DATA SECURITY FAQS

WHO WE ARE - We serve the automotive and related industries by providing technology that powers intelligent marketing across every touchpoint. Through our omni-channel marketing solutions, we help our clients, primarily automotive, RV, marine and power sport dealerships and manufacturers, to increase vehicle sales and service. Our company, Data Driven Holdings, LLC, operates multiple brands, each focusing on a specific industry sub-sector or service category. Our industry-leading brands include Team Velocity, Level 5, Advid, Tier10 and SocialDealer.

OUR TECHNOLOGY - Our patent pending technology platform Apollo® (marketed as Compass™ by Level 5) is the most advanced in the industry. Our platform eliminates the risks of traditional marketing techniques by utilizing intelligent, automated technology to generate dynamic campaigns across all advertising mediums, including Mail, Email, Consumer Portals, Search, Social Media and Point of Sale.

OUR APPROACH TO PRIVACY - We are committed to protecting the privacy of personal information and the responsible use of that information to deliver personalized, relevant content to consumers on behalf of our clients. We have implemented additional policies and procedures to comply with the California Consumer Privacy Act (CCPA). Please review our **Privacy Policy** located on each of our brand websites to learn more about our privacy and CCPA compliance practices.

OUR CLIENT'S INFORMATION AND CONSUMER DATA - To provision our services, we require limited access to client systems to obtain certain information about their operations, as well as certain data about their customers. This data belongs to the client; we cease using and promptly remove it from our systems upon client request or conclusion of our business relationship.

OUR APPROACH TO SECURITY - We have implemented cybersecurity policies and procedures across our organization based on industry best—practices and regulatory requirements. Our security measures including hosting data offsite at Equinix SSAE16 compliant datacenters, deploying firewall and security protocols across our network, encrypting sensitive data in transit, limiting data access to designated groups, requiring multifactor user authentication, and deploying physical security at our facilities and colocation sites. We regularly monitor our systems, including through independent third party-audits, to ensure on-going compliance.

OUR THIRD PARTY SERVICE PROVIDERS - We have partnered with, industry-leading DMS and data processing and integration providers. We contractually require any of our service providers who have access to client data to maintain cybersecurity insurance, meet all federal and state legal requirements, and follow industry-leading data security practices. We remain liable to our clients for our vendors' actions.

OUR CONTRACTUAL OBLIGATIONS - Our client agreements contain service provider data access and safeguards protections, in accordance with industry standards, and applicable laws, including the Gramm-Leach-Bliley Act, FTC Safeguards Rule, and CCPA. This includes our commitment to use consumer data for the sole, limited purpose of providing our services to our clients - and for no other purpose. We do not sell their data. Clients may review our contractual commitments under the Data Safeguards sections in the Terms & Conditions that govern their agreement with us.

YOUR DATA; OUR COMMITMENT - No company can guarantee information security with absolute certainty. But at our company, protecting client information and consumer data is at the core of our business philosophy. It informs every decision we make, from how we architect our IT systems, to the vendors we choose. Our clients entrust us with information about their most precious assets – their customers. We hold that trust sacred.