Alliance Background, LLC

DATA PRIVACY AND PROTECTION POLICY

Table of Contents:

ALLIANCE BACKGROUND
COMING TOGETHER TO REDUCE RISK

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 via the OneTrust form. 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 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 a 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.

Cyberinsurance. Company maintains cyberinsurance.

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 isn't 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
  allocated responsibility for managing breaches to a dedicated person or team.