Data Driven Safety, LLC
9525 Birkdale Crossing Dr, Ste 300
Huntersville NC 28078
www.datadrivensafety.com

Current Revision: MARCH 3, 2017

DATA DRIVEN SAFETY, LLC

DATA PROTECTION

Background

Data Driven Safety, LLC ("**DDS**", "**we**" or "**us**") is committed to protecting the privacy of our corporate subscribers, their employees and visitors to datadrivensafety.com or any of its affiliated subdomains (the "Website"). DDS is determined to safeguard from improper use or disclosure sensitive information about you. To protect that information, DDS has adopted this Privacy and Data Security Policy ("**Policy**") and other related procedures and practices. This Policy limits access to the personally identifiable information that was provided to us by you or on your behalf as a result of your enrollment in our Envision employer notification and safety system ("**Driver Monitoring System**") or your enrollment in our criminal activity alert system ("**Criminal Monitoring System**"). This information will be referred to throughout as "Your Personal Data."

Policy Applies to DDS

This Policy covers Your Personal Data under our control and requires us to maintain reasonable safeguards to protect against its loss, misuse or unlawful disclosure. Information disclosed or made available through the Website will often contain information from third parties that are not required to abide by this Policy. Please view and access such third-party content on or through the Website at your own risk and with an understanding that our Policy does not control the content, practices, polices or actions of any person or organization other than DDS and its **employees.**

Revisions to this Policy

This Policy may evolve over time in response to changes in our service offerings, available technology, accepted industry practices and new legal requirements. Any material changes to this Policy will be communicated, to the extent practical, via a notification on the Website at least thirty (30) days before the change goes into effect. Policy revisions made without this advance notice shall be accompanied by a Website notification. Information collected under a prior version of this Policy will continue to be protected by the terms of that prior Policy.

Information We Collect

We collect Your Personal Data from a variety of sources. The data you choose to input into this Website is one such source. For example, we record the information you submit through the Website for the Driver Monitoring System when creating or updating your driver profile, reporting traffic incidents, or requesting additional information. Provided you are enrolled in the Driver Monitoring System and changes are permitted by your employer, you may modify, delete or add additional personal information through your account online at any time via the Website or by contacting us directly. We will also use other sources to collect and confirm Your Personal Information for both the Driver and Criminal Monitoring Systems. These may include your employer, various state and federal governmental agencies and certain public record sources.

Information We Do Not Collect

Traffic to the Website is monitored for administrative purposes only. We do not offer services to individuals under the age of 13 or knowingly collect information about children under the age of 13.

Using Collected Information

We use your personally identifiable information to provide the Monitoring Systems. This service requires that we access various governmental organizations that create or store information about you. Some of these sources require authentication by providing a portion of Your Personal Data.

If you are enrolled in the Driver Monitoring System, then you have authorized us to access these sources by providing confirmation of Your Personal Data (a state agency responsible for issuing driver records, for example, may require your birth date and driver's license number to permit a driver status check). Some aspects of the information we gather about you will be provided to your employer. If the driver portal has been authorized by your employer, then we will use our best efforts to provide a copy of that notification to you through the Website at the same time it is provided to your employer. If the provided information is incorrect, redundant or incomplete, then you should ensure that it is updated. We do not and cannot update public records maintained by governmental agencies, as our access rights are "read only."

We also reserve the right to share your personally identifiable information to the extent we believe disclosure is required of us by law or is necessary to protect or enforce our legal rights.

Disclosure Restrictions

Many state and federal laws are designed to protect the privacy of personally identifiable information. DDS complies with (and shall continue to adhere to) all applicable laws, placing special emphasis on meeting the requirements of those state and federal laws focused on data security and privacy.

We do not sell, trade, or rent Your Personal Data that was provided to us by your employer or by you with any others accept to the extent that such disclosure has been permitted by you or is permitted by the DDS Terms and Conditions of Use. Please contact us if you wish to obtain a copy of all written documents (including reproductions of electronic forms submitted through the Website) in which you authorized us to share any aspect of your personal information with others.

Security and Data Redundancy

We limit access to your personally identifiable information within the DDS organization to those persons who must have the information to provide our services to our customers. We meet (and will continue to meet) strict physical, electronic and procedural security standards, including stringent internal access protocol, to protect your information. For example, our data servers are centrally located within our offices and both physical and network access to the information contained therein is restricted and highly controlled. Diverse layered firewalls with stringent access control lists also help us to insulate sensitive data from unauthorized access. A secure data connection accompanies all information transfers that relate to your personal information. In addition, all subscribers to the Notification Systems are required to use Client/Server Identification and Authorization. As an additional security measure we “back up” the data stored on our systems and maintain one or more off-site copies of the data stored at our facility. Data archived for back-up purposes at a given point in time may include information that you corrected or deleted after that back-up was made. We do not rely on archived data in the normal course of business. We follow procedures to restore only the most up-to-date information in the rare instance that we are required to utilize back-ups of a portion of our system information.

Contact Us

We respect the privacy of your personal information and understand the importance of keeping it secure. We are always open to your input on this important issue. You can reach us with any privacy questions or comments via the contact form on this website or by mail to: Privacy at Data Driven Safety, LLC,9525 Birkdale Crossing Drive, Suite 300, Huntersville, NC 28078.