DATA SECURITY FAQS

MAY 2022

WHO WE ARE – Our company, Data Driven Holdings (*DDH*) is dedicated to serving the automotive industry. Through our industry-leading brands - Team Velocity®, Tier10®, Advid®, SocialDealer®, OfferLogix® and Qualified Customer - we deliver data-driven technology that powers intelligent advertising across every customer touchpoint, offering dealers and OEMs the most advanced sales and service marketing solutions in the business.

OUR CLIENTS' INFORMATION AND THEIR CUSTOMERS' DATA – We use customer data for the sole purpose of providing services to our clients; *we do not sell client or customer data*. This data belongs to our clients; we cease using and promptly remove it from our systems upon client request or conclusion of our business relationship.

OUR APPROACH TO PRIVACY – We are committed to protecting the privacy and ensuring the responsible use of our clients' customer information. We have implemented policies and procedures to comply with federal and state privacy laws and regulations. To learn more about our privacy practices, please read our **Privacy Policy**, located at the bottom of each of our brand websites.

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 include hosting data in the Google Cloud, deploying firewall and security protocols across our network, encrypting sensitive data, limiting user access, requiring multifactor authentication, and securing our facilities and colocation sites. We regularly monitor our systems and conduct independent third party audits to ensure on-going compliance.

OUR INSURANCE – Despite state-of-the-art security protections, data breaches and security incidents can occur. Therefore, we back up our commitments with professional and cybersecurity liability insurance.

OUR SERVICES PROVIDERS – We have partnered with industry-leading DMS and data processors/integrators. We contractually require our third party service providers with access to client data to meet all federal and state legal requirements, maintain cyber insurance, and follow industry-leading data security practices. At the same time, we remain liable to our clients for our vendors' actions.

OUR CONTRACTUAL OBLIGATIONS – The **Data Safeguards** section of our client **Terms & Conditions** set forth our contractual commitments to safeguarding our clients' and their customers' data, in accordance with industry standards and applicable laws, including the Gramm-Leach-Bliley Act, FTC Safeguards Rule and California Consumer Privacy Act.

OUR COMPLIANCE WITH FTC SAFEGUARDS – We comply with the amended FTC Safeguards Rule by:

- Appointing an IT expert to oversee our security procedures and report annually to our board of directors;
- Establishing a written incident response plan;
- Implementing policies and procedures for monitoring network activity and detecting unauthorized access;
- Providing employee security training;
- Evaluating service providers with access to customer information, requiring them to implement safeguards and monitoring their compliance;
- Establishing multifactor authentication for anyone accessing our information systems;
- Encrypting customer information in transit and at rest; and
- Securely disposing of customer data within the required timelines.

YOUR DATA; OUR COMMITMENT – No company can guarantee information security with absolute certainty. But at **DDH**, protecting client information and customer 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.