Amerisearch Background Alliance Data Privacy Framework Notice

Last updated on 26/02/2024

1. Introduction

Amerisearch Background Alliance ("**Amerisearch**") respects individual data privacy and values the confidence of its customers, employees, consumers, business partners and others. Amerisearch processes personal information in the course of the provision of its services only in a manner consistent with all applicable laws and regulations of all countries in which it does business.

2. What Is Covered by this Privacy Notice?

This Data Privacy Framework Notice (this "**Notice**") applies to personal information, which means any information or set(s) of information that identifies or could be used to identify an individual, including but not limited to name, mail or email address, biometric data, or any other relevant information. Personal information does not include information that is encoded or anonymized, or publicly available information that has not been combined with non-public personal information. It also applies to sensitive personal information, which means personal information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, views, or activities, which concerns health or sex life, information about social security benefits, or information on criminal or administrative proceedings and sanctions other than in the context of pending proceedings. Amerisearch will treat as sensitive personal information any information received from a third party where that third party treats and identifies the information as sensitive.

In particular, this Data Privacy Framework Notice (this "**Notice**") addresses individuals whose personal information Amerisearch processes in the context of the provision of its background screening services (**job applicants or employees of Amerisearch's customers**).

This Notice applies to Personal Information, in any format, including electronic, paper or verbal.

In particular, this Notice outlines the privacy principles followed by Amerisearch with respect to **personal information it receives** as a U.S. based corporation **from its customers in the UK, Switzerland, and the European Economic Area** (EEA), which includes all member states of the European Union (EU), as well as Iceland, Liechtenstein, and Norway. This Notice describes what personal information Amerisearch processes, and how Amerisearch processes and protects such personal information.

3. What Is Not Covered by this Privacy Notice?

This Notice does not apply to personal information Amerisearch obtains about job applicants or employees of Amerisearch's customers by conducting further research on the individuals. It only applies to personal information Amerisearch receives from its customers about the individuals.

This Notice does not apply to the personal information of employees, job applicants, contractors, business owners, directors, and officers of Amerisearch. It also does not apply to the personal information of website visitors of our website, nor the personal information of our business contacts and partners.

If we do not maintain information in a manner that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household, such information is not considered personal information and this Notice will not apply to Amerisearch's processing of that information.

4. Compliance with the Data Privacy Framework

With respect to personal information processed in the scope of this Notice, Amerisearch complies with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**") and the UK Extension to the EU-"U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") (the "**Data Privacy Framework**") as set forth by the U.S. Department of Commerce.

Amerisearch has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("**EU-U.S. DPF Principles**") with regard to the processing of personal information received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

Amerisearch has also certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles ("**Swiss-U.S. DPF Principles**") with regard to the processing of personal information received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Notice and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

To learn more about the Data Privacy Framework program, please visit https://www.dataprivacyframework.gov/. To view Amerisearch's certification, please visit https://www.dataprivacyframework.gov/s/participant-search.

5. Categories of Personal Information

Amerisearch may receive the following information from its customers in the EEA, UK and Switzerland:

- First and last name
- Email address
- Physical address
- Telephone number
- Date of birth
- Social security number or other identification number
- Passport number
- References
- Criminal records
- Employment history
- Educational records (e.g. degrees, certifications)
- Biographical information.

6. Sources of Personal Information

In the context of this Notice, we receive personal information from your prospective or existing employer, as included in the relevant service request, such as background screening requests. Your employer may obtain information about you to verify and investigate your background for pre-employment or employment purposes from, among other parties, Amerisearch, which acts as a reporting agency, and Owens OnLine LLC (3802 Ehrlich Road, Suite 307, Tampa, FL 33624, USA or their representative Owens Europe GmbH, Medipark 1, D-83088 Kiefersfelden, Germany) ("**Owens**"), which acts as a furnisher.

7. Our Role with Respect to Personal Information

In the context of this Notice, Amerisearch acts as an agent for the personal information we process. This means that our customers determine the type of personal information they provide us with to process on their behalf. We typically have no direct relationship with the individuals whose personal information we receive from our customers.

8. Purposes of Processing

In the context of this Notice, Amerisearch processes personal information for various purposes, including but not limited to verifying accuracy of information provided by job applicants or employees, assessing their suitability for employment, ensuring compliance with regulatory requirements, and helping employers make informed decisions to maintain workplace safety and integrity. We may also use this information to conduct background checks, which can include, among others, criminal history, employment, and education verification as well as credit checks, to support the hiring process.

9. Sharing Personal Information with Third Parties

The information your existing or prospective employer provides Amerisearch with, and any information that you supply directly to Amerisearch, may be disclosed to third parties including:

- agents or vendors of your employer, Owens, and Amerisearch;
- law enforcement agencies;
- state or federal agencies;
- courts;
- institutions schools, or universities (public or private);
- information service bureaus;
- employers, employees, or insurance companies to verify and investigate your background;
- our service providers, including employment screening software providers such as Accio Data.

In accordance with the host nation's laws and the laws applicable to you depending on your location regarding the release of information, you understand that information may be transmitted from any country to the above listed parties located in any country, including countries outside your jurisdiction or region. Those jurisdictions may have a different level of data protection or inadequate data protection laws in comparison with those of your country of residence.

For the purpose of this section, “agent” means any third party that collects or uses personal information, under the instructions of, and solely for, Amerisearch and its clients to which Amerisearch discloses personal information for use of its clients for the sole purpose of providing its services.

Pursuant to the Data Privacy Framework, some third parties that receive your personal data may be located outside of the United States; however, we will either obtain your explicit consent to transfer your personal data to such third parties, or we will require those third parties to maintain at least the same level of confidentiality that we maintain for such personal data ourselves.

We remain liable for the protection of your personal data that we transfer to our agents, except to the extent that we are not responsible for the event giving rise to any unauthorized or improper processing. Amerisearch may be liable if it knowingly transfers appropriate onward personal information to third parties or agents, employees, college, or partner who Amerisearch is aware of, or has been made aware of, failing to follow any of these Data Privacy Framework required principles.

In particular, Amerisearch will obtain legally adequate assurances from its agents that they will safeguard personal information consistent with this Notice. Examples of appropriate assurances that may be provided by agents include:

- Already being subject to the EU General Data Protection Regulation, the Swiss Federal Act on Data Protection, or UK data protection laws.
- Being certified under the Data Privacy Framework certification.
- Being in a territory, sector or country that has obtained an adequacy finding. You can see here the list of countries, territories and specified sectors that the European Commission recognized as providing an adequate level of protection for personal data, the UK's list here, and Switzerland's list here.
- Entering into a contract with Amerisearch obligating the agent to provide at least the same level of protection as is required by the relevant Data Privacy Framework Principles. We can refer to the Data Privacy Framework Principles or rely on Binding Corporate Rules or the Standard Contractual Clauses approved by the European Commission under Article 46.2 of the GDPR, with necessary adjustments for transfers from the UK or Switzerland, or use specific transfer instruments like the UK International Data Transfer Agreement.

10. Other Disclosures of Personal Information

We may disclose your personal information to the extent required by law, or if we have a good-faith belief that we need to disclose it in order to comply with official investigations or legal proceedings (whether initiated by governmental/law enforcement officials, or private parties). If we have to disclose your personal information to governmental/law enforcement officials, we may not be able to ensure that those officials will maintain the privacy and security of your personal information.

We may also disclose your personal information if we sell or transfer all or some of our company's business interests, assets, or both, or in connection with a corporate restructuring. Finally, we may disclose your personal information to subsidiaries or affiliates, but only if necessary for business purposes, as described in the section above.

We reserve the right to use, transfer, sell, and share aggregated, anonymous data for any legal purpose. Such data does not include any personal information.

11. Privacy Rights

We acknowledge the right of EEA, UK and Swiss individuals to access their personal information pursuant to the Data Privacy Framework and will grant individuals reasonable access to personal information we received pursuant to the Data Privacy Framework. In addition, we will take reasonable steps to permit individuals to correct, amend, or delete such information that is demonstrated to be inaccurate or processed in violation of the Data Privacy Framework Principles. Additionally, if we have received your personal information in reliance on the Data Privacy Framework, you may also have the right to opt out of having your Personal information shared with third parties and to revoke your consent to our sharing of your personal information with third parties. You may also have the right to opt out if your personal information is used for any purpose that is materially different from the purpose(s) for which it was originally collected or which you originally authorized. An individual may request to access their personal information, or otherwise correct, amend, delete, withdraw their consent or limit the processing of their personal information in line with the Data Privacy Framework Principles by contacting us or our customer.

11.1. Access & Review

If you are an individual about whom we have received personal information, you may have a right to request access to, and the opportunity to update, correct, or delete, such personal

information. To submit such requests or raise any other questions, please use the details included in the Contact Us section of this Notice.

11.2. Choice

Amerisearch will offer individuals the opportunity to choose (opt out) whether their personal information is to be disclosed to our clients for employment purposes only. The applicant will be notified immediately upon this decision that this may jeopardize their opportunity for employment with an Amerisearch client. However, Amerisearch Background Alliance do not recommend or make any determination in regard to its client's decision. Should the client's decision be adverse, thereby negatively affect the applicant's opportunity for employment with an Amerisearch client, Amerisearch will in accordance with FCRA rules provide individuals with Pre-adverse and Adverse action letters along with copies of their report. These documents will provide precise instructions to allow the applicant to exercise the process of disputing any information they believe to be incorrect.

At the time data is collected, the applicant must affirmatively opt in to allow Amerisearch to disclose or use sensitive personal information, including data related to health, racial or ethnic origin, political and religious opinions, trade union membership, or information revealing an individual's sex life.

To withdraw your consent to a background check, contact Amerisearch or Owens in writing or by e-mail at the addresses listed on www.owens.com/contact-us. If you choose to withdraw your consent, your background check will not be completed if it was still in process. This may affect the decision relating to the purpose for which the background check was requested.

12. Security

Amerisearch will take reasonable and appropriate precautions to protect personal information in its possession from loss, misuse and unauthorized access, disclosure, alteration, and destruction.

13. Data Integrity and Purpose Limitation

Amerisearch will collect and use personal information in the scope of this Notice only in ways that are relevant and compatible with the purposes for which it was collected or subsequently authorized by the individual, and in compliance with applicable laws. Amerisearch will take reasonable steps to ensure that personal information is reliable and relevant to its intended use, accurate, complete, and current.

14. RECOURSE, ENFORCEMENT, AND LIABILITY

Amerisearch will conduct compliance audits of its relevant privacy practices to verify adherence to this Notice. Any employee, partner, agent, and contractor that Amerisearch determines is in violation of this policy will be subject to disciplinary action up to and including termination of employment, agreement, or contract between that party and Amerisearch.

15. Changes to this Notice

If we make any change to this Notice, we will post the revised Notice to our website and update the "**Last updated**" date above to reflect the date on which the Notice was last updated.

16. Contact Us

If you have any questions about this Notice or our processing of your personal information, or want to submit a request to exercise your privacy rights, please write to our VP Compliance by email at mikeb@americanbga.com, or by postal mail at:

Attention: Michael Brown, VP Compliance
Amerisearch Background Alliance
2529 South Ridge Rd
E Ashtabula Ohio
44004

17. Dispute Resolution

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Amerisearch commits to resolve complaints about your privacy and our collection or use of your personal information. Individuals with inquiries or complaints regarding this Notice or Amerisearch's processing of personal information within the scope of this Notice should **first** contact Amerisearch using the contract details in the section immediately above.

Where a privacy complaint or dispute relating to Personal information received by Amerisearch in reliance on the Data Privacy Framework (or any of its predecessors) cannot be resolved through our internal processes, we have agreed to participate in the VeraSafe Data Privacy Framework Dispute Resolution Procedure. Subject to the terms of the VeraSafe Data Privacy Framework Dispute Resolution Procedure, VeraSafe will provide appropriate recourse free of charge to you. To file a complaint with VeraSafe and participate in the VeraSafe Data Privacy Framework Dispute Resolution Procedure, please submit the required information here: https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/

18. Binding Arbitration

If your dispute or complaint cannot be resolved by us, nor through the dispute resolution program established by VeraSafe, you may have the right to require that we enter into binding arbitration with you pursuant to the Data Privacy Framework's Recourse, Enforcement and Liability Principle and Annex I of the Data Privacy Framework.

19. Regulatory Oversight

Amerisearch is subject to the investigatory and enforcement powers of the United States Federal Trade Commission.