ApplicantInsight.com Privacy Policy

Your privacy on the Internet is important to us. We would like to explain the types of information we gather and how we intend to utilize that data.

Information Collected by Applicant Insight

Applicant Insight collects two types of information.

1. **Personal Data** - is data that is information that in the aggregate, would be unique to an individual. Personal data includes, but is not limited to, a person's name, social security number, date of birth, home address, job history, etc. Generally, **Personal Data** is provided to our database by a person who is utilizing our system to apply for a job. **Personal Data** maybe also be provided to us from other sources such as client corporations, or other third party databases. It is our policy that **Personal Data** belongs to the person to whom the information relates. The data is not given, transferred, shared, sold or traded to anyone unless the person to whom the information relates instructs **Applicant Insight** to do so.

2. **System Utilization or Aggregated Data –** is any information that is not included under our **Personal Data** category described in the previous paragraphs. **System Utilization or Aggregated Data** includes answers to survey questions, web site utilization statistics, site registration data and/or the frequency with which a page on our web site is visited. For example, **Applicant Insight** collects IP addresses. An IP address is a number that is automatically assigned to a User's computer whenever he/she is "surfing" the Web. Web servers - the computers that "serve up" Web pages - automatically identify the User's computer by its IP address. When a page is requested from **Applicant Insight**, our servers log the requesters IP address. **Applicant Insight** collects IP addresses for the purposes of system administration and to provide aggregated data to advertisers about the volume of use on **Applicant Insight's** website.

Personal Information Disclosure: United States Or Overseas

Generally, **Applicant Insight** does not transfer information to third parties outside of the United States or its territories. Such transfers would only be done if necessary to complete an international background check (e.g., conducting an international criminal check).

Use of Cookies

Applicant Insight uses *cookies* to collect information. A *cookie* is a small data file that most major web sites write to your hard drive for record keeping purposes when a person visits a site. Cookies allow **Applicant Insight** to measure activity on the Site and to improve the User's experience. This information is continuously analyzed by **Applicant Insight** to make improvements and updates based on which areas are popular and which are not. **Applicant Insight** does not use cookies to retrieve information from a User's computer that was not originally sent in a cookie. Except for personal information voluntarily provided by the User **Applicant Insight** does not use information transferred through cookies for any promotional or marketing purposes, nor is that information shared with any third parties at any time. A User may occasionally get cookies from our partners, which is standard in the Internet industry. **Applicant Insight** does not control these cookies, and these cookies are not subject to **Applicant Insight's** privacy policies.

Most browsers are initially set to accept cookies. If the User would prefer, he/she can set their browser to refuse cookies or to be alerted when cookies are being sent. However, it is possible that some parts of the Site will not function properly if you do so.

Links to Other Sites

It is important to note that **Applicant Insight's** web site contains links to sites other than our own and that those sites may not follow the same privacy policies as we do. For instance, if the User clicks on an advertisement on **Applicant Insight's** web site; this will take him/her away from **Applicant Insight's** web site to an entirely different site. This can include links from advertisers, content providers and partners who may use **Applicant Insight's** logo and or style as a result of a co-branding agreement. These sites may send their own cookies to the User, and may collect information and make uses of it that **Applicant Insight** would not.

Safe Harbor Framework

Applicant Insight continues to comply with the previously established U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Applicant Insight continues to adhere to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement, detailed as follows.

1. **Notice:** Applicant Insight collects consumer or applicant data from and for prospective and current employers related to the background screening process for the purpose to making employment decisions.

2. **Choice:** Applicant Insight provides individuals the opportunity to choose (opt out) whether their personal information can be disclosed to a third party or will be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.

3. **Onward Transfer:** To disclose information to a third party, Applicant Insight applies the Notice and Choice Principles. When applicant Insight transfers information to a third party that is acting as an agent, Applicant Insight requires the agent or agency to enter into a written and legally binding agreement requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles applied by Applicant insight.

4. **Security:** Applicant Insight has taken exceptional care in the development of our physical security, internal processes, and systems to ensure that sensitive information remains secure and protected from loss, misuse and unauthorized access, disclosure, alteration and destruction. Ai's systems implement several layers of security features that are designed to ensure confidentiality and integrity of applicant and client data. These layers are a combination of industry proven concepts and industry standard software, including but not limited to a User ID / password paradigm for web and system access, data transfers under the HTTP / SSL industry requirements, industry standard vendor IDS (Intrusion Detection System) solutions, and virus defense software scanning application of all data file transfers to and from Ai's Servers.

5. **Data Integrity:** To the extent necessary for the purpose of ensuring personal information be

utilized and relevant only for the purposes for which it is to be used, and minimizing the risk of information being collected or applied in a way that is incompatible with the initial purposes as authorized by the individual, Applicant Insight takes reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

6. **Access:** In compliance with, and as dictated by the Fair Credit Reporting Act, individuals and consumers have access to personal information about them that Applicant Insight holds and are able to correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access is not in violation of the FCRA and would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. **Enforcement:** Applicant Insight's privacy protection includes mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relates are affected by non-compliance with the Principles, and consequences for involved entities when the Principles are not followed. These mechanisms include, but are not limited to:

    a. Available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide

    b. Appropriate follow up procedures for verifying that the attestations and assertions made by businesses about their privacy practices are true, and that privacy practices have been implemented as presented; and

    c. Acknowledgement obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations.

Complaint Resolution

Regulated by the Federal Trade Commission and the Consumer Financial Protection Bureau, Applicant Insight has committed to cooperate with all reputable data protection authorities and/or their appointed representatives for dispute resolution related to certifications and practices.

Contact Information Regarding Privacy Policy

To obtain additional information regarding our Privacy Policy, or to obtain information regarding policies in the event of a compromise of your personal information, please contact us at:

Gregory Kirsch
Executive Vice President, Operations and Compliance
Applicant Insight
PO box 458
New Port Richey, FL 34656
compliance@ainsight.com
1-800-245-2318

Applicant Insight reserves the right to change this policy at any time by posting a revised privacy policy online.

USE OF THIS SITE SIGNIFIES YOUR AGREEMENT TO THE USAGE AGREEMENT.