. Payment information, billing address. This data is collected to process transactions, fulfill orders, and manage financial accounts.
- ☐ Commercial Information. Records of products or services purchased, obtained, or considered. This data is collected to maintain records of transactions, analyze purchase patterns, and personalize offerings.
- ☐ Professional or Employment-Related Information. Job title, employer information, or performance evaluations. This data is collected to facilitate business relationships, provide professional services, and manage employment-related matters.
- ☐ Internet or Network Activity. Browsing history, search history, and interactions with our website. This data is collected to improve website functionality, personalize user experience, and analyze usage trends.

7.2 Purpose of collection. In accordance with applicable data protection regulations, GHAS collects data for the following purposes:

- ☐ Statutory Requirements. The provision of personal data is partly required by law (e.g., tax regulations) or can result from contractual provisions (e.g., information on the contractual partner).
- ☐ Necessity for Contract. If the processing of personal data is essential for the performance of a contract or pre-contractual measures, there may be a requirement to provide such data. For instance, the Data Subject is obliged to provide personal data when our company signs a contract

with them. Non-provision would have the consequence that the contract could not be concluded.

- ☐ Obligation of the Data Subject. Data Subjects may have an obligation to provide specific personal data, especially when entering into contractual agreements or fulfilling legal requirements.
- ☐ Consequences of Non-Provision. Failure to provide the required personal data may result in the inability to enter into a contract or fulfill contractual obligations. Additionally, non-provision may lead to legal consequences, such as non-compliance with statutory obligations.

Before personal data is provided by the Data Subject, it is advisable to contact us. We will clarify to the Data Subject whether the provision of personal data is required by law, or contract, or is necessary for the conclusion of the contract. We will also communicate any obligation to provide personal data and explain the consequences of non-provision. This ensures transparency and enables informed decisions by the Data Subject. If there are uncertainties or inquiries regarding the specific data required and the implications of non-provision, please contact us for clarification.

Use of Data. When using these general data and information, GHAS does not draw any conclusions about the Data Subject. Rather, this information is needed to:

- ☐ deliver the content of our Website correctly,
- ☐ optimize the content of our Website as well as its advertisements and running marketing campaigns,
- ☐ ensure the long-term viability of our information technology systems and website technology,
- ☐ for analytics purposes,
- ☐ run financial statistics, and
- ☐ provide law enforcement authorities with the information necessary for criminal prosecution in case of a cyber-attack.

Therefore, GHAS analyses data and information statistically, to increase the data protection and data security of our enterprise and achieve 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.

8 HANDLING OF SENSITIVE DATA

The Company handles sensitive personal information with strict adherence to the following principles:

- 8.1 Purpose Limitation. Sensitive information is collected and used solely for specified, legitimate purposes disclosed to the Data Subject.
- 8.2 Security Measures. Robust security protocols, including encryption and access controls, safeguard sensitive data from unauthorized access or disclosure.
- 8.3 Consent Requirement. Explicit consent is obtained before collecting or processing sensitive personal information, except where another legal basis applies.
- 8.4 Limited Disclosure. Sensitive information is shared with third parties only when necessary for the disclosed purposes or with explicit consent from the Data Subject.
- 8.5 Right to Limit Use. Data Subjects have the right to limit the use of their sensitive personal information through:
 - ☐ Opt-Out Options. Mechanisms to opt-out of using sensitive information for marketing or specific purposes.
 - ☐ Access and Correction. Ability to access, correct, or restrict further processing of their sensitive information where applicable.
 - ☐ Withdrawal of Consent. Option to withdraw consent for the processing of sensitive personal information, where consent is the legal basis.

9 SOURCE OF PERSONAL DATA

The personal data processed by us may be obtained from various sources, including but not limited to:

- 9.1 Data Subject. Data collected include without limitation name, email address, phone number, address, and account preferences.
 - ☐ Source. Provided directly by the Data Subject through interactions, inquiries, or service usage.
 - ☐ Reason. Collected to fulfill service requests, manage customer relationships, and provide personalized experiences based on preferences.

9.2 Contractual Partners. Data collected include without limitations business contact information (e.g., name, job title, email), contractual terms and agreements, and service usage details related to the partnership.

☐ Source. Obtained from collaborators, clients, or service providers as necessary for contract performance.

☐ Reason. Collected to facilitate business transactions, manage partnerships effectively, and ensure contractual obligations are met .

9.3 Publicly Available Sources. Data collected include without limitations professional or educational background (e.g., from public LinkedIn profiles), publicly listed contact information, and news articles or publications

☐ Source. Gathered from publicly accessible sources where permissible under applicable laws.

☐ Reason. Used to verify information provided by Data Subjects or partners, conduct background checks, or enhance data accuracy.

9.4 Automated Processes. Data collected include without limitations IP addresses, cookies and browsing history, and device information (e.g., browser type, operating system)

☐ Source. Generated or collected through authorized automated services and processes including website interactions and cookies.

☐ Reason. Utilized for analyzing website usage patterns, improving user experience, personalizing content, and providing targeted advertisements where applicable and permitted.

9.5 Legal Obligations. Data collected include without limitations tax identification numbers, compliance-related documentation, and regulatory filings.

☐ Source. Collected to comply with legal and regulatory requirements imposed by authorities.

☐ Reason. Necessary for fulfilling legal obligations such as tax reporting, regulatory filings, and responding to legal requests or investigations.

When applicable and required by law, we will inform Data Subjects about the specific sources from which their personal data is collected. If you have questions or concerns regarding the source of your personal data, please contact us for further information.

10 DO NOT SELL MY PERSONAL INFORMATION

The Company affirms that it does not sell personal information. This means that we do not exchange, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate personal information to another business or third party for monetary or other valuable consideration.

11 CONTACT POSSIBILITY VIA THE WEBSITE

The Website of GHAS contains information that enables quick electronic contact with our enterprise, as well as direct communication with us, which also includes a general address of the email address. If a Data Subject contacts the controller by email or via a contact form, the personal data transmitted by the Data Subject are automatically stored. Such personal data transmitted voluntarily by a Data Subject to the data controller are stored for processing or contacting the Data Subject. There is no transfer of this personal data to third parties.

12 RIGHTS OF THE DATA SUBJECT UNDER GDPR

- 12.1 Right of confirmation. Under European legislation, every Data Subject has the right to obtain from the controller confirmation as to whether or not their personal data are being processed. If a Data Subject wishes to exercise this right of confirmation, they can contact us or another employee of the controller at any time.
- 12.2 Right of access. Data Subjects, in accordance with European legislation, have the right to obtain from the controller free information about their personal data stored at any time and a copy of this information. This right includes access to the following details:
- ☐ Purposes of the processing.
 - ☐ Categories of personal data involved.
 - ☐ Recipients or categories of recipients, including those in third countries or international organizations.
 - ☐ Envisaged storage period or, if not possible, the criteria used to determine that period.
 - ☐ Right to request rectification, erasure, or restriction of processing, and the right to object.
 - ☐ Right to file a complaint with a supervisory authority.
 - ☐ Source of personal data if not collected from the Data Subject.

- ☐ The existence of automated decision-making, including profiling, with meaningful information about the logic involved and the envisaged consequences for the Data Subject.

Additionally, the Data Subject has the right to know whether personal data are transferred to a third country or an international organization, along with information about the appropriate safeguards for the transfer. To exercise this right of access, the Data Subject can contact the Company at any time.

12.3 Right to rectification. Under European legislation, Data Subjects have the right to obtain from the controller the rectification of inaccurate personal data concerning them without undue delay. Considering the purposes of the processing, the Data Subject also has the right to have incomplete personal data completed, which may include providing a supplementary statement. If a Data Subject wishes to exercise the right to rectification, they can contact us or another employee of the controller at any time.

12.4 Right to erasure (Right to be forgotten). Data subjects, in accordance with European legislation, have the right to obtain from the controller the erasure of their personal data without undue delay. The controller is obligated to erase personal data without undue delay when one of the following grounds applies, provided the processing is not necessary:

- ☐ Personal data are no longer necessary for the purposes for which they were collected or otherwise processed.
- ☐ The Data Subject withdraws consent, and there is no other legal ground for processing.
- ☐ The Data Subject objects to processing, and there are no overriding legitimate grounds, or the Data Subject objects to processing under specific circumstances.
- ☐ The personal data have been unlawfully processed.
- ☐ Erasure is required for compliance with a legal obligation.
- ☐ The personal data were collected in relation to information society services.

If any of the above reasons apply, and a Data Subject wishes to request the erasure of personal data stored by the Company, they can contact us or another employee of the controller at any time. The Company or another

employee will promptly ensure compliance with the erasure request. If the controller has made personal data public and is obliged to erase them, reasonable steps, including technical measures, will be taken to inform other controllers processing the personal data about the erasure request. The Company or another employee will coordinate the necessary measures in individual cases.

12.5 Right of restriction of processing. Data Subjects, under European legislation, have the right to obtain from the controller a restriction of processing in the following circumstances:

- ☐ The accuracy of personal data is contested by the Data Subject, allowing the controller time to verify its accuracy.
- ☐ The processing is unlawful, and the Data Subject opposes the erasure of the personal data, requesting instead the restriction of their use.
- ☐ The controller no longer needs the personal data for processing, but the Data Subject requires them for the establishment, exercise, or defense of legal claims.
- ☐ The Data Subject has objected to processing under Article 21(1) of the GDPR pending verification of whether the legitimate grounds of the controller override those of the Data Subject.

If any of the above conditions are met, and a Data Subject wishes to request the restriction of processing of their personal data stored by GHAS, they can contact us or another employee of the controller at any time. The Company or another employee will facilitate the restriction of processing.

12.6 Right to data portability. Data subjects, as granted by European legislation, have the right to receive their personal data in a structured, commonly used, and machine-readable format. This data can be transmitted to another controller without hindrance, provided the processing is based on consent, a contract, or automated means, and is not necessary for the performance of a task in the public interest or the exercise of official authority. When exercising the right to data portability, the Data Subject has the additional right to have personal data transmitted directly from one controller to another, where technically feasible and without adversely affecting the rights and freedoms of others. To assert the right to data portability, the Data Subject may contact the Company or another employee at any time.

- 12.7 Right to object. Data subjects, under European legislation, have the right to object, based on their particular situation, at any time to the processing of personal data concerning them, if such processing is based on Article 6(1)(e) or (f) of the GDPR, including profiling. If an objection is raised, the Company will cease processing the personal data unless compelling legitimate grounds override the Data Subject's interests, rights, and freedoms or for the establishment, exercise, or defense of legal claims. For personal data processed for direct marketing purposes, the Data Subject can object at any time, leading to the cessation of processing for such purposes, including related profiling. Additionally, the Data Subject has the right to object to the processing of personal data for scientific, historical, or statistical purposes unless such processing is necessary for reasons of public interest. To exercise the right to object, the Data Subject can directly contact the Company or another employee. Furthermore, within the context of information society services, the Data Subject is free to use automated means, notwithstanding Directive 2002/58/EC, to exercise their right to object through technical specifications.
- 12.8 Automated individual decision-making, including profiling. Data Subjects possess the right, as conferred by European legislation, not to be subjected to decisions based solely on automated processing, including profiling, if such decisions result in legal or similarly significant effects on them. This right is upheld unless the decision is necessary for a contract between the Data Subject and the data controller, authorized by applicable law with measures safeguarding the Data Subject's rights, or based on explicit consent. Suppose the decision falls within the exceptions mentioned above, such as contractual necessity or explicit consent. In that case, the Company will implement measures to protect the Data Subject's rights, including the right to human intervention, the expression of their viewpoint, and the ability to contest the decision. To exercise rights regarding automated decision-making, the Data Subject can directly contact the Company or another employee of the data controller.
- 12.9 Right to withdraw data protection consent. Data Subjects have the right, as granted by European legislation, to withdraw their consent for the processing

of personal data at any time. To exercise this right, the Data Subject can directly contact the Company or another employee of the data controller.

13 RIGHTS OF THE DATA SUBJECT UNDER CCPA

California Data Subjects have certain rights with respect to their personal information. These rights include the following:

13.1 Right to Know and Access. Data Subjects have the right to know what personal information the Company collects, uses, and shares about them. This includes (i) Information Collected; (ii) Sources; (iii) Purpose; and (iv) Third Parties.

13.2 Right to Request Deletion. Data Subjects have the right to request the deletion of personal information that the Company has collected about them, subject to certain exceptions. Upon receiving a verified request, the Company will delete the personal information from our records and direct our service providers to do the same.

Exceptions to Deletion. The Company may deny a deletion request if retaining the information is necessary for us or our service providers to (i) Complete a Transaction; (ii) Security; (iii) Detect security incidents; (iv) Errors; (v) Legal Obligations; and (vi) Other Exceptions such as engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, enable solely internal uses that are reasonably aligned with the expectations of the Data Subject based on their relationship with Company, or otherwise use the data internally in a lawful manner that is compatible with the context in which the Data Subject provided the information.

13.3 Right to Opt-Out of Sale. The Company does not sell any personal information. However, to ensure transparency and compliance with applicable regulations, the Company provides a "Do Not Sell My Personal Information" link and an opt-out mechanism on the Website. This allows Data Subjects to easily opt out of any potential sale of their personal information. Opt-Out Mechanism. Data Subjects can exercise their right to opt-out of the sale of their personal information by:

☐ Using the Platform Link. Clicking on the "Do Not Sell My Personal Information" link available on the Website.

- ☐ Contacting Us Directly. Reaching out to the Controller or Company to request the opt-out. Contact details are provided below.

By using either method, Data Subjects can ensure that their personal information is not sold. The Company will honor these requests promptly and ensure that the personal information is excluded from future sales activities.

- 13.4 Right to Non-Discrimination. The Company will not discriminate against any Data Subject for exercising their rights under the California Consumer Privacy Act (CCPA). This includes, but is not limited to (i) Access to Services; (ii) Pricing; and (iii) Service Quality. Exercising CCPA rights will not result in any adverse treatment or penalties.
- 13.5 Right to Designate an Authorized Agent. Data Subjects may designate an authorized agent to exercise some of their rights. To protect the security of personal information, the authorized agent must follow the same authentication procedures required if the Data Subject exercises their rights directly. The Company will verify requests made through authorized agents to ensure the safety of the Data Subject's account and to comply with our policies and procedures.
- 13.6 Right to Notice. Data Subjects have a right to receive notice of our practices at or before collection of personal information.
- 13.7 Right to Correct. Data Subjects have the right to request that Company correct any inaccurate personal data held about them. Upon receiving a verified request, Company will take appropriate steps to correct the inaccurate information in our records.
- 13.8 Additional information on exercising your rights. Data Subjects under CCPA and CPRA have the right to access, delete, opt out of the sale of, non-discriminate, correct, or verify the specific pieces of personal information the Company has collected about them in the past 12 months.
- 13.9 Contact Us. To exercise their rights under CCPA, and CPRA Data Subject may contact us at support@gnhautomation.com or this Contact Form. The Company will, however, for additional security, be required to verify the Data Subject's identity before providing the information and may request further identification proof to accommodate such request. Data Subjects may enforce these rights free of charge or penalty, but we may limit the number of requests you make or charge reasonable fees as legally permitted. The

Company commits to responding to requests within 45 days upon receipt. Should additional time be necessary, the Company reserves the right to extend the response period by an additional 45 days. Requestors will be promptly notified in writing regarding the reason for the extension and the revised timeframe.

14 VERIFICATION PROCESS FOR IDENTITY OF REQUESTOR

To protect the security and privacy of personal information, Company follows a detailed process to verify the identity of any Data Subject making a request to exercise their rights under applicable data protection laws. The verification process is as follows:

14.1 Initial Request. When a Data Subject submits a request, they must provide:

- ☐ Full name
- ☐ Contact information (e.g., email address or phone number)
- ☐ Details of the request (e.g., access, deletion, correction)

14.2 Identity Verification

- ☐ For Online Accounts. If the Data Subject has an online account with the Company, they must log in to their account to verify their identity before submitting the request.
- ☐ For Non-Account Holders. If the Data Subject does not have an online account, they must provide two or more pieces of personal information that we have on file (e.g., billing address, last transaction amount, last order number).

14.3 Additional Verification Steps. The Company may request additional information or documentation, such as a government-issued ID, to confirm the identity of the Data Subject if the initial verification is insufficient. For requests made by authorized agents, the Company will require proof of the agent's authorization (e.g., a signed authorization letter) and may contact the Data Subject directly to confirm the request.

14.4 Confirmation. Once the Data Subject's identity has been verified, the Company will process the request. The Company will inform the Data Subject of the outcome of their request within the legally required time frame.

14.5 Denial of Requests. If the Company cannot verify the identity of the requestor, we will deny the request and inform the Data Subject of the reason for the denial. The Data Subject will be given the opportunity to provide additional information to verify their identity.

15 TRANSFER OF PERSONAL DATA

In the course of our business operations, personal data may be transferred to legal representatives, contractors, marketing and sales departments, and accounts departments, which may be located internationally. This section provides details on such transfers in accordance with the General Data Protection Regulation (GDPR).

15.1 Legal Basis for International Transfers. The legal basis for the transfer of personal data internationally is based on the necessity of processing for the performance of a contract, compliance with legal obligations, the protection of vital interests, consent, the performance of a task carried out in the public interest or the exercise of official authority, and legitimate interests pursued by the Company or a third party.

15.2 International Recipients. Recipients of personal data may include:

- ☐ Legal Representatives. Personal data such as name, contact information, and legal matters related to individuals may be shared with legal representatives for legal and contractual purposes.
- ☐ Contractors. External contractors engaged by the Company may receive personal data such as name, contact information, and project-related details for the provision of services and support.
- ☐ Marketing and Sales Departments. Personal data such as name, contact details, and purchasing behaviour may be shared with international marketing and sales departments for promotional activities and customer communication.
- ☐ Accounts Departments. International accounts departments may receive personal data such as name, billing details, financial transactions for financial and accounting purposes.

15.3 Safeguards for International Transfers. To ensure the security and confidentiality of personal data transferred internationally, we implement appropriate safeguards, which may include:

- ☐ Standard Contractual Clauses. Contracts with international recipients may include standard contractual clauses approved by the European Commission.
- ☐ Data Protection Impact Assessments. Assessments are conducted to identify and minimize risks associated with international transfers.
- ☐ Data Minimization. Only necessary personal data is transferred to international recipients.

16 RETENTION PERIODS FOR PERSONAL DATA

- 16.1 Client Information. Personal data will be retained only for as long as necessary for the purposes outlined in this notice and no more than 12 months or as required by applicable laws.
- 16.2 Employee Information. Personal data collected for contractual requirements, payroll, and other legitimate business purposes is retained for the duration of the employment relationship and as required by applicable legal obligations.
- 16.3 Data Disposal. Upon the expiration of the applicable retention periods, personal data is securely disposed of to prevent unauthorized access or disclosure.
- 16.4 The criteria used to determine the period of storage of personal data is the respective statutory retention period. After the expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract. If the Data Subject requests for termination or terminates their GHAS Account, the personal data shall be retained for a period of 12 months from the date of termination or as statutorily obligated.
- 16.5 It is important to note that the obligation to provide personal data is communicated transparently to individuals before or at the time of data collection. If there are uncertainties about the specific obligations related to the provision of personal data, individuals are encouraged to contact us for clarification.

17 ROUTINE ERASURE AND BLOCKING OF PERSONAL DATA

- 17.1 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.

- 17.2 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.

18 AUTOMATED DECISION-MAKING

We want to inform you about the existence of automated decision-making processes as part of our data processing activities. Here are the key details:

- 18.1 Automated Decision-Making. Our systems may, in certain instances, make decisions automatically without human intervention.
- 18.2 Legal Basis. Automated decision-making activities are conducted based on the legal basis provided by applicable data protection laws, and appropriate measures are in place to safeguard your rights and interests.
- 18.3 Significance and Consequences. When automated decisions are made, we ensure that individuals are informed of the significance and potential consequences of such decisions. You have the right to contest decisions made through automated processes.
- 18.4 Right to Explanation. If you are subject to an automated decision, you have the right to request an explanation of the decision-making process and express your point of view.

If you have questions, or concerns, or would like more information about the automated decision-making processes we employ, please contact us. We are committed to ensuring transparency and providing individuals with the necessary information to understand and exercise their rights.

19 DATA PROTECTION MEASURES

The Company implements robust data protection measures to safeguard the personal information we collect and process. These measures include:

- 19.1 Data Encryption. Utilizing encryption technologies to protect data both in transit and at rest, ensuring that unauthorized parties cannot access or decipher sensitive information.

- 19.2 Access Controls. Implementing strict access controls and authentication mechanisms to limit access to personal information to authorized personnel only.
- 19.3 Data Minimization. Collecting and processing only the necessary personal information required for specified purposes, and retaining it only for as long as necessary to fulfill those purposes.
- 19.4 Security Audits and Monitoring. Conducting regular security audits and assessments to identify and mitigate potential vulnerabilities in our systems and infrastructure. We also maintain continuous monitoring to detect and respond to security incidents promptly.
- 19.5 Employee Training. Providing regular training and awareness programs to employees handling personal information, emphasizing the importance of data protection and privacy compliance.
- 19.6 Privacy by Design. Integrating privacy considerations into the design and development of our systems, products, and services to ensure that data protection measures are implemented from the outset.
- 19.7 Third-Party Compliance. Ensuring that any third-party service providers or partners that process personal information on our behalf adhere to stringent data protection standards through contractual obligations and regular audits.

20 PERSONS UNDER THE AGE OF 18

Our Website is not intended for persons under 18 years of age. No one under the age 18 may provide any information to the Website. The Company does not knowingly collect personal information from anyone under 18. If you are under 18, do not use or provide any information on this Website or through any of its features make any purchases through the Website, use any of the interactive features of this Website, or provide any information about yourself to us, including your name, address, telephone number, email address, or any screen name or user name you may use. If the Company learns it has collected or received personal information from a child under 16 years of age without verification of parental consent, the Company will delete that information. If you believe the Company might have any information from or about a child under 16, please contact us. The Company does not sell any personal information, including the personal information of individuals under the age of 16.

21 DATA COLLECTED IN 12 MONTHS

The Company has in the last 12 months collected the following categories of data from Data Subjects. All data collected are for the purpose of fulfilling the Company's obligations with respect to employee payroll, contractual obligations, marketing and advertising, and legal compliance.

21.1 Identifiers. Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

21.2 Personal Records. Birthdate, age, education, employment history, or other similar personal records.

21.3 Professional or Employment-Related Information. Current or past job history or performance evaluations.

21.4 Internet or Electronic Network Activity Information. Information regarding a consumer's interaction with a website, application, or advertisement.

21.5 Commercial Information. Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

22 PRIVACY POLICY UPDATE

The Company commits to updating its privacy notice annually to ensure compliance with data protection laws and to reflect any changes in our practices or legal requirements. This ensures Data Subjects receive current and transparent information about how their personal information is handled.