



DATA DRIVEN SAFETY, LLC (“Company”)

Data Acquisition, Storage and Dissemination Policy

1. Purpose.

This policy explains Data Driven Safety's (hereinafter “we/us/our”) policies, practices and expectations for gathering, storing, managing and distributing data. It is intended as guidelines to help us maintain a rational and consistent approach to procuring/managing data while giving our data partners visibility into the standards we expect them to adhere to.

2. Data Acquisition.

We limit our acquisition of public and non-public information (hereinafter, the “DDS Data”) to established, reputable sources in the government and private sectors (hereinafter, the “Data Sources”). Our strong preference is to obtain information directly from the governmental source that created the relevant records.

All information within the DDS Data is and shall continue to be obtained by the Company in a lawful manner, consistent with any contractual obligations imposed by the Data Sources.

We will not consume from public records any “highly-sensitive information” including, medical records, social security numbers, restricted juvenile information, sealed case data or financial account numbers.

All information provided to us by our customers for matching and other similar services (hereinafter, the “Customer Data”) will be used in strict conformity to all legal and contractual obligations and, in no event, shall such data be commingled with the DDS Data.

We shall always strive to reduce the administrative burden of our requests for DDS Data on governmental personnel. This includes an obligation to make timely payments to Data Sources.

3. Accuracy of Collected Information.

At all times we shall use reasonable efforts to accurately consume, store, manipulate and reproduce the DDS Data. This means that we shall continue to pay special attention to properly interpreting records rather than “blindly” consuming information made available to us by governmental agencies.

No representation as to the accuracy, correctness, timeliness or completeness of the DDS Data will be made to customers and a disclaimer of such warranties will accompany all provision of data to third parties at least to the extent contractually required by the Data Sources.



4. Data Storage.

We shall at all times securely protect the integrity and confidentiality of the DDS Data and the Customer Data, specifically including any component of the information that identifies the individual associated with the record (e.g., date of birth, driver license number, etc.). DDS Data shall be purged in a timely manner and in accordance with all legal requirements. DDS shall not retain any protected health information data obtained from any third party (including, without limitation, its customers) for longer than is absolutely necessary to provide the contractually-required services. All such input data shall be purged in a manner that electronically separates the data such that it is unreadable by any known-to-DDS software program and DDS shall ensure re-assembly is not possible without a specialized script. DDS shall not create such re-assembly script nor shall it retain access to any portion of the electronically separated data sets.

DDS's executive team shall ensure that all employees and contractors receive routine training (at least annually) that highlight the importance of safeguarding all Customer and DDS Data. DDS shall continue to employ reasonable safeguards to limit access of the Customer and DDS Data within the employee group to those persons with a documented need-to-know.

Customer Data will be purged from all DDS systems within ten (10) business days of the earlier of (i) the cessation of services for such customer or (ii) such customer's written request to DDS. In addition, DDS shall honor a request to return such Customer Data to the originating customer if the request is made in writing. Notwithstanding the foregoing, DDS reserves the right to retain an archival copy of all Customer Data for legal compliance and audit purposes for ten (10) years. Such archived data shall not be accessed for any reason other than as necessary for DDS to comply with applicable legal requirements.

5. Data Dissemination.

We will only transact business with reputable customers that have provided satisfactory assurances of their legitimate, legal purpose for using DDS Data. DDS shall, to the extent commercially reasonable, take industry-acceptable efforts to confirm the foregoing before entering into a data arrangement with any prospective customer. Our provision of information to all customers shall be conditioned on execution, in advance, of a DDS-approved contract covering receipt and use of the DDS Data.

In no event shall we provide a subset of DDS Data to a customer (or any other third party) if the dissemination of that information will run counter to our contractual obligations or is adverse to any other lawful obligations imposed on DDS. In support of the foregoing, DDS shall maintain records (on a per-Data Source basis) as to use and dissemination limitations associated with the DDS Data.