California Apartment Association Privacy Statement

Effective Date: October 31, 2019

1. Introduction

This Privacy Statement ("Statement") explains our privacy practices and provides information on how the California Apartment Association ("California Apartment Association," "CAA", "we," or "us") collects, uses, and discloses such information. This Statement applies to any California Apartment Association website, application, product, software, or service (collectively, our "Services") that we operate and in which we post a direct link to this privacy policy.

The CAA is committed to the responsible handling and protection of the data it collects and receives, including personal information. Generally, personal information ("PI") is any information that that can be used directly or indirectly to identify, contact, or locate someone. Examples of personal information include real names, property addresses, mailing addresses, social security numbers, email addresses, phone numbers, bank account numbers, and driver's license numbers. Additionally, in California, personal information can include other information that can reasonably link to a particular person, such as IP addresses, unique device identifiers, employment information, and internet activity.

2. Updates to The Privacy Statement

It is important to check back often for updates to this Statement. If we make material changes, we will notify you by email or through a notice on our website.

3. Who This Privacy Statement Applies To

This Statement applies to individuals eighteen (18) years or older who use CAA's website, or any application, product, software or service that we operate and in which we post a direct link to this privacy statement. No parts of our services are directed, designed, marketed, or advertised to attract anyone under the age of eighteen (18). CAA does not knowingly collect personal information from anyone under the age of eighteen (18).

4. Data That We Collect and Receive

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device. We have collected the following categories of PI from consumers within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, e-mail address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card	YES

Records statute (Cal. Civ. Code § 1798.80(e)).	number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	YES
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	NO
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	YES

When you interact with us through the Services, we may collect specific pieces of PI from you or from other sources. This may be information that you directly provide to us, such as personal information you provide when you visit the Services, or information that is passively or automatically collected from you, such as information collected from your browser or device.

The specific pieces of PI data we collect consists of:

- **Data that you provide directly when you register for, or use, the Services.** This data will vary, but typically consists of name, email address, postal address, phone number and other similar contact data. We also receive data from the communications you send to us, such as customer service inquiries, product reviews and other feedback regarding the Services, such as customer satisfaction surveys.
- **User credentials**, such as username, password, password hints and similar security information used to create an account and authenticate users of the Services.
- **Demographic data**, such as age, birth date, address, gender, country and language preference.
- **Payment data**, such as credit card information (note: only the last four digits are collected) and billing address.
- **Device data**, such as type of device, operating system and other software installed on the device, device settings, IP address, device identifiers and error reports.
- **Usage data**, such as the programs and features you access, items you purchase, and the timing, frequency and duration of your interactions through the Services.
- **Location data**, such as IP addresses received from your device.
- **Information about your interests and preferences**, such as your favorite classes, compliance events, political events and credit screening, your home city or your communications preferences.
- **Third party integrations.** If you connect your use of the Services through a third-party service (e.g., on-line forms), the third party may share certain information from your third-party account with us.
- **Other third-party data**, such as data from our affiliates (chapters), partners or vendors, or public sources.

5. How We Collect Data

We collect personal information (PI) about you from your interactions with us, and from your employer if providing access to our Services (such data would be limited to the identity of your employer and your job title).

We obtain personal information **from you through**:

- **your interactions with us and our Services** such as, when you purchase or use our Services, register for an event, request information or call us for support (please note that we may record or monitor our telephone calls and events for compliance and quality assurance purposes);
- **your system/device and use of our Services** such as, our servers automatically collect certain information to help us administer, protect and improve users' experience. The information collected includes:
    - IP address and browser type;
    - Device information including Unique Device Identifier (UDID), MAC address;
    - Device operating system and other technical facts;
    - The city, state, and country from which you access our website;
    - CAA website pages visited and content viewed, stored, and purchased;
    - Information or text entered;
    - Links and buttons clicked;
- **cookies and similar technologies included on our Services**. A cookie is a small text

file that is placed on a computer or other device and is used to identify the user or device and to collect information. We use cookies and other similar technologies such as:

- **Flash cookies**: Flash cookies (also known as local shared objects) are designed to support browser content supported by Adobe® Flash. They are usually used to enable ads and video content on websites. Like other cookies, they will store information on your device, some of which will be specific to the Flash-enabled content. Flash cookies can only be deleted within Adobe Flash rather than via your browser.
- **Web beacons**: Our web pages may contain electronic images known as web beacons (also called single-pixel gifs and transparent graphic images) that we use to help deliver cookies on our sites, count users who have visited those sites, deliver Services, and analyze the effectiveness of our promotional campaigns, for example. We may also include web beacons in our marketing email messages or newsletters to determine whether an email is opened or if links are clicked.

We also collect personal information about you from **third parties and service providers** such as:

- **the person(s) arranging for you to access our Services** (e.g., your employer or our subscriber) in order to set up a user account;
- **an organization to which you belong** where that organization provides you access to our Services (such as a library providing you access to certain of our Services, like our legal information products);
- **partners and service providers who work with us** in relation to your Service.

6. Use of Personal Information (PI)

We use PI for legitimate business purposes, as well as for compliance purposes. For example, we use PI to provide and improve Services, administer our relationship with you, for marketing, and in order to exercise our rights and responsibilities. More detailed information about these legitimate interests follows below:

- to set up and administer your account, provide technical and customer support and training, verify your identity, and send important account, subscription and Service information;
- to administer our relationship with you, our business and our third-party providers (e.g., to send invoices);
- to deliver and suggest tailored content such as news, forms, education, and business information. We analyze the way you use our Services to make suggestions to you for features or Services that we believe you will also be interested in, and so that we can make our Services more user-friendly;
- to personalize your experience with our Services. We may retain your browsing and usage information to make your searches within our Services more relevant and use those insights to target advertising to you online on our websites and apps. Your choices in relation to marketing are explained in this Statement;
- to contact you in relation to, and conduct, surveys or polls you choose to take part in and to analyze the data collected for market research purposes;
- to display information you choose to post, share, upload or make available in chat rooms, messaging services, and community and event forums (including in community and event profiles) and for related collaboration, peer connection, games and information exchange;
- to provide any third party, who has made our Services available to you (e.g., your employer or our subscriber), insights about use of the Services;

- for internal research and development purposes and to improve, test and enhance the features and functions of our Services;
- to provide you with marketing as permitted by law;
- to meet our internal and external audit requirements, including our information security obligations (and if your employer or our subscriber provides for your access to our Services, to meet their internal and external audit requirements);
- to enforce our terms and conditions;
- to protect our rights, privacy, safety, networks, systems and property, or those of other persons;
- for the prevention, detection or investigation of a crime or other breach of law or requirement, loss prevention or fraud;
- to comply with requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, including where they are outside your country of residence;
- in order to exercise our rights, and to defend ourselves from claims and to comply with laws and regulations that apply to us or third parties with whom we work;
- in order to participate in, or be the subject of, any sale, merger, acquisition, restructure, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings).

Where we rely on legitimate interests as a lawful ground for processing your personal information, we balance those interests against your interests, fundamental rights and freedoms. We will not collect additional categories of personal information or use your personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

7. How We Share Personal Information (PI)

We share PI within the CAA, with our business partners, affiliates and service providers, the person providing for your access to our Services (if that is not you) and in accordance with law. Our service providers are not permitted to share or use PI we make available to them for any purpose other than to provide services to us.

We share your information for the purposes set out in this Statement, with the following categories of recipients:

- CAA affiliates (e.g. CAA Insurance, CAA Divisions and Chapters);
- Third parties providing your access to our Services (e.g., your employer or our subscriber);
- Service providers with whom we deliver co-branded Services, provide content, or to host events, conferences and seminars;
- Service providers that help us deliver Services or act on our behalf;
- Third parties where we have a duty to or are permitted to disclose your personal information by law (e.g., government agencies, law enforcement, courts and other public authorities);
- Third parties in order to participate in, or be the subject of, any sale, merger, acquisition, restructure, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings), in which case we may disclose your personal data to prospective buyers, sellers, advisers or partners and your data may be a transferred asset in a business sale;
- Third parties where reasonably required to protect our rights, users, systems and Services (e.g., legal counsel and information security professionals).

In the proceeding twelve (12) months, we have not sold any personal information.

8. How We Secure Personal Information (PI)

CAA takes the security of PI seriously and we use appropriate technologies and procedures to protect PI (including administrative, technical and physical safeguards) and protect against unauthorized access, use, and disclosure. We have an Information Security and Risk Management team, led by our Chief Information Security Officer, who is responsible for implementing secure data handling practices at CAA. Additionally, we require our third-party providers to implement and maintain similar security practices and procedures as well.

Our information security policies and procedures are based on generally accepted security practices, reviewed regularly, updated as necessary, and designed to meet the sensitivity of the personal information we handle, changes in technology, and regulatory requirements.

9. Your Rights Under California Law

The California Consumer Privacy Act of 2018 provides California residents specific rights regarding their personal information. Any terms defined in the CCPA have the same meaning when used in this notice.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past twelve (12) months. Once we receive and confirm your verifiable request, we will disclose to you:

- Categories of personal information we collected about you;
- Categories of sources of personal information we collected about you;
- Business or commercial purposes for collecting and selling your personal information;
- Categories of third parties with whom we share your personal information;
- Specific pieces of personal information we collected about you (data portability request);
- If we sold or disclosed your personal information for a business purpose, two (2) separate lists disclosing:
    - Sales, identifying the personal information categories that each category of recipient purchased; and
    - Disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from your records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our

contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise your free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *seq.*).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling 800-967-4222 or
- Emailing membership@caanet.org

Only you or a person registered with the California Secretary of State that you authorize to act on your behalf may make a verifiable consumer request related to your personal information. Additionally, you may make a verifiable consumer request on behalf of your minor child. You may only make two (2) verifiable consumer requests for access or data portability within a twelve (12) month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative and
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm that the personal information is yours. Making a verifiable consumer request does not require you to create an account with us and we will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We strive to respond to a verifiable consumer request within 45 days of receipt. If we require more time, we will inform you of the reason and extension period (up to 90 days) in writing. If we have an email for you when submitting a verifiable consumer request, we will deliver our responses by email, otherwise it will be through mail. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response will also explain the reasons we cannot comply with a request, if applicable. For data portability requests,

we will select a format to provide your personal information that is readily usable and should allow you to transmit the information form one entity to another entity without hinderance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by CCPA, we will not:

- Deny you goods or services;
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits or imposing penalties;
- Provide you a different level or quality of goods or services;
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

California Do Not Track (DNT) Disclosure

Your browser settings may allow you to automatically transmit a "Do Not Track" signal to online services you visit. The CAA website does not track its visitors over time and across third party websites to provide targeted advertising and therefore does not respond to Do Not Track (DNT) signals. For more information on "Do Not Track," visit http://www.allaboutdnt.com.

10. Additional Terms for International Visitors

We are based in the U.S. and the information we and our service providers collect is governed by U.S. law. If you are accessing the Sites from outside of the U.S., please be aware that information collected through the Sites may be transferred to, processed, stored and used in the U.S. Data protection laws in the U.S. may be different from those of your country of residence. Your use of the Sites or provision of any information therefore constitutes your consent to the transfer to and from, processing, usage, sharing and storage of your information, including Personal Information, in the U.S. as set forth in this Statement.

11. Additional Terms for EU Visitors

The following applies to individuals protected by the European Union's General Data Protection Regulation ("GDPR") who accesses our Services or otherwise provides us with personal information.

The data collector for this website is CAA. We process your personal information on several different legal bases, as follows:

- Contract Performance: Where we have a contract with you, we will process your personal information in order to fulfil that contract (i.e. to provide you with Services).
- Consent: If we are required to obtain your consent to process your personal information, we may perform such processing on the basis of your consent. In such cases, you may withdraw your consent at any time without affecting the lawfulness of prior processing. Providing your consent is voluntary, but we may not be able to provide you with a service for which we require your consent

until we obtain it.

- Legal Obligation: We may process your personal information as necessary to comply with relevant laws, regulatory requirements, and to respond to lawful requests, court orders, and legal process.
- Legitimate Interest: We may process your personal information as necessary to pursue our legitimate interests, for example to fulfill any requests you may make in connection with your submission of personal information, to monitor and improve the quality of the website, and to protect and defend our rights, property or safety or that of our other users of the website.

Data Subject Rights

Under the GDPR, you may have the following rights:

- The right to obtain form us confirmation as to whether your personal data is being processed, and, where that is the case, to request access to the personal data;
- The right to have personal data rectified if it is inaccurate or incomplete;
- Subject to limitations as provided for in the GDPR, the right to ask us to erase your personal data;
- Subject to limitations as provided for in the GDPR, the right to request restriction of processing of your personal data;
- The right to obtain your personal data in a structured, commonly used, and machine-readable form which you have provided to us, and to reuse it for your own purposes across different services;
- The right to object to processing based on legitimate interests or direct marketing.

To exercise your rights, please contact us at the information given in Section 13 below.

12. Third-Party Providers

Within our Services, there may be links to third-party websites or applications that are controlled by third-party providers. This Privacy Statement does not apply to any third-party website or service you may access through our website. You should check those websites or applications for their privacy statements and terms that apply to them.

13. How to Contact Us

If you have questions or concerns about this notice, our privacy practices, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please contact us at:

California Apartment Association Data Protection Officer:

Kevin Pellegrino
California Apartment Association
980 Ninth Street, Suite 1430
Sacramento, CA 95814
Website: caanet.org
Email: kpellegrino@caanet.org