CCPA Policy

I. Policy

Ganas Holdings, LLC ("Company") will ensure that it provides all consumer rights and otherwise complies with all applicable obligations of the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.* (the "CCPA"), and applicable regulations when finalized.

II. Governing Law

A. Scope

The CCPA provides "consumers" with certain rights relating to their "personal information" collected by certain "businesses." Those businesses and their service providers are required to honor consumer rights and comply with other obligations under the law, subject to several express exemptions and exceptions. The CCPA's scope is defined by these three terms:

- "Business" means:
  - A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
    - Has annual gross revenues in excess of $25 million. This amount will be adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.
    - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices.
    - Derives 50% or more of its annual revenues from selling consumers' personal information.
  - Any entity that controls or is controlled by a business as defined above and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

- "Consumer" means a natural person who is a California resident, however identified, including by any unique identifier. The term "resident" includes (1) every individual who is

in California for other than a temporary or transitory purpose, and (2) every individual who is domiciled in California who is outside California for a temporary or transitory purpose.

- "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
    - Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
        - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.
        - Any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card 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. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
        - Characteristics of protected classifications under California or federal law.
        - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
        - Biometric information.
        - Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
        - Geolocation data.
        - Audio, electronic, visual, thermal olfactory, or similar information.

        - Professional or employment-related information.
        - Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C.§ 1232g, 34 C.F.R. Part 99).
        - Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.
    - "Personal information" does not include publicly available information, deidentified, or aggregate consumer information, as defined:
        - "Publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.
        - "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.
        - "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer provided that a business that uses deidentified information:
            - Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
            - Has implemented business processes that specifically prohibit reidentification of the information.
            - Has implemented business processes to prevent inadvertent release of deidentified information.
            - Makes no attempt to reidentify the information.

B. Rights and Obligations

The CCPA provides the following consumer rights and business obligations:

1. <u>Notice at Collection</u>

A business that collects a consumer's personal information must, at or before the point of collection, inform consumers of:

- The categories of personal information to be collected; and
- The purposes for which the personal information will be used.

A business may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice.

2. Right to Know

Upon receipt of a verifiable consumer request, a business that collects personal information must disclose to the consumer the categories and specific pieces of information that the business has collected in the previous 12 months. That disclosure must include:

- The categories of personal information the business has collected about the consumer. The categories of personal information track the definition of personal information.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with whom the business shares personal information.
- The specific pieces of personal information the business has collected about that consumer.

Upon receipt of a verifiable consumer request, a business that sells the consumer's personal information or that discloses it for a business purpose, must disclose to the consumer:

- The categories of personal information that the business has collected about the consumer.
- The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.
- The categories of personal information that the business disclosed about the consumer for a business purpose.

Here, "business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information is reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

- Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

- Debugging to identify and repair errors that impair existing intended functionality.
- Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
- Undertaking internal research for technological development and demonstration.
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

The business must disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request. The business must promptly take steps to determine whether the request is a verifiable consumer request, but this will not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

The disclosure must be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested but may not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account. A business may provide personal information to a consumer at any time but is not required to provide personal information to a consumer more than twice in a 12-month period.

A business is not required to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

The business must make available to consumers two or more methods for submitting requests for this information, including, at a minimum, a toll-free telephone number, except that a business that operates exclusively online and has a direct relationship with a consumer from

whom it collects personal information is only required to provide an email address for submitting requests. A business that maintains an internet website must make the website available to consumers to submit requests.

3. Right to Opt Out

A consumer has the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. A business that sells consumers' personal information to third parties must disclose to consumers that their information may be sold and that consumers have the right to opt out of the sale of their information. Once a consumer has effected an opt-out, the business is prohibited from selling that consumer's personal information unless the consumer subsequently provides express authorization for the sale of his or her personal information.

The CCPA also imposes additional notice obligations on a business subject to the opt-out requirement:

- Provide a clear and conspicuous link on its Internet homepage entitled "Do Not Sell My Personal Information." The link must take a consumer to a web page where the consumer, or a person authorized by the consumer, can opt-out of the sale of the consumer's personal information. The business cannot require the consumer to create an account in order to elect the opt-out.
- A description of a consumer's right to opt-out of the sale of personal information, as well as a link to the "Do Not Sell My Personal Information" web page must be included in:
    - The business's online privacy policy; and
    - Any California-specific description of consumers' privacy rights.
- Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or compliance with CCPA are informed of all requirements related to the Notice at Collection, the rights to disclosure of personal information collected, sold, and disclosed for a business purpose, the right to have certain personal information deleted, the opt-out right and how to instruct consumers to exercise their opt-out rights, and the right to be free from discrimination based upon the exercise of these rights.
- When a consumer has opted-out of the sale of his or her personal information, the business must wait at least 12 months before asking the consumer to authorize the sale of personal information.
- Any personal information collected from the consumer in connection with an opt-out request must be used only for the purpose of complying with the opt-out request.

The CCPA expressly authorizes businesses to comply with the opt-out request by setting up a separate homepage dedicated to California consumers, if the business takes reasonable steps to ensure that California consumers are direct to the California homepage. We would note however, that there are a number of practical challenges with this approach. Using IP addresses or geo-fencing will not be sufficient to identify California consumers that are traveling or using

another person's computer or device.

A consumer can authorize another person solely to opt-out of the sale of personal information on the consumer's behalf.

4. Right to Delete

Upon receipt of a verifiable consumer request, the business must delete the consumer's personal information from its records and direct any service providers to do the same.

There are a number of important exceptions from the right to deletion. A business or service provider is not required to delete a consumer's personal information if it is necessary to, among other things:

- Complete a transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- Comply with a legal obligation; or
- Otherwise use the consumer's personal information internally and in a lawful manner that is compatible with the context in which the consumer provided the information.

Additionally, a business that collects personal information about consumers must disclose to consumers the right to delete.

5. Right to be Free from Discrimination

A business must not discriminate against a consumer because the consumer exercised any of the consumer's rights under the CCPA, including, but not limited to, by:

- Denying goods or services to the consumer.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services to the consumer.
- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

A business is not prohibited from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

A business may offer financial incentives, including payments to consumer as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

A business that offers financial incentives must notify consumers with a clear description of the financial incentives and obtain the consumer's opt-in consent. A business must not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

6. Online Privacy Policy

Businesses that collect or sell consumer information, or who are subject to the opt-out right, must create a California-specific statement of privacy rights or include in its online privacy policy the following:

- A description of a consumer's rights to be informed of the categories of personal information to be collected and the purposes for which the categories of personal information are to be used, have personal information provided by the consumer to the business deleted, and request information from businesses that collect or share personal information, including the right to request the specific pieces of personal information the business has collected about the consumer.
- A description of a consumer's rights to be free from discrimination and, if applicable, any financial incentives that are offered and an opt-in.
- A list of the categories of personal information the business has collected about consumers in the preceding 12 months.
- A list of the categories of sources from which the personal information is collected.
- A list of the business or commercial purposes for collecting or selling personal information.
- A list of the categories of personal information the business has sold about consumers in the preceding 12 months, or if the business has not sold consumers' personal information in the preceding 12 months, a statement of that fact.
- A list of the categories of personal information the business has disclosed about consumers for a business purpose in the preceding 12 months, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, a statement of that fact.
- If applicable, a description of the consumer's right to opt-out of the sale of personal information and a link to the "Do Not Sell My Personal Information" Internet web page.

C. Exemptions

The CCPA does not restrict a business's ability to:

- Comply with federal, state, or local laws.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
- Exercise or defend legal claims.
- Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph does not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

The CCPA does not apply to the following:

- Where compliance by the business with the CCPA would violate an evidentiary privilege under California law. The CCPA does not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.
- Certain types of medical information.
- An activity involving the collection, maintenance, disclosure, sale, or use of personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, a furnisher of information, and a user of a consumer report, but only to the extent that such activity is subject to regulation under the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 *et seq*.) ("FCRA") and the information is not used, communicated, disclosed, or sold except as authorized by the FCRA.
- Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102) ("GLBA"), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code).
- Personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 *et seq*.).

- With regard to the right to opt out only, vehicle or ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or recall, provided that the dealer or manufacturer with which the information is shared does not sell, share, or use that information for any other purpose.
- Except with regard to the notice at collection, personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.
- Except with regard to the right to opt out of the sale of personal information and the right to be free from discrimination based on exercise of rights provided by the CCPA, personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a for-profit, non-profit, or government entity and whose communications or transactions with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such entity. Note that this exception is effective only through December 31, 2020. This exception could apply to personal information related to a business-to-business transaction or a vendor relationship.

Finally, the CCPA does not require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

III. Oversight & Training

Vanessa Mata (the "Compliance Director") is the Company employee responsible for coordinating this CCPA Policy. It is the Compliance Director's responsibility to manage the adoption, implementation, and maintenance of this CCPA Policy. In this role, the Compliance Director oversees Company's privacy protocols and ensures that Company employees adhere to these and other Company policies and procedures.

To the extent the Compliance Director is required to perform a task, the Compliance Director may appoint a person to act on his or her behalf.

All employees, agents and independent contractors that work for Company ("Personnel") will receive privacy training appropriate to their job responsibilities. The Compliance Director will be responsible for ensuring that new hires are trained, and that periodic and recurring training is

conducted for all Personnel. New hire training will be conducted within 30 days of an employee's hire date, and periodic and recurring training will be at least annually, or more frequently as changes in applicable laws may require.

IV. Procedures

Company will comply with the following as part of its CCPA compliance efforts.

Company is a regulated "business" under the CCPA when it collects, shares, and otherwise processes "personal information" on "consumers."

Company collects, shares, and otherwise processes personal information subject to certain of the exemptions from the CCPA.

To the extent that Company collects, shares, and otherwise processes personal information not subject to the CCPA's exemptions, Company will comply with consumer rights and business obligations as provided for above.

V. Recordkeeping

Company will retain paper and electronic records containing customer information for 2 years. Upon expiration of 2 years, any such records will be disposed of in a secure manner.

VI. Periodic Review and Legal Review

Company will actively monitor legal and regulatory changes that require changes to this Policy and any of the policies, procedures, or documents that support it, and will adopt any and all changes required to ensure that Company is in compliance with all applicable laws at all times.

The Compliance Director will review this Policy annually to ensure that it remains current (taking into consideration, at a minimum, changes and developments in the law, changes and developments in Company's operations, industry best practices, audit/testing results, complaint data, Company's litigation, and a study/analysis of exceptions). In connection with this annual review, the Compliance Director will ensure that a legal review is conducted.

Revision History

Company will log any changes or modification to this document in the Revision History table that follows. Company will reflect minor modifications with a decimal increment (*e.g.*, 1.4 would be followed with 1.5; 3.1 would be followed with 3.2). It will reflect major modifications in whole number increments to the version (*e.g.*, 1.4 would be followed with 2.0; 3.7 would be followed with 4.0).

Version	*Effective Date*	*Name & Title of Person Making Changes*	*Name & Title of Person Approving Changes*	*Description & Comments*