Alliance Background, LLC

DATA PRIVACY AND PROTECTION POLICY

Table of Contents:

Purpose and Scope

The purpose of this policy is for Alliance Background (COMPANY) company and legal and regulatory requirements under current applicable privacy laws. “Privacy Laws” mean laws, in multiple jurisdictions worldwide, that relate to (a) the confidentiality, collection, use, handling, processing, security, protection, transfer, or free movement of personal data, personally identifiable information, or consumer or client information, (b) electronic data privacy, (c) trans-border data flow or (d) data protection.

“Personal Data” means a type of data regulated by Privacy Laws.

This policy applies to all COMPANY employees, independent contractors, and Personal Data as defined above.

Data Protection Policy Statement.

COMPANY is classed as a Data Controller/Data Processor based on the context of the processes under current privacy law. This policy confirms our commitment to protecting the privacy of the personal data of our consumers, clients, employees, and other individuals. Our Information Security Policy is aligned to standard ISO027001 to ensure that personal data processes are conducted using best practice processes.

COMPANY DATA POSITION

As a collector of first-party data, COMPANY has adopted the following principles:

- Be transparent about what we collect, why we collect it, how we use it, and who we share it with.
- Use clear statements in all privacy-related communications and provide a plain language privacy policy.
- Obtain just-in-time, informed consent *before* collecting or processing personal data, especially Sensitive Personal Information.
- Collect the least amount of data needed, relevant and limited to what is necessary.
- Delete means deleting everything a reasonable person would intend for the deletion or confirming if the consumer could be adversely affected.
- Use standard industry practices to secure personal data from unauthorized access when stored and during usage.
- Unless otherwise required by Privacy Laws, all Personal Information is classified as Confidential with Medium or High Risk or otherwise recommended by industry standards**.**
- Sensitive Personal Data is classified as Confidential and High Risk, or as otherwise recommended by industry standards.

Overview of the Privacy Team and Role of the Data Privacy Officer

The Privacy Team is responsible for complying with individual rights requests. However, all employees and contractors who receive communication from a data subject must forward it to EMAIL. When responding to requests, the Privacy Team will work with support from the Data Privacy Officer (or designated delegate) who received the request, their manager, IT, and the Legal team. The Privacy team will manage and respond to all

individual rights requests.

Data Protection Principles

COMPANY employs Fair Information Privacy Practices.

Data purpose minimization. COMPANY ensures that the data collected is not excessive and is appropriate to the purpose for which it was collected. We conduct PIAs/DPIAs (if required) as part of our project lifecycle.

Accuracy. COMPANY takes reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, measures will be put in place to ensure that personal data is kept up to date. We provide data that is reviewed and assessed for accuracy periodically. We have implemented processes [LIST] to rectify and erasure data without undue delay.

Data Retention. Personal data will be kept only as long as needed, or once the legitimate business purpose expires. COMPANY will establish a data archiving/retention policy for all categories of processed personal data. This policy will be reviewed annually and determine data retention standards.

Questions to consider include: What data is retained? Why is the data retained? For how long? In which format is data retained? (PI, de-identified, archived) Who has access to archived data? How is data deleted/destroyed? When?

Data Destruction. Personal data is retained and destroyed in line with our Information Security Policy. COMPANY has established a data deletion process for all Data Subjects. For all deletion requests, regardless of origination source, the Privacy Team will delete the Data Subject's PI and SPI across all COMPANY information systems.

Security. COMPANY will ensure that personal data is stored securely using modern and up-to-date software.

Record Keeping Requirements. The Privacy Team will maintain and annually review all privacy-related policies, records, and documentation to ensure ongoing regulatory compliance. Data storage will be in line with the Data Retention Policy.

Data Privacy by Default. All user settings are set to privacy-protected by default. The user requires no action to ensure their privacy is protected. COMPANY provides just-in-time warnings for public-facing personal data at the registration and before posting (e.g., "Username is public, so choose wisely").

Data Privacy By Design. It helps to identify and address the data protection and privacy concerns at the project's design and development stage, building data protection compliance from the outset rather than bolting it on as an afterthought.

Privacy Impact Assessments (PIA). COMPANY will conduct a privacy impact assessment, or PIA, each time a new personal data processing activity or data processing tool is implemented. Following best practices, employees must complete a PIA and submit it for legal review.

Complete and submit the PIA for Legal review and approval before kickoff meetings for any activity that:

- Uses or affects personal information or sensitive personal information;
- Creates a significant change to a current process; or
- Your project or product is a new initiative for the business or community.

Some examples include

- Profiling, evaluating, ranking, or scoring data subjects for **predictive purposes.**
- Automated-decision making.
- Systematic monitoring.
- Processing sensitive data or data of a highly personal nature.
- Large-scale data processing.
- Matching or combining data sets.
- Processing data concerning vulnerable data subjects.
- Innovative uses or applications of new technologies or organizational solutions to personal data.

Legal will review the PIA within the time period specified in the Service Level Agreement.

Data Protection Impact Assessment (DPIA). If, after reviewing a PIA, the Legal Department determines further review is required, a meeting will be scheduled to conduct a Data Privacy Impact Assessment (DPIA).

Rights of Data Subjects Data Subject Access Requests. All DSAR requests will be handled following the process outlined via the COMPANY RIGHTS AND REQUEST POLICY.

Right to be Informed. Individuals have the right to be informed about how we use their Personal Information. These rights include:

1. What: The name and contact details of COMPANY
2. Who: Name and contact details of our Data Privacy Officer
3. What: Purposes of the processing
4. Why/How: Lawful basis of processing

Right of Access. Individuals have the right to access their personal data. Any such requests

to COMPANY will be handled promptly and according to legal requirements.

Right to correct or "rectify." The GDPR includes the right to have inaccurate personal data rectified or completed if it is incomplete.

Right to Erasure (Be Forgotten). The GDPR introduces the right to have personal data erased and is known as 'the right to be forgotten."

All personal data will be permanently deleted or deidentified across all COMPANY systems, regardless of the request's origin. When deleting personal data, it must be irrecoverable.

Appropriate backup and disaster recovery solutions are in place and detailed in COMPANY BUSINESS CONTINUITY POLICY.

Right to Portability. This right allows individuals to obtain and reuse their personal data for tier own purposes across different services. It allows them to safely and securely move, copy or transfer personal data from one IT environment to another safely and securely without affecting usability. This allows individuals to use applications and services that may use this data to find a better deal or help them understand their consumption habits. This only applies to information the individual has provided to COMPANY or a controller.

Reliable, fair, lawful, and transparent processing.

To ensure its processing of data is reliable, lawful, fair, and transparent, COMPANY will maintain and annually review a "Register of Systems,"

- **Lawful basis or Legitimate Business Purpose.** All data processed by COMPANY must be done on at least one (1) of the following lawful bases:
    - **Contractual obligations and relationships;**
    - **Providing services;**
    - **Advertising and marketing; AND/OR**
    - **Consent-based.**
- **Legal obligation.** Taxes, compliance records, warrants, subpoenas, or other lawful court orders.
- **Marketing and advertising.** Includes all media products and communications. Note Consent-based requirements.
- **Public Interest.**
- **Consent.**

COMPANY primarily relies upon consent for a lawful basis to process. It will establish documentation that the data subject has consented to processing their personal data.

Suppose the data subject's consent is given in the context of a written declaration that also concerns other matters. In that case, the request for consent will be presented in a manner that is distinguishable from the other issues, in an intelligible and easily accessible form, using clear and plain language.

The data subject will have the right to withdraw their consent anytime. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. Before giving consent, the data subject will be informed thereof. It will be as easy to withdraw as to give consent.

When assessing whether consent is freely given, the utmost account will be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

- Does this involve the collection of new information about an individual?
- Does this require individuals to provide information about themselves?
- Does this involve making decisions or taking actions that can significantly impact an individual?

Compliance; Record of consent. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be available. Systems in place ensure such revocation is reflected accurately in COMPANY's compliance documentation.

Risk Assessments. Risk is defined as "data processing that is 'likely to result in a high risk to the rights and freedoms of natural persons.'" If yes to any of the above questions, identify the types of risk:

- illegitimate access,
- loss of personal data
- repurposing
- data-based discrimination
- highly sensitive data
- new technology which may be perceived as invasive

Contractual Obligations. All contracts involving the transfer of personal data, regardless of data format, must be reviewed by the Data Privacy Officer or Legal Counsel, and supplemented with the applicable Data Privacy Agreement.

Cyber Insurance. Company maintains Cyber Insurance.

Security. COMPANY will ensure that personal data is stored securely using modern and up-to-date software. Access to personal data will be limited to personnel who need access, and appropriate security should be in place to avoid unauthorized information sharing.

Breach
In the event of a breach, employees will inform their direct supervisor, a member of the Technology Team, or a member of the Data Privacy Team and invoke the Incident Management Process.

Breaches are assessed, and where appropriate and required, the Data Subjects and the Information Commissioners Office will be informed without undue delay.

In the event of a breach of security leading to the accidental, unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data, COMPANY will promptly assess the risk to people's rights and freedoms.

Legal Representation. In the event of a breach of security leading to the accidental, unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data, COMPANY is represented by INSERT FIRM. In-House counsel will manage all communications with outside counsel.

Data Incident Response Plan. COMPANY will create a Data Incident Response Plan to demonstrate:

- how to recognize a personal data breach and why a personal data breach is not only about loss or theft
  of personal data;
- how to escalate a security incident to the appropriate person or team in our organization to determine whether a breach has occurred;
  a response plan for addressing any personal data breaches that occur; and allocate responsibility for managing breaches to a dedicated person or team.

Alliance Background Privacy Policy (w GDPR)

1. Introduction

1.1. Your privacy is important to us. This privacy policy provides you with information regarding the processing of your personal information when you make contact with us or use one of our services.

1.2. This privacy policy is provided per the General Data Protection Regulation 2016/679 ("GDPR") and any EU national laws implementing or supplementing the same (the "Data Privacy Laws").

2. About us and our privacy commitment

2.1. Alliance Background, LLC ("Alliance Background" or "We"), provide services under "Alliance Background", which is headquartered in Florida, United States and assists entities around the world to provide its clients background screening and due diligence ("Services") through an End User Agreement agreed upon between Alliance Background and the client ("Service Agreement").

2.2. We are firmly committed to respecting your right to privacy and take seriously our responsibilities concerning the processing of personal information. We do not collect or process personal information unnecessarily.

2.3. The privacy policy (the "Policy") sets out important information about your rights concerning the processing of your personal information in the course of using our services.

The Policy also outlines the basis on which any personal information we collect from you or that you provide to us, will be processed in connection with your use of our services.

2.4. If you have any questions about this Privacy Policy or want to exercise your rights set out in this Privacy Policy, please contact us by sending an email to **info@Alliance Background.com**

3. What information do we collect?

3.1. Alliance Background's GDPR Privacy Policy is primarily related to personal information collected and processed in order to operate our business.

3.2. We may collect personal information from you in the course of our business, including through your use of our website, when you contact or request information from us, when you engage our team to provide Services.

3.3.3 We collect information such as name and contact details in order to communicate and facilitate the provision of our services with our clients, potential clients, or suppliers.

Initial information about you can be provided by the company you are working for. You may provide us with information by using our services or by corresponding with us by phone, e-mail, or otherwise.

Other occasions during which you provide us information are when searching for a product, placing an order, reporting a problem, or engaging with any other form of communication with us. We may collect information to respond to inquiries regarding our products and services or to provide you with information, reports, or updates.

3.4. When you visit our website or use our platforms, we may collect, as a data controller, information about your visit such as your IP address, login information, browser type, time zone setting and the pages you visited and, when you use our Services we may collect Privacy Policy information on how you use those services.

Our websites and online platforms may use cookies from time to time. Cookies may be used to save your personal preferences, so you do not have to re-enter them each time you access our services. For more information
about our use of cookies and how you can disable them, please see our Cookie Policy.

3.5. In the course of providing our Services to our clients, they engage us on screening matters to help them mitigate risk such as conducting due diligence on a potential partner, employee, volunteer.

3.5.1. The personal information we process in the performance of Services for and on behalf of our international clients, as a data processor, includes but is not limited to any information relating to an identified or identifiable individual ("Data Subject"), for example, the individual's name, contact information, education information, work history, directorships, as well as, where necessary, data concerning criminal convictions and offenses and financial information. We treat such information within the strict confines of the GDPR when performing Services for our international clients and/or Data Subjects.

3.5.2. The lawful bases for such data processing are defined by our client in their privacy policy or another document and will vary depending on the nature of the information and the project. Before ordering, Alliance Background's client has assessed the necessity, permissibility, and relevance of the service. Alliance Background's client warrants to Alliance Background that:

(1) the personal data is processed in a lawful, fair, and transparent manner in relation to the data subject;

(2) the personal data is collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(3) the personal data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed; and

(4) if applicable after seeking appropriate legal advice, information notice or authorization form or any other mandatory document, has been duly provided to/required from the data subject.

3.5.3. Alliance Background warrants the legality of the access to the information expected to be verified and defines the scope. Alliance Background does not guarantee compliant use of the data in this report by the client. Alliance Background has used its professional care and diligence to verify information against authorized public and/or private sources.

4. What do we do with your information?

4.1. We will only process personal information when the law allows us to.

4.2. We may use your information for the following purposes: Fulfilment of Services, business administration, and legal compliance.

4.2.1. Where we process your personal information to register you as a customer/user, accept your orders, deliver Services , collect our fees; we do so on the basis that it is necessary to perform our obligations under a contract with you or a company you work for. It may also be necessary to comply with certain legal obligations.

4.2.3. Where we process your personal information for business administration and legal compliance, we comply with our legal obligations, to enforce our legal rights, in connection with a business transaction; we do so on the basis that we have a legal obligation to do so.

4.2.4. Where we process your personal information for a client's employment purposes to assess whether such application has been received by us online, via email, or by hard copy or an in- person application. We will not process any special category data except where we can do so under applicable legislation.

4.3. We will only use your personal information for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with this Policy, where this is required or permitted by law.

5. Our information Privacy Policy

5.1. We only share your personal information with your consent or following this Policy. We will not otherwise share, sell, or distribute any of the information you provide to us except as described in this notice.

5.2. We may disclose information to any department or authorized person within our company or any affiliated company within Alliance Background and selected third parties only in the circumstances where it is necessary, and the supplier has agreed to the same standards and terms of privacy as set out in the Policy.

5.3. We may also share personal information with a variety of the following categories of third parties as necessary:

5.3.1. Professional advisers such as lawyers and accountants.

5.3.2. Government or regulatory authorities.

5.3.3. Third parties to whom we outsource certain services such as, without limitation, translation services, confidential waste disposal.

5.3.6. Third parties engaged in the course of the services we provide to clients such as information furnishers.

6. International transfers

6.1. In order to provide the Services, we may need to transfer your personal information to locations outside the jurisdiction in which you provide it.

6.2. If you are based within the European Economic Area (EEA), please note that where necessary to deliver the Services we will transfer personal information to countries outside the EEA (including the United States, Mexico, Tunisia, and India).

6.3. All Alliance Background has signed a data sharing agreement which is based on the EU standard contractual clauses to ensure we will comply with our legal and regulatory obligations in relation to personal information, including having a lawful basis for transferring personal information and putting appropriate safeguards in place to ensure an adequate level of protection for the personal information.

7. How long we keep your personal information?

7.1. We will only retain your personal information for as long as necessary to fulfill the purposes we collected it for, including to satisfy any legal, accounting, or reporting requirements.

The period for which we store your personal information may depend on the type of information we hold.

7.2. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information, and whether we can achieve those purposes through other means, and the applicable legal requirements. For example, we may hold personal data as needed for our accounting or tax compliance purposes or where needed for our compliance with anti-money laundering regulations per the respective statutory periods.

7.3. For Data Subjects, we store their personal information for as long as the data controller (our client) has instructed us to in the Service Agreement.

8. Security measures

8.1. We use accepted standards of physical and technical measures and require our hosting partners to use the same standard of care to protect personal information. Despite our best effort to protect personal information, the transmission of information via the internet may not be completely secure. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorized access.

9. Your rights

9.1. You have the following rights in relation to the personal information we hold about you:

9.1.1. Your right of access: If you ask us, we will confirm whether we are processing your personal information and, if necessary, provide you with a copy of that personal information (along with specific other details). If you require additional copies, we may charge a reasonable fee.

9.1.2. Your right to rectification: If the personal information we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we have shared your personal information with others, we'll let them know about the rectification where possible. If you ask us where possible and lawful to do so, we will also tell you who we've shared your personal information with so that you can contact them directly.

9.1.3. Your right to erasure: You can ask us to delete or remove your personal information in some circumstances such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we have shared your personal information with others, we'll let them know about the erasure where possible. If you ask us where it is possible and lawful for us to do so, we will also tell you who we've shared your personal information with so that you can contact them directly.

9.1.4. Your right to restrict processing: You can ask us to 'block' or suppress the processing of your personal information in certain circumstances, such as where you contest the accuracy of that personal information, or you object to us. If you are entitled to restriction and if we have shared your personal information with others, we'll let them know about the restriction where we can do so. If you ask us, whether it is possible and lawful for us to do so, we will also tell you who we've shared your personal information with so that you can contact them directly.

9.1.5. Your right to data portability: You have the right, in certain circumstances, to obtain personal information you have provided us with (in a structured, commonly used, and machine-readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.

9.1.6. Your right to object: You can ask us to stop processing your personal information, and we will do so if we are relying on our own or someone else's legitimate interests to process your personal information, except if we can demonstrate compelling legal grounds for the processing.

9.1.7. Your right to withdraw consent: If we rely on your consent (or explicit consent) as our legal basis for processing your personal information, you have the right to withdraw that consent at any time.

9.1.8. Your right to complain with the supervisory authority: If you have a concern about any aspect of our privacy practices, including the way we've handled your personal information, you can report it to the relevant Supervisory Authority.

9.2. Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data.

10. Third-party material

10.1.The website and/or Services may contain links to other sites whose information practices may be different than ours. Visitors should consult the other sites' privacy notices as Alliance Background has no control over information that is submitted to, or collected by, these third parties.

11. Changes to this policy

11.1.Any changes made to this Policy from time to time will be published on the Platform.

Any material or other change to the data processing operations described in this Policy that is relevant to or impacts on you or your personal data will be notified to you. In this way, you will have an opportunity to consider the nature and impact of the change and exercise your rights under the GDPR in relation to that change (e.g., to withdraw consent or to object to the processing) as you see fit.

12. Contact

12.1.If you have any comments or questions about our privacy policy or our processing of your information, please contact Alliance Background at info@AllianceBackground.com.

Address:

12651 Walsingham Road, Suite C

Largo, FL 33774

Telephone:

866-590-8715

Appendix 1 – List of sub-processors that may have access to your personal data is available upon request.

Appendix 2 – Security measures

Alliance Background has developed and implemented a comprehensive security program that includes reasonable administrative, technical, and physical safeguards, which are reasonably designed to protect: the security and confidentiality of Personal Data; against unauthorized access to or use of Personal Data.

Procedures and Controls. Alliance Background has developed, documented, and will maintain procedures and controls: for the secure handling, transfer, and disposal of Personal Data, whether in electronic or physical form; to protect against destruction, loss, or damage of Personal Data due to human error, potential environmental hazards, or technological failures; to restrict access to Personal Data at physical locations, such as buildings, computer facilities, and records storage facilities; to authenticate and limit access to its systems to authorized individuals.

For the secure configuration and maintenance of information systems (e.g., servers, network infrastructure devices, and networks), including procedures for change management; the pseudonymization and encryption of Controller Data; for detecting, preventing, and responding to attacks, intrusions, or other systems failures, including actions to be taken in the event of suspected or detected unauthorized access to its systems.

Safeguards. Alliance Background has designed and implemented reasonable safeguards to control reasonably foreseeable internal and external risks to its systems by restricting access to those who have a business need to access various systems, via control of administrative and user account privileges.

Monitoring. Alliance Background monitors security within its organization by: Using tools to monitor workstations, laptops, and servers for malware, with central compilation of such logging; Leveraging firewalls and intrusion prevention systems to monitor externally facing assets;

Collecting and analyzing audit logs of events and Privacy Policy generated alerts, to help detect an attack; performing penetration testing on an annual basis.

Access. Alliance Background manages and controls system access by: using Active Directory to control administrative privileges for Windows servers and some applications; restricting user account privileges to what is necessary in order to do their job.

Disaster Recovery/Business Continuity and Incident Response Plans. Alliance Background has designed plans for responding to a: disaster, including processes and procedures for resuming business operations; network and/or system attack, including incident handling.