



## **Safe Harbor Privacy & Security Policy Statement**

As a global provider of electronic discovery and related services, InfoCheckUSA, LLC places the highest value on ensuring the security of all data entrusted to us by our law firm and corporate clients. We respect individual privacy rights and have established internal protocols to assure that our security and privacy practices and procedures comply with both US and international law. The following Safe Harbor Privacy Policy describes the principles we agree to follow with respect to the collection, preservation and transfer of personal data from the European Union ("EU") and/or the European Economic Area ("EEA") to the United States for electronic data discovery processing, Web hosting, and related services.

### **Safe Harbor**

The European Parliament and the Council of the European Union adopted Directive 95/46/EC on Data Protection to set standards for the security and transfer of personal data. The Data Directive limits the transfer of personal data to countries outside of the EU and the EEA for processing to only those countries that can ensure an adequate level of protection for an individual's personal data. The United States Department of Commerce and the European Union developed a set of Safe Harbor Principles regarding personal data privacy and security that, when followed, permit an organization to certify that it provides adequate protection for the transfer of EU personal data to the US for processing. InfoCheckUSA, LLC fully commits to follow the Safe Harbor Principles with respect to all personal data received from any individual or entity in the EU or the EEA.

### **Definitions**

Directive -- The Directive is the European Union's Directive on Data Protection which took effect in October 1998.

Safe Harbor Privacy Principles - - These are the principles developed by the EU and the United States Department of Commerce to ensure that entities not covered by the Directive adhere to privacy principles after receiving personal data and personal information from the EU.

Personal data - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Processor - A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

Controller - The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of

personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

### **Notice and Choice**

When acting as a data processor within the meaning of the Data Directive, InfoCheckUSA, LLC reserves the right to process personal information on behalf of and under the direction of our law firm and corporate clients without providing notice to individuals or Data Protection Authorities to the extent permitted by the Safe Harbor Agreement. When collecting data in the EU, InfoCheckUSA, LLC acts on behalf of and under the direction of our law firm and/or corporate clients, to collect only data relevant to the litigation or other matter at hand. Individuals and business entities from which we collect data are provided with information regarding the purpose for which data is being collected, how it will be used and the type of non-agent third parties, if any, to which we disclose personal information. These individuals or entities are also provided with information about the choices and means offered by InfoCheckUSA, LLC for limiting the use or disclosure of their personal data.

### **Disclosure and Transfer**

InfoCheckUSA, LLC will not disclose an individual's personal data to any third party without the consent of our company or corporate clients unless one or more of the following are true:

- The individual has consented, in writing, to the disclosure;
- The disclosure is required by law or other professional standards;
- The personal data is publicly available;
- The disclosure is reasonably necessary for the establishment or defense of legal claims;
- The transferee provides an adequate level of protection for the personal data within the meaning of the Data Directive or has agreed in writing to provide an adequate level of protection for the personal data consistent with the options provided in the Data Directive for transfers pursuant to written agreements;
- In the event of a sale or transfer of assets in connection with an acquisition, merger, reorganization, sale or bankruptcy, InfoCheckUSA, LLC reserves the right to make such disclosure upon providing notice to the law firm and/or corporate clients for whom such data is being held.

### **Access**

InfoCheckUSA agrees to offer individual citizens of the EU or EEA with access to their personal data for purposes of correcting, amending or deleting inaccurate information unless the cost or burden of providing the access and changing or deleting the data proves unreasonable in view of the risk to the individual's privacy. A reasonable fee compensating InfoCheckUSA, LLC for resource use related to accessing, changing or deleting the personal information may be imposed.

### **Security**

InfoCheckUSA, LLC takes reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Our security measures include physical, electronic, workflow and managerial protocols to safeguard and secure the personal data we process.

The InfoCheckUSA web system automatically reviews passwords as clients, researchers and administrator log onto the system. If the password doesn't meet the "strong password" standard, the user will be taken to a page to update the password. The system also has an auto timed logout feature.

We monitor all Client Account Registrations and record the IP ADDRESSES for Security purposes. Our system monitors all credit card transactions for fraud. Credit Card fraud will be investigated and prosecuted to the fullest extent of US and International law by our legal team.

All InfoCheckUSA background investigators are licensed by the State of Florida and have passed fingerprinted background checks. All Court Researchers are ISO certified and have been background checked.

The system utilizes a 256-bit SSL certificate which is the industry standard level of encryption for communication. In addition, the system is password protected and gives each user their own account name and password. For each order that is placed, we store the IP address which the order originates from. The login activity and IP address is also logged with each login attempt and success.

***Sensitive Information such as DOB's and SSN's are obscured on all reports that are accessible via the Internet and also when in delivery transit (email & fax).***



The network is protected by an enterprise level firewall system, and the OS is audited weekly to make sure the latest security patches are installed on the system. The database server is password secured on the OS level and then on the database application level. Additionally, the systems are located at a dedicated co-location facility that has electronic and physical security 24/7/365.

**Here are some additional details about the infrastructure:**

***Security Summary***

- *128/256 bit encryption (GeoTrust)*
- *IP tracking for logins*
- *Login history tracking*
- *IP tracking for orders*
- *Obscuring of Personal Identifiers*
- *Enterprise Firewall Protection*
- *Enterprise AntiVirus Software*
- *Weekly OS security patches*
- *Tri level password protection at the application, database, and OS levels*
- *24/7/365 Electronic and physical security*

***Desktop Security Summary***

- *Norton Internet Security Suite*
- *Rapport Web Browser Security Software*
- *Weekly OS security patches*
- *PC & Screensaver password protected*



Due to the State of Massachusetts Law 201 CMR 17.00, MVR report results cannot be transmitted via email or fax. For your complete MVR report results, please view the report within your secure online account.

Instead of the full results, we will now send the following eMail message only for Massachusetts MVR's:

*"The Massachusetts Driving History Report is complete for [Applicant Name]. Due to the State of Massachusetts law 201 CMR 17.00, the results cannot be transmitted via email or fax. For the complete results, please view this report within your secure online client portal."*

### **Disaster Recover**

*We do data backups every 30 minutes on a continuous basis. The data is transferred to a separate backup server so the active data and backups are in physically different locations. In regards to disaster recovery, our servers are located in a state-of-the-art facility with a 24-7 physical presence and automated monitoring to minimize any disaster events.*

We also have multiple database and application servers which client systems can be operated from, so in the case of a failure, we are able to bring client systems online from different servers which are already configured and waiting to be utilized.

### **Data Integrity**

InfoCheckUSA, LLC processes personal information only in ways that are compatible with the purpose for which the data was collected or subsequently authorized by the individual. InfoCheckUSA, LLC will take reasonable steps to ensure information is relevant to its intended use and remains accurate, complete and current.

### **Compliance:**

InfoCheckUSA, LLC will follow any advice given by the Data Protection Authorities, including remedial or compensatory measures for individuals affected by non-compliance, and will provide the Data Protection Authorities with written confirmation that such corrective action has been taken, subject to the Company's right to dispute the requested actions or remedial measures with the Federal Trade Commission.

### **DISPUTE RESOLUTION:**

Any questions or concerns regarding the use or disclosure of Personal Information should be directed to the InfoCheckUSA, LLC Privacy Office at the address given below. InfoCheckUSA, LLC will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Information in accordance with the principles contained in this Policy. For complaints that cannot be resolved between InfoCheckUSA, LLC and the complainant, InfoCheckUSA, LLC has agreed to participate in the dispute resolution procedures of the panel established by the European data protection authorities to resolve disputes pursuant to the Safe Harbor Principles.

## **Contact Info for Consumer Complaints and Investigations**

InfoCheckUSA, LLC

13820 Old St. Augustine Rd Suite 113-151

Jacksonville, FL 32258

PH: 1-888-968-8374

FAX: 1-888-827-4468

E: [Sales@InfoCheckUSA.net](mailto:Sales@InfoCheckUSA.net)

InfoCheckUSA.com websites may contain links to other "non-InfoCheckUSA" websites. InfoCheckUSA assumes no responsibility for the content or the privacy policies and practices on those websites. InfoCheckUSA encourages all users to read the privacy statements of those sites; their privacy practices may differ from those of InfoCheckUSA.

## **In Summary**

InfoCheckUSA, LLC is committed to full compliance with Safe Harbor Privacy Principles under this Privacy & Security Policy. Questions or complaints should be directed to the Company's president & Chief Executive Officer. We are committed to protecting your privacy. We use the information we collect on the site to make ordering at InfoCheckUSA, LLC. possible and to enhance your experience. We do not sell, trade or rent your personal information to others. We utilize and implement the best security protocols available to protect consumers data and personal information.