GENERAL PRIVACY AND SECURITY POLICIES
INCLUDING
PRIVACY/SECURITY POLICY FOR OBTAINING INFORMATION FROM EUROPEAN UNION, UNITED KINGDOM AND SWITZERLAND

PRIVACY POLICY

Shield Screening ("Shield Screening") is a consumer reporting agency. It is required by the Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.* ("FCRA") to maintain the confidentiality of all consumer information. We are considered a "processor" under the General Data Privacy Regulation ("GDPR") of the European Union and similar laws.

Shield Screening obtains information on an individual consumer only upon the request of a user who has a legal permissible purpose under the FCRA to request information on that consumer in order to provide consumer reports. The FCRA requires a user for employment purposes to certify to us that it has a permissible purpose for the report and has obtained the written consent of the consumer to request information before we can supply the requested information.[1] The user must submit to reasonable audits by us to confirm that it is, in fact, obtaining such consents. All users must certify that they have a permissible purpose to request a report such as credit, insurance, and renting an apartment. Our customers agree to keep consumer information confidential and secure.

We do not maintain a database of consumer information. However we do maintain historic copies of prior reports to establish prior and current compliance with federal and state privacy laws. An individual, when we have obtained information from the European Union, United Kingdom or Switzerland, may request that we delete all information that we have on them obtained from those countries. This request will be honored unless there is a legal requirement that we keep the information, e.g., California requires that we keep copies of all reports for two (2) years.

We do not send consumer information outside of the United States for any purpose other than to deliver a report to an end user. Of course if information is sought from outside of the United States, the information is gathered in that country and then transmitted to us here in the United States where it is treated as any other confidential consumer information.

Any information gathered on any consumer may only be provided to the user authorized by the consumer or permitted by the FCRA or the GDPR or similar state law to receive the information. We cannot and do not share, sell or distribute consumer information with or to any third party other than the requesting party thereof. Any consumer, upon proper identification, has the right, under the FCRA or GDPR, to request us to furnish to the consumer any and all information we may have on that consumer. The consumer has the right to dispute the accuracy or completeness of any information contained in the consumer's file. Such investigations under the FCRA are completed within thirty (30) days of receiving the dispute which has been reasonably identified.

[1] There is an exception for employer investigations of suspected employee misconduct or for compliance with law or employer policies, e.g., sexual harassment investigations, but this exception will not apply to GDPR covered information or information from United Kingdom or Switzerland.

The following information is gathered from the person the consumer has authorized to obtain a consumer report on them, which are "identifiers" which help us to correctly identify information as relating to the subject consumer such as: full name, former names, alias names, nicknames, addresses, email addresses, full date of birth, social security number, other government issued identification information and driver's license number. In turn, we retrieve the following information: civil and criminal court records, bankruptcies, worker's compensation, past and current addresses, employment, license and education verifications, employment histories, tenant history, driving records (including personal identifying information) and credit. Not all reports have all this information. Each requestor will elect to receive information needed for their relationship with the consumer. Further, there may be federal, state or local law that prohibit the user from obtaining or using some information and we do not provide that when such limitations are known.

Email addresses are obtained to facilitate communication with the subject consumer in an efficient way. To protect the consumer we do not share your email account.

We process information by either contacting the original source of the information, such as a court or government agency or through a third party vendor. Those sources will be provided some or all of the identifiers we received from the requestor to be able to locate records or information on the subject. This information is communicated by encrypted email or fax to protect the information. These third parties may be outside of the United States, but no information on the consumer is maintained by these parties.

The information we collect is used solely to create "consumer reports" for the requestor. The requestor must have a use, reason, authorized by law to request the information. Each user is investigated to establish that it is a legitimate business and has the claimed permissible purpose. Generally our reports are ordered for employment or tenant screening.

The information we collect is used solely to create reports. We do not disclose it to anyone other than the requestor and the subject consumer. On occasion, a report may be shared with those who are participating in the same transaction with the requester, e.g., subcontractor and general contractor, placement service and employer, etc.

The following third parties will have access to the information: the requestor, joint users and third parties from when we obtain the information. Information may be requested or subpoenaed by the government or private citizens engaged in civil litigation. Disclosures in civil actions are subject to protective orders issued by the court to protect the consumer's information.

We do not engage in the use of "cookies". There is no release of information to others than the consumer except for those authorized by the consumer. The information is secured as noted below. If there is a breach of security involving your information, you will be promptly advised.

Rights Under the GDPR

In regard to information received from the European Union, United Kingdom and Switzerland you have the following rights:

- To know that we are processing your information. We are identified in any consent to a report being obtained.

- To receive the data we have on you in a readable format.

- To dispute and request correct information and be advised as to outcome of such a request. You may contact us at: (918) 970-2802.

- To have your data removed or blocked unless we are legally required to keep it. You can contact us at: (918) 970-2802.

- To revoke your prior consent. You can contact us at: (918) 970-2802.

- To restrict processing of your information, if:
  - you are disputing it;
  - processing is unlawful;
  - controller, our customer that received the report, no longer needs the data;
  - you have contested the basis for the controller to have information;
  - you may consent to the specific processing;
  - right to know if a redaction or processing is being lifted;
  - right to complain to our privacy data protection officer at: (918) 970-2802.

However, we may be required, upon receipt of a court order to release the information in civil or criminal litigation, or as otherwise required by law, to disclose information, regarding a consumer to law enforcement or regulatory agencies.

SECURITY POLICY

Shield Screening maintains the following security measures among others to protect consumer information:

- Access to confidential consumer information is limited within and without our company to those who have a need to know the information: obtaining and transmitting information on the consumer or those dealing with a consumer request for information, providing information to us or consumer disputes.

- Access to our computer terminals, file cabinets, fax machines, trash bins, desktops, etc. are secure from unauthorized access.

- We maintain a secure network to safeguard consumer information from internal and external threat, e.g., firewall and antivirus protection.

- Any backup data is maintained in an encrypted form.

- Access by users over the internet requires a confidential user name and strong alpha/numeric password.

- Email transmission of personal identifying information is encrypted.

- We maintain records on each request for information and identify each user who requested information on a consumer.

- Our employees are prohibited from “browsing” files or databases without a business justification.
- Any non-employee on our premises is subject to approval for entry and is monitored.
- Employees are not allowed to order reports on themselves, family, friends or associates without approval of management.
- Destruction of consumer information follows the federal regulatory requirements that the information be unreadable upon disposal.
- We maintain an ongoing relationship with a technical security service to monitor and update our system as needed.