

This Privacy Statement covers the following entities, Data Search, Inc. referred to as “we”, “us”, and “our” throughout this statement.

We are committed to protecting our clients’ and their customers’ personal, public, non-personal, and nonpublic information. In the course of providing title, appraisal, and closing services to our clients, we need to collect and maintain certain nonpublic personal information about their customers. This privacy statement addresses what nonpublic personal information we collect, what we do with it, and how we protect it.

We do not disclose any nonpublic personal information about our clients or their customers to any nonaffiliated third parties, except when needed to perform the daily operations we have been contracted to perform or as described below.

When a client places an order, we sometimes require certain nonpublic types of information on their customer. We obtain this information via secure online order forms, fax, or through discussions we have with the client. This information could include the name, address, social security number, and phone number, of the customer(s).

We do not disclose any nonpublic information we collect to anyone, except if requested from the proper law enforcement agencies. We may also be required to disclose certain nonpublic information to our insurance agencies during the investigation of claims on title insurance policies or other title related products.

We maintain physical, electronic, and procedural safeguards that meet or exceed industry standards to guard all public and nonpublic information. We protect client account information and all of their customer information on secure sectors of our web servers. We use firewalls and other security technology to protect our network and systems from external attacks, and require the client to enter a unique username and password to access their account information online and to place orders for services online. We do not allow anonymous connections for placing orders or sending of information. Also, our servers have been enabled with Secure Socket Layer (SSL) technology to prevent unauthorized parties from viewing the public or nonpublic information that a client provides or accesses during a secure session. Data stored on the file systems are encrypted and protected with Access Control Lists (ACL).

In addition, if the client accesses information online, we use digital certificates to authenticate the client that is transacting with our Web site.

Our employees have access to the nonpublic information only on a “need to know” basis. We conduct regular internal audits of our business practices and procedures, examining confidentiality standards and information access in order to protect the nonpublic information.

We use “cookies” but only for authentication purposes. Our web servers utilize “session-based” authentication, whereby when a secure login to our web site is requested, the username and password are encrypted, sent to our servers and if authenticated, a “token” or “cookie” is sent back to the browser. This cookie contains only a session ID that matches that of the server and only for that specific browser session. Once the browser is closed, the session is terminated and the cookie destroyed.

We respect the privacy concerns of those that visit our sites. As a general policy, no personal information is automatically collected from the users of our sites. We do record certain non-personal information such as, the type of browser, operating system, pages viewed, and internet domain information in order to better customize the visitors experience. Other uses of this information include internal review of the number of users to the sites, but only in an aggregate and non-personally identifiable form. This data will not and never is provided to other parties for marketing, advertising or any other use.